



## **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 North Central Audit Committee Network (NCACN) 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 NCACN was held by telephone on February 16, 2005, and focused on three questions related to enterprise-wide risk management:

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

The members of the network present at the meeting, who sit on the boards of more than 21 large-, mid-, and small-cap public companies between them, were:

- Jim Boland, Audit Committee Chair, The Goodyear Tire & Rubber Company
- Michael Gellert, Audit Committee Chair, Humana
- Frank Gori, Area Managing Partner, AABS, Ernst & Young
- Michael Losh, Audit Committee Chair, TRW Automotive
- Al Paulus, Partner, Ernst & Young
- George Smart, Audit Committee Chair, FirstEnergy Corporation
- Bill Smithburg, Audit Committee Chair, Corning

*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>

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



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). 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.

Despite broad agreement in many areas, ACLN and NCACN members diverge on the scope of the audit committee's responsibility for enterprise-wide risk management. ACLN members generally believe that the audit committee should address both financial and non-financial risks. In contrast, NCACN members do not believe the audit committee has the time or expertise to properly oversee non-financial risks; they believe it is the responsibility of the full board to review those risks. They also express concern that regulatory compliance may be encroaching on time available to effectively deal with more strategic activities, such as ERM.

- **Intuition trumps strategic process** (*Page 3*)

Although most NCACN members agree that risk management processes are important, not all have developed formalized mechanisms to identify and prioritize enterprise-wide risk in a systematic way. Members generally use experience and intuition to anticipate the most significant risks.

- **Integration of ERM with Section 404 is unlikely** (*Pages 3-4*)

Members disagree with observers who suggest that a company's Section 404 infrastructure could be extended to manage a more complex enterprise risk management effort, and they worry that frustration with the cost and disruption of Section 404 would decrease support for an integrated Section 404/ERM implementation.

- **Whose job is it, anyway? The full board should take responsibility** (*Pages 4-5*)

Members agree that audit committees are responsible for overseeing financial risks. However, several members feel the audit committee has neither the time nor the background to oversee non-financial risks, saying the full board should review these risks. Members do not want internal audit to lose their focus on important financial and/or operational risk areas, and feel internal audit's current competencies are not always aligned with those required to take a comprehensive view of enterprise-wide risks.

- **Disclosure decisions focus on financial risks** (*Page 5*)

Although companies routinely include a discussion of risks in their regulatory filings, members said that the audit committee's review of these filings was focused on financial reporting and those risk factors that have the greatest impact on the financial statements (including reserves, derivative exposures, etc.).



## Intuition trumps strategic process

Although “a lot of what the [audit] committee does, and says grace over, is risk,” members’ approaches to dealing with that risk exist along a spectrum, ranging from highly sophisticated processes to pure intuition. One member noted that “the process a company goes through [to oversee risk] is critical.”

- **Less complex processes**

In their December 2003 meeting, several ACLN members described reporting systems in which risks were assigned a priority rating (for instance, red, yellow, or green “traffic light” colors). Few NCACN members’ companies have adopted a similar risk reporting mechanism, and several members described a risk management process driven primarily by experience and instinct. Members following this approach do not use a prioritized list of risks, and some members doubted whether such a list would be practical. One member said, “As a board member, I could identify the top three [risks] maybe, not [the top] ten.”

- **More complex processes**

One of the members whose company adopted a more formalized approach to risk management said his audit committee discusses risk at every meeting, and “it’s a healthy discussion.” Another said the audit committee receives minutes from meetings of a corporate risk policy committee that includes the chief operating officer, chief financial officer, and chief risk officer. These members described a senior-level focus on risk, with one company even incorporating risk management into the strategic planning process.

Discussing the role of one audit committee member who had unusually sophisticated financial expertise, members voiced the opinion that as risks become more complex, individual directors may be asked to draw on their specific expertise. One member observed, “If you’re going to be on an audit committee, or be an audit committee chair, you may be called on more often individually.”

An ACLN member observed, “The process we use is more important than the checklist we use because the checklist cannot be complete.”<sup>2</sup> Ultimately, whether the process used was formal or informal, NCACN members agreed with the ACLN that “Process is the key word. What processes do we have to identify and prioritize the key risks?”

## Integration of ERM with Section 404 is unlikely

In September 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published its framework for enterprise-wide risk management. In publishing the framework, COSO indicated that a “strong system of internal controls supports the achievement of the organization’s business objectives and therefore good internal control is a way of managing risk. However, enterprise-wide risk management is much broader than internal control. In addition to supporting management’s efforts to

---

<sup>2</sup> Audit Committee Leadership Network, “Enterprise Risk Management and the audit committee,” *ViewPoints*, December 22, 2003, 4.



achieve business objectives, it aligns risk management with strategy setting and aids a company's ability to assess whether the organization is accepting risk appropriately."<sup>3</sup>

Because the COSO ERM framework is an extension of the earlier COSO framework used to assess internal controls for Section 404, some people have suggested that "[Sarbanes-Oxley] compliance could provide a much-needed infrastructure to support ongoing risk management."<sup>4</sup>

However, members viewed the COSO frameworks as overly complicated, and some questioned how much support the idea of integrating Section 404 and ERM processes would receive, given that many executives and directors are frustrated by the resources required to implement Section 404.

### **Whose job is it, anyway? The full board should take responsibility**

Members grouped risks into two broad categories: financial risks (including reserves, interest or exchange rate exposure, internal controls, etc.) and business risks (including pricing, competition, industry or global economic trends, material costs, etc.). One member described the latter category as *"the major risks that can put a company under."*

### **Board and CEO responsibility, not audit committee responsibility**

Although members agreed that the audit committee was responsible for overseeing financial risks, they questioned whether the committee was the appropriate forum for a discussion of non-financial risks other than those with an immediate impact on financial statements (e.g., reserves for environmental risk). Supporting a narrower focus on financial risks, one member said, *"I'm not sure audit committee members have the time or background to [review risk] on an enterprise-wide basis."* Some members thought that other board committees (e.g., compensation, finance) might be better suited to review specific risk areas.

Several members felt that enterprise-wide risk management was senior management's responsibility, with involvement from the board. One member said, *"Companies have to have the structure to deal with all this and report to the board because it's a board matter."* Furthermore, as the executive with the broadest perspective, *"the CEO should think about [risks] every day."* This view is consistent with that of ACLN members, one of whom observed, "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."<sup>5</sup>

### **Internal audit – back to basics**

Because of the unanticipated workload associated with Section 404 compliance, the role of internal audit has shifted in recent months. In one member's words, internal audit *"had the arms and legs and skill set, so they got drafted when it got to crunch time."* Audit committee chairs and internal auditors are starting to look ahead, and many anticipate a reduction of internal audit time devoted to compliance with Section 404. One

<sup>3</sup> Committee of Sponsoring Organizations of the Treadway Commission, "FAQs for COSO's *Enterprise Risk Management: Integrated Framework*," D3, [http://www.coso.org/Publications/ERM/erm\\_faq.htm](http://www.coso.org/Publications/ERM/erm_faq.htm)

<sup>4</sup> Joanne Sammer, "Companies Migrating from SOX 'Myopia' to ERM," *Compliance Week*, November 2004, 26.

<sup>5</sup> Audit Committee Leadership Network, "Enterprise Risk Management and the audit committee," *ViewPoints*, December 22, 2003, 6.



head of internal audit recently said his department's mission was to answer the question "Where is there risk?"<sup>6</sup> While the objective is well intentioned, audit chairs question whether internal audit currently has the competencies required to effectively identify or manage non-financial risks, and most believe that internal audit should take on a more narrowly defined role rather than a broader one.

One member observed that only a very senior-level executive has the perspective and credibility to influence enterprise-wide risk management activity. Members of both the ACLN and the NCACN felt some internal audit functions did not have the necessary competencies to develop a comprehensive view of risk. Further, they felt most internal audit functions had more than enough work reviewing the organization's financial and/or operational risks and controls. As one member said, *"Every now and then I see a head of internal audit who sees an opportunity to increase [the function's] mandate, and this always puts me on guard."*

### **Disclosure decisions focus on financial risks**

Regardless of the audit committee's role in overseeing enterprise-wide risks, it still bears primary responsibility for approving filings to the Securities and Exchange Commission (SEC), many of which include a discussion of key risk factors facing the company.

Members described a more comprehensive review process in recent years, with one member saying, *"I think there is more rigor on the part of audit committees. I see committees reading 10-Qs, reading 10-Ks, [holding] full audit committee meetings telephonically to discuss MD&A, when in the past it would have been delegated to the audit committee chair."*

Members felt audit committees' review of SEC filings should focus primarily on the financial controls and processes that impact the integrity of financial statements, and said they are not signing off on strategic business risks (e.g., excess global capacity). One member said that the corporation's general counsel spends a lot of time verifying areas of risk, while another said that the independent auditors review the entire 10-K carefully for consistency and completeness. This member noted, *"As an audit committee member, I take a lot of comfort in that."*

Still, members worried that in a defensive attempt to disclose all possible areas of risk, the discussion of risk factors in corporate 10-Ks has become increasingly expansive. One member described the listed risk factors as *"a laundry list of risks the lawyers think should be included."* Another member observed with some concern that *"increased boilerplate and formality get in the way of the bigger picture."* Given that risk disclosures are similar across companies, one member said that the best insight often comes from a review of changes to a company's list of risks from year to year.

---

<sup>6</sup> Audit Committee Leadership Network, "The Internal Auditor's Perspective," *InSights*, July 6, 2004, 4.



## **Conclusion**

Risk management is not about eliminating business risks, but rather about creating a process to identify 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.

Further, with directors relying on the CEO to provide leadership and perspective on enterprise-wide risks, the full board must ensure the CEO is identifying, prioritizing, and managing risks in a manner consistent with the company's strategic objectives.

## **About this document**

The North Central 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 North Central Audit Committee Network is a group of audit committee chairs from leading companies based in the Lake Erie and Ohio Valley regions. 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 North Central 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.*