



## **Risk management: in search of a practical approach**

### **About this document**

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

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

### **Introduction**

The North Central Audit Committee Network met on June 13, 2006, to discuss practical ways to manage enterprise-wide risks. They also discussed the evolving role of internal audit, the theme of a previous network meeting held on December 15, 2005. The members of the network present at the meeting, who sit on the boards of 17 large-, mid-, and small-cap public companies between them, were:

- John Baily, Audit Committee Chair, Erie Indemnity
- Jim Boland, Audit Committee Chair, The Goodyear Tire & Rubber Company
- Gordon Harnett, Audit Committee Chair, PolyOne
- Bill Lawrence, Audit Committee Chair, Ferro
- Dave McCammon, Audit Committee Chair, Pulte Homes
- John Shuey, Audit Committee Chair, Cooper Tire & Rubber Company
- Paul Smith, Audit Committee Chair, Constellation Brands

Other participants in the meeting included:

- Frank Gori, North Central Area Managing Partner, Audit and Advisory Business Services, Ernst & Young
- Steve Klemash, Pittsburgh Office Managing Partner, Ernst & Young
- Al Paulus, Senior Client Service Partner, Ernst & Young

*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**

The network's discussion revolved around several important ideas, summarized below and expanded upon in subsequent pages:

- **Risk management matters** (*Pages 3-4*)

Members said it is both important and timely for corporate leaders and directors to discuss risk management now, since external stakeholders are pushing companies to develop more effective risk management practices. Although many companies' risk management processes are at an early stage of development, members seek to actively influence the agenda to prevent risk management from becoming a value-subtracting, mechanistic activity. They recognize that effective risk management is about more than loss avoidance; they know it can be a meaningful source of shareholder value.

- **The audit committee is a catalyst for board oversight of risk** (*Pages 4-5*)

Members agreed that the full board has responsibility for risk management, but said it is not practical to oversee all risks as a group. Instead, management and the board should work together to allocate risk areas to specific committees. The audit committee is not responsible for all enterprise-wide risks, but it can serve as an important catalyst at the board level to ensure that major risk areas are being covered by the appropriate board committees.

- **Risk management is a process, not a project** (*Pages 5-6*)

Risk management is not a project to be checked off a to-do list. Instead, it is a fundamental management activity that is most effective when it is integrated with other business processes. Members said many companies are able to identify key strategic risks; however, not all companies monitor those risks consistently over time. Members described a wide range of effective practices, from highly analytical processes that engage the whole organization to more ad hoc processes that engage the executive team. A "top 10" list may help management and the board to align their understanding of key risk areas.

- **Senior executives drive risk management** (*Pages 6-7*)

Although a chief risk officer may drive the risk management process, the CEO is ultimately the one responsible for enterprise-wide risk management. Without senior management commitment, the risk management process is not likely to be effective.

- **Internal audit plays an important monitoring role** (*Pages 7-8*)

Members said internal audit generally has neither the time nor the broad skill set that may be required to lead the enterprise-wide risk management effort, but agree that it should play an important role.

The North Central Audit Committee Network first discussed risk management in February 2005; however, only one audit chair at the June 2006 meeting was in attendance 16 months earlier. Members at the February 2005 meeting said management typically reported risks to the audit committee, although the criteria used to prioritize risk were not always clear to audit chairs. Furthermore, they did not believe the audit committee had the time or expertise to properly oversee non-financial risks; they believed it was the responsibility of the full board to review those risks. Compared with the February 2005 meeting, the June



2006 discussion focused to a greater extent on the value of effective risk management, the importance of executive-level commitment, practical approaches to risk management, and the audit committee's ability to influence the process at the board level.

### **Risk management matters**

Members reflected on the fact that risk management has increased in prominence in recent years, which they say is a natural by-product of the Sarbanes-Oxley legislation, and believe more time should be spent on important discussions of risk identification, minimization, and mitigation. Members noted that some industries have more experience with risk management than others and described the importance of the Federal Deposit Insurance Corporation Improvement Act (FDICIA) of 1991<sup>1</sup> in driving enhanced risk management practices in the financial services industry. Members observed that while increasingly sophisticated risk management practices have evolved naturally over the last 15 years in the financial services industry, companies in less regulated industries now feel heightened urgency regarding effective enterprise-wide risk management practices.

Members are somewhat concerned that a one-size-fits-all risk management framework will be imposed by regulators, stock exchanges, large institutional investors, or ratings agencies. Standard & Poor's currently uses an enterprise-wide risk management metric when it rates insurance companies,<sup>2</sup> and members expect this practice to spread into other industries over time. Reflecting on the fact that management and board directors had little control over the shape of the Sarbanes-Oxley legislation, members feel they need to take the lead to avoid the imposition of ineffective processes.

### **In most industries, risk management activities are at an early stage of development**

Members agreed that risk management practices are most advanced in regulated industries such as financial services and utilities. However, they noted that *"it is a new discussion"* for executives in many other industries. Operating and strategic risks associated with manufacturing activities are very different from those associated with product distribution, and historically, few unregulated companies have tried to aggregate risks across corporate silos.

Members noted the lack of well-defined best practices, and one member claimed, *"There is no good business model [for risk management] in the industrial world."* It is therefore not surprising that many enterprise-wide risk management discussions are at an early stage. One member observed, *"We are [only] at the forming and storming stage,"*<sup>3</sup> while another noted, *"We're barely off the ground."*

---

<sup>1</sup> FDICIA was enacted in response to the widespread failures of savings and loan institutions in the 1980s.

<sup>2</sup> Standard & Poor's Ratings Services has added an enterprise risk management (ERM) criterion when rating insurance companies. S&P is basing its ERM rating on five key metrics: risk management culture, risk controls, extreme risk management, risk and economic capital models, and strategic risk management. The evaluations of each of these areas will be combined to yield a single rating – excellent, strong, adequate, or weak – of ERM quality. For more details, see the sidebar "Agency Develops ERM Metric" at [http://www.riskandinsurance.com/060501\\_specreport\\_1.asp](http://www.riskandinsurance.com/060501_specreport_1.asp).

<sup>3</sup> In 1965, Bruce Tuckman first proposed a model of team development that maintained that several phases are necessary and inevitable in order for a team to grow, to face up to challenges, to tackle problems, to find solutions, to plan work, and to deliver results. The phases are: forming, storming, norming, and performing.



### **Risk can be a source of value**

While fear of regulation may be driving a heightened focus on risk management, members also recognize that effective risk management practices can have many benefits. One member spoke of a recent *BusinessWeek* article that described how some investment banks have used advanced risk management techniques to drive superior financial performance.<sup>4</sup>

Some risks can destroy a company, while others are associated with unique strategic opportunities. Members said that companies are in business to take measured risks and agreed it was important for management and boards to understand the key operating and strategic risks. Board directors often support management's decision to take well-understood risks in order to seize opportunities. For example, members said there are many risks associated with expansion into Asia (e.g., protecting intellectual property, choosing the right partners, repatriating profits), yet they are confident telling management, *"You have to go [to China]."*

Members said the challenge was to integrate the risk-based perspective with a strategic-opportunity-based perspective. One member described a new product launch in which management focused primarily on market opportunity, competitive environment, etc., rather than on risk. The launch had public-policy implications and created new categories of risks (e.g., product recall, production challenges, potential litigation). However, the business plan did not address those risks specifically; instead, it *"assumed [we would] manage the risks along the way."* Although the decision to launch the product was sound, the member said management and the board would have approached the implementation differently had they viewed the launch from a risk-based perspective.

### **The audit committee is a catalyst for board oversight of risk**

While appreciating the value of strategic risk management, members also noted the limits of directors' oversight responsibility. Many wonder, *"[As a board director,] how do you add value, make sure [risk management is] not a paper exercise?"* One member was concerned that many of the most significant risks are those *"we have no control over at all."* Ultimately, members believe that boards can provide value by ensuring that in crafting corporate strategy, management also has a plan to manage or mitigate the associated enterprise-wide risks (whether strategic, operating, or compliance related).

Members agreed that although the audit committee has an important role to play in enterprise-wide risk management, it should not be solely responsible for overseeing all risks. Several members said financial and compliance-oriented risks fall within the audit committee's charter, but did not feel the audit committee was ideally suited to review the broader set of risks. Ultimately, the full board needs to agree on *"how to divvy up risk, because nobody wants to look at the whole thing."* One board worked with management to assign permanent board committees responsibility for overseeing each of the major risk areas. As one member observed, *"the [full] board has responsibility [for risk management] ... [the question is] how you get it done."*

---

<sup>4</sup> Emily Thornton, "Inside Wall Street's Culture of Risk," *BusinessWeek*, June 12, 2006. Available at [http://www.businessweek.com/magazine/content/06\\_24/b3988004.htm](http://www.businessweek.com/magazine/content/06_24/b3988004.htm).



Ultimately, the audit committee's involvement in risk management may range from full responsibility for risk oversight to process leadership only, ensuring that risk is discussed by the full board or a committee of the board. One member said the audit committee should play a "facilitation" role, making sure an adequate risk management process exists and is being followed. That level of involvement is the minimum specified for the audit committee in New York Stock Exchange (NYSE) regulations.

Some members wondered whether the governance committee might take a more active role in allocating responsibilities for oversight of risk management across board committees. However, others noted that governance committee charters are often too narrow to encompass this role. Most members feel the audit committee is the logical catalyst for risk management oversight at the board level, and several members described situations in which the audit committee had shaped the full board's approach to risk management.

**What is the audit committee's role with respect to risk oversight? The NYSE listing rules state:<sup>5</sup>**

- "While it is the job of the CEO and senior management to assess and manage the company's exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the company's major financial risk exposures and the steps management has taken to monitor and control such exposures.
- The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken.
- Many companies, particularly financial companies, manage and assess their risk through mechanisms other than the audit committee. The processes these companies have in place should be reviewed in a general manner by the audit committee, but they need not be replaced by the audit committee."

**Risk management is a process, not a project**

Members agree that effective risk management is not a one-time project that can be checked off a list; it is an ongoing process of continuous review and revision. As one member said, "It's a forever project," not unlike Section 404, which began for many companies as a project but is slowly becoming embedded in business processes.

**Focus on the "M" not the "R"**

When executives and board directors think of enterprise risk management (ERM), many naturally focus on the "R" (risk). However, one meeting participant said the real value is in the "M" (management). This participant asserted that the most effective risk management practices are embedded in existing business processes, not developed as separate and distinct processes. Since one-size-fits-all approaches are rarely aligned with a company's existing processes, a risk management program usually must be customized to the specific needs and capabilities of the organization.

<sup>5</sup> Commentary from the *Final NYSE Corporate Governance Rules* 303A.07(c)(iii)(D). Available at <http://www.nyse.com/pdfs/finalcorpgovrules.pdf>.



Members said many companies manage risks effectively at the operating-unit level, but they described challenges when it comes to communicating and mitigating risks across silos. Furthermore, members said that many companies need to follow up methodical processes for identifying risks with equally robust processes for monitoring them. One member said, *“We have a good handle on what [strategic risk] is, but we’re nowhere on monitoring it.”* Another agreed that *“consistency of monitoring is not there.”*

### **There is no single correct approach to risk management**

In an effort to measure risk more rigorously, some companies have developed extensive polling processes. One audit committee chair described a survey that is sent to all board directors and the top 1,500 leaders of the company, asking each to evaluate up to 25 risks according to both the likelihood and the effect of occurrence. The data can then be analyzed along many dimensions (e.g., management and board perceptions of risk, differences across geographies, changes in the perception of risk from year to year).

Members agree that there are many ways companies can identify and assess the most significant risks to the enterprise. However, members said that even the most sophisticated analytical models have limitations. One member asked rhetorically, *“Which model identified the backdating of stock options as a risk?”* Some members wondered if senior management could generate a meaningful list of risks using a less analytically rigorous process: *“If [management] spent two hours [generating a list of key risks], could they save reams of paper and hours of staff time?”*

One member described a situation from his own career, when a senior executive asked him *“to list the ten top problems the company faces by tomorrow morning.”* The member delivered the list and was relieved that he had been given only a short time to work on the request.

Another member described an instance recently when the board was uncomfortable with the lack of analytical rigor in the company’s strategic plan and pushed the CEO to present a list of key risks associated with the strategy. The board asked, *“What are the 10 biggest risks, and what are you going to do about them?”* The company’s top executives developed a seven-page document that represented their assessment of the top 15 risks, and the member was *“overwhelmed”* by the output. While many of the risks were well-known to both management and the board, the member said that the board directors had not recognized the significance of about a third of the risks. Moreover, the member noted, *“The management team took ownership [of the risks] in creating the document.”*

### **Senior executives drive risk management**

Members said the energy behind any risk management effort must come from senior management, not the board. As one member said, *“It’s not [effective] for the board to have a view [on risk management] without management being committed to it.”*

### **The CRO is a process owner**

The chief risk officer (CRO) title is widely held in the financial services and utility sectors. However, it is found less frequently in businesses that are subject to lower levels of regulation. Members said a CRO



should not be expected to “own” all enterprise-wide risks, but should instead be responsible for ensuring that an effective risk management process is in place and functioning smoothly. One member said the CRO’s job is to *“move the ball, but not get the ‘attaboys’ [when things go well], or get shot if there is a problem.”* However, despite the importance of an effective risk management process, another member observed, *“Trying to find someone internally who wants to be in charge of that is [hard].”*

### **The CEO is the real chief risk officer**

Members agree that senior leadership is critical to the success of an enterprise-wide risk management program and that *“it’s not going to work in any company unless the CEO takes the lead.”* One member said the CEO needs to take a personal interest in risk management, noting *“[Where the CEO has] delegated [risk management] to other high-ranking executives, it has stumbled.”*

Members said the CEO should be involved in risk management from the start, even before a list of key risks is created. Furthermore, members said the CEO’s commitment is important, regardless of whether the company is regulated or not. One member said, *“The industry doesn’t matter. It’s a leadership issue, no matter what industry you are in.”*

While some board directors are comfortable pushing management for a comprehensive risk assessment and mitigation plan, others are less so. One member asked the others, *“When was last time you challenged the CEO [about the risks to the business]?”*

### **Internal audit plays an important monitoring role**

Although members said the CEO must drive the risk management effort, they also agreed that *“internal audit should be part of the team.”* One member qualified that by saying that internal audit plays an *“important part, but they don’t lead [risk management efforts].”*

Given the importance of information technology, many companies are especially interested in monitoring and mitigating IT risks. However, members said it is exceedingly difficult to retain internal audit staff with up-to-date technology skills. As one member said, *“The IT gap is serious.”*

To help close the gap, some companies are outsourcing IT audit services. This approach offers dual benefits: companies are provided with the necessary expertise required to complete the IT audit work, and outsourced IT professionals offer de facto training for in-house IT auditors. Alternatively, companies with decentralized IT functions may be able to assess IT risks by assigning IT professionals in one business unit to audit the IT operations in another part of the company.

Members said that internal audit often performed an operational improvement role before Sarbanes-Oxley. However, in recent years, internal audit has focused on financial audits and Section 404 internal control testing. Members are concerned that the new compliance requirements mean that *“internal audit has changed, maybe forever.”*

As many companies transition Section 404 testing responsibilities from the internal audit function to the operating-unit level, some internal auditors are looking for *“white space”* in which to pursue a broader



agenda, which may include risk management. However, members question whether that is the best use of internal audit's time and talent. Reflecting on the operating audits that were postponed in the initial flurry of Section 404 activity, one member said, *"I don't see a whole lot of white space."*

Some companies, however, have sought to reduce Section 404 compliance costs by shifting work from external resources to internal audit. Members are concerned that this may be a false economy. While the decision to shift Section 404 responsibility to internal audit may appear cost-effective in the near term, over time it may be difficult to recruit and retain talented internal auditors who derive satisfaction from a role that is largely focused on regulatory compliance. For companies with a small internal audit group, the problem is exacerbated by limited flexibility in creating developmental opportunities for internal auditors.

Consequently, members said it remains difficult to hire and retain talented internal audit staff. One member said internal audit salaries have increased 20% over the last 18 months, prompting another member to raise concerns about pay equity across the company. Some question the sustainability of a model in which internal audit continues to perform a substantial amount of Section 404 work.

## **Conclusion**

A popular Chinese proverb says that "a journey of a thousand miles begins with a single step." In the quest for a practical approach to risk management, this much is clear: risk management is a journey, and companies should not wait until they have a clear road map to set out. Rather, they can take a first step and begin to identify enterprise-wide risks, then develop a plan to mitigate those risks. Despite members' assertion that, over the long term, risk management is a process rather than a project, it may be necessary to first launch a limited risk management project. Over time, companies may decide to modify scope, redeploy staff, or realign activities with existing business processes.

At the same time, risk management should not be misinterpreted as risk elimination. One member warned, *"The worst thing that could come out of [enterprise-wide risk management] is that you create a risk-free environment, or shoot someone for taking a risk."* The challenge for management and directors is to develop a risk management framework that not only minimizes the likelihood and effect of undesirable outcomes, but also supports and enhances the company's strategic growth agenda.

*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.*