



Risk management: in search of a practical approach

Synopsis

Audit committees play a meaningful, and often vital, role overseeing corporate risk management policies and procedures, and probing management with revealing questions about specific risks. Management retains responsibility for assessing, managing and mitigating risks. Audit committee chairs agree that the level of the committee's involvement depends on the nature of the risks, the board structure, and the capabilities of individual directors. They question the efficacy of comprehensive risk management frameworks. While they recognize the value of centralizing some risk management activities, audit chairs note the lessons of Sarbanes-Oxley compliance and caution boards not to favor form over function.

Introduction

The Mid-Atlantic Audit Committee Network¹ met for the seventh time on April 13, 2006. Members discussed practical ways for boards and audit committees to oversee enterprise-wide risk management activities effectively. Increasing interest in risk management has not necessarily led to further clarity. While standardized frameworks can be helpful in overseeing certain types of risk, audit chairs are seeking a more practical approach. They were interested in discussing the relative roles of the audit committee and the full board in risk management and in how best to fulfill the responsibilities that fall to the audit committee.

Network members participating in this face-to-face meeting included:

- Jim Brady, Audit Committee Chair, Constellation Energy Group
- Bob Grafton, Audit Committee Chair, CarMax
- Charlie Hopkins, Audit Committee Chair, Charming Shoppes
- Mike Ressler, Audit Committee Chair, Magellan Health Services
- John Schwieters, Audit Committee Chair, Smithfield Foods
- Paul Shapiro, Audit Committee Chair, Toll Brothers
- Jim Zug, Audit Committee Chair, Amkor Technology
- Mark Bartlett, Senior Client Service Partner, Ernst & Young
- John Tierney, Managing Partner, Assurance and Advisory Business Services, 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.

¹ The Mid-Atlantic Audit Committee Network is a group of audit committee chairs drawn from leading companies based in the Mid-Atlantic region 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 audit environment.

VantagePoint is a synthesis of some key issues arising from a facilitated discussion among members of the Mid-Atlantic Audit Committee Network. It is intended 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.



Executive summary

Lively discussion among the members of the Mid-Atlantic Audit Committee Network centered on several important issues, all with substantial implications for audit committee chairs. These issues are summarized below and expanded upon in subsequent pages:

- **What is risk management?** *(Pages 2-3)*

Members unanimously agreed that risk management matters a great deal. However, they also recognize that not all risks should be managed the same way, and they believe the board should focus on the risks that most impact shareholder value. Moreover, they are less concerned with treating risk management as a discrete discipline and more with simply assuring that the company is effectively managing risks.

- **What is the role of the audit committee and the board?** *(Pages 3-5)*

Members said it was most important for the audit committee to have a clear understanding of what the risks are, how the risks are being managed, and the audit committee's role in risk management. They agreed that while the audit committee should have responsibility for overseeing some risk areas (including financial reporting and regulatory compliance), the full board is ultimately responsible for the enterprise-wide risk management effort (including operating and strategic risks). The board's work style, committee structure, and individual director capabilities all determine how and where specific risks are overseen.

- **What is management's role?** *(Pages 5-6)*

Members agree that management plays the lead role in risk management. By design, businesses take risks – for which they earn a return. Management and organizational capability is required to effectively mitigate strategic and operational risk.

- **Is there a single best-practice approach for risk management?** *(Page 6)*

Risk management is a pervasive board and management activity. It is integral to board discussions of strategy, capital spending, compensation and management development, regulatory compliance, and crisis planning. While frameworks such as COSO may be effective for managing certain types of risk (e.g., financial reporting and compliance), members say they are less effective in managing strategic and operating risks that do not lend themselves to categorization within existing frameworks. Members also report that much can be learned from how their companies handled – or would have handled – catastrophes.

Does risk management matter?

Mid-Atlantic Audit Committee Network members unanimously endorsed the proposition that risk management matters a great deal in public corporations. While management is ultimately responsible for developing and executing processes to assess and mitigate risk, the board plays an important and valuable oversight role.

The members agreed that most financial services, utility, and energy companies do an exceptionally good job managing enterprise-wide risks. However, outside those industries, members said the focus on risk



management varies considerably. One member said candidly of a company he represents, *“We are doing a lousy job of [risk management], if we really admit it.”* Ultimately, members said it was most important for the audit committee to have a clear understanding of what the risks are, how the risks are being managed, and the audit committee’s role in risk management.

Members said many risks develop slowly over time, and their impact may be almost imperceptible until it is too late. Members spoke of the challenges currently facing some vehicle manufacturers, and some noted that the situation was the result of the cumulative effect of decisions made many years ago. Although *“management makes the best decisions they can at [a] point in time,”* members agreed that *“a couple of innocuous decisions [can] take you down a [destructive] path.”* A forensic analysis may isolate those key inflection points in retrospect, but one member observed that *“it is hard to see [those] point[s] when you are in it,”* and failure to recognize them may make it impossible to break the chain of events that can lead to a *“death spiral.”*

In considering their company’s risk management capabilities, members distinguished between management of financial reporting and regulatory compliance risks, which they believe is usually well-structured, and management of operating or strategic risk, for which *“the structure isn’t there.”* Members are concerned about risks that may impact the company’s reputation and agree that *“what bites you in the [rear end] are the risks you never thought of.”*

This view is consistent with the findings of a recent Booz Allen Hamilton (BAH) study of companies whose stock price significantly underperformed over a six-year period. The BAH analysis determined that “only 13 percent of the value destroyed by these companies resulted from compliance failures; the other 87 percent was attributable to strategic and operational blunders.”² Members agreed that while regulatory compliance is important, the board needs to focus its attention on risk factors that most impact shareholder value.

Moreover, members agreed that merely talking about a risk factor is not the same as managing it effectively. Some risks are complex, and a company’s ability to properly mitigate a risk may be limited. One member said management and the board can talk about managing risks, but in some cases there may be few solutions available. When dealing with seemingly intractable problems, *“we’re human, so we do the easy thing ... we build a model.”*

What is the role of the audit committee and the board?

Members unanimously agreed that their boards shoulder responsibility for oversight of risk management and that they take those responsibilities seriously. Although every board will allocate risks differently, members generally believe the full board is responsible for overseeing operating and strategic risks, while the audit committee should focus on financial and compliance risks.

Interestingly, the published corporate governance guidelines of several ACN member companies never mention the word “risk,” although the delineated responsibilities of some boards clearly encompass many

² Paul Kocourek and Jim Newfrock, “Are Boards Worrying About The Wrong Risks?” *The Corporate Board*, March–April 2006, 2. The complete document is available at http://www.boozallen.com/media/file/worrying_about_the_wrong_risks.pdf.



risk elements. Further, consistent with the New York Stock Exchange listing rules, audit committee charters almost always explicitly lay out the committee's role in overseeing corporate risk management policies and reviewing financial risk exposures.

What is the audit committee's role with respect to risk oversight? The NYSE listing rules state the following:³

- "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."

Audit committee role

The Mid-Atlantic Audit Committee Network first discussed enterprise-wide risk management in March 2005. The *VantagePoint* produced after that meeting reported that:

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."*⁴

One member said he was surprised that in the March 2005 meeting the network had concluded that the audit committee is only responsible for financial statement risks. This member believes the audit committee *"needs to be involved [more broadly], but not be a dumping ground for risk."* Another member said the audit committee can be a catalyst for risk management because *"as an audit committee, we look at risks all the time. That's what we do."*

To some extent, senior management is encouraging a broad focus on the part of audit committees. Last December, Tapestry Networks interviewed nine CFOs and reported, "As the amount of time spent on

³ Commentary from the *Final NYSE Corporate Governance Rules* 303A.07(c)(iii)(D), <http://www.nyse.com/pdfs/finalcorpgovrules.pdf>.

⁴ Mid-Atlantic Audit Committee Network, "Enterprise Risk Management and the audit committee," *VantagePoint*, March 16, 2005, 3.



Section 404 compliance subsidies, CFOs are seeking to involve the audit committee in broader initiatives, including enterprise-wide risk management.”⁵

One member said the audit committee took responsibility for overseeing an extensive risk assessment process led by the CFO and the head of internal audit. Management came back to the committee with a comprehensive list of risks and a clear, concise summary of those that were most important. The committee didn’t focus on the full 242-page report, but rather on that summary of the top ten risk areas.

The following represents a typical allocation of the board’s risk oversight responsibilities:

Full board

- Management succession
- Sourcing/suppliers
- Competition
- Political risks

Audit committee

- Financial reporting and regulatory compliance
- Ethics
- Legal risks
- Business continuity

Full-board role

While some audit committee chairs believe that, in an ideal world, discussion of enterprise-wide risks should take place at the full-board level, their board colleagues sometimes disagree. One member tried to initiate a risk management discussion with the full board and was told, *“It’s an audit committee issue ... bring it up at the audit committee meeting.”* The full board only agreed to include risk management on their agenda after another board director supported the audit committee chair.

Members agreed that support for risk management *“has to start with the CEO, at the full-board level.”* However, some members said risk management rarely gets adequate coverage at board meetings because *“the CEO doesn’t explicitly deal with it [on the agenda].”* Instead, *“we get consumed by near-term agenda items.”*

In addition, every board has a different operating structure, so *“every board handles [risk management] differently.”* Some boards are highly centralized, while at other companies most of the work is done at the committee level. Reacting to the view that the full board should play an active role overseeing risk management, one member argued, *“It’s not practical at our company for that to happen.”*

What is management’s role?

By design, businesses take risks – for which they earn a return. As Cynthia Glassman of the Securities and Exchange Commission (SEC) has observed, *“Companies need to take risks to make money. This is about companies managing risks appropriately, eliminating some risks if they can, and managing those risks if they can’t.”*⁶

⁵ Tapestry Networks and Ernst & Young, “The CFO’s perspective,” *InSights*, December 22, 2005, 5. Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_Dec05_InSights.pdf.

⁶ Joanne Sammer, “Pressure Grows to Disclose ERM Information in MD&A,” *Compliance Week*, January 2005, 6.



Members agreed that no amount of risk management coordination can substitute for the capabilities of the management team. After all, management is hired to spend all day, every day working on typical business risks. In comparison, for pure business risks, members felt the board should be simply *“dotting I’s and crossing T’s.”*

Ultimately, *“the board’s job is to ensure that management is doing its job ... Is there anything that we’ve thought of that they haven’t?”* Members said they would be concerned if management was not on top of core business risks; one member noted, *“If management doesn’t know what to do when the competition drops its price, that’s a board to get off.”*

Is there a single best-practice approach for risk management?

Members recognized that while many companies are increasing their focus on risk management, they are *“all doing [it] somewhat differently.”* Members say there is no single best practice, and note that regulated businesses often approach risk management in a different way from those that are unregulated. They agreed with the member who noted, *“It’s okay for us all to do it differently, but it’s important that we do it.”*

The most commonly discussed risk management framework is COSO, developed by the Committee of Sponsoring Organizations of the Treadway Commission. Members are skeptical of the value of any standardized framework for managing risks. Despite COSO’s value in Section 404 compliance, several members said that COSO was not a suitable framework for broader risk management activities.

Members said that management and the board should formalize risk assessment *“in order to ensure you have done as good a job as you can.”* However, companies periodically face catastrophes whose magnitude *“shocks and overwhelms you.”*

Although *“management and boards are not expected to be prescient,”* with regard to predicting a disaster, members believed it was possible to draw important lessons from catastrophic events after the fact. Looking at catastrophes that have befallen others (e.g., Hurricane Katrina), members felt it was useful to ask management, *“How would you have reacted?”*

In particular, members said companies should have a thoughtful disaster recovery plan. Although every situation will warrant a different response, members said it was important to determine in advance who needs to be in the room so the company doesn’t spend two or three days preparing a response. After all, when CNN calls, *“The first words out of the CEO’s mouth can make or break you.”*

Members were especially concerned about the threat of an outbreak of avian flu. One member noted that companies shut down for weeks at a time during the 1918 influenza pandemic. Another member said a flu outbreak was *“probably more real than Y2K,”* but members noted a gap between the significance of the threat and the planning activity to date. As one member asked, *“What are you going to do if you have a pandemic? None of us really knows.”*



Conclusion: Boards should take a strategic view of risk, balancing risk oversight cost with benefits

While members agree that all significant enterprise-wide risks should be managed, they warned against creating a bureaucratic risk management process whose cost exceeds its value. Considering a hypothetical case in which many people have been assigned responsibility for the key risk areas but there is no centralized coordination, one member warned against *“creating another Sarbanes-Oxley.”* He explained, *“We don’t want to spend a lot of time and money forcing the company to do something it’s already doing [just because] it doesn’t know who’s doing it.”*

Members agreed it was important for the board to solicit perspectives on enterprise-wide risks from across the organization. One member helps to facilitate an annual discussion of senior leadership that focuses on a single open-ended question: *“What’s bothering people?”* This discussion helps to set the agenda for *“out-of-the-ordinary”* topics that should be covered in future audit committee meetings and determines what presentations should be made to the full board. Another member regularly asks senior leadership, *“What keeps you up at night?”* This member reports getting some interesting responses when the question is posed to the external auditors, including perspectives on the number and quality of the financial staff.

Several members described an annual strategy-setting retreat, which they felt offered an ideal opportunity to integrate a risk perspective with business planning. Unfortunately, from year to year, *“the strategy gets better, and risk management limps along with it.”* One company does a classic SWOT analysis as part of their strategic planning process, but doesn’t link the weaknesses with specific risks listed in the 10-K. Another member believes boards should review the risk factors set out in the 10-K and compare those that are actively managed with those that *“we pay lip service to.”*

Merriam-Webster defines risk as the “possibility of loss or injury,” and it is therefore not surprising that members viewed risk management through the lens of loss avoidance. However, even well-managed companies routinely miss upside opportunities as well: lacking the foresight to enter new markets, charging too little for their products, or deciding not to aggressively pursue executive talent. From a practical perspective, shareholders should be equally loathe to pass up an opportunity to earn \$100 as they are to lose \$100.

Instead of defining risk management as a set of activities that protect against negative events, might not companies broaden the boundaries of risk management to include activities that not only protect shareholder value, but serve to enhance it as well? How would this impact companies’ approach to risk management? These are questions that boards and audit committees might well consider.

The views expressed in this document represent those of the Mid-Atlantic Audit Committee Network and other similar networks of audit committee chairs. 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.