



Enterprise risk management and the audit committee

Introduction

The Southeast Audit Committee Network (SEACN) held its second meeting in Atlanta, GA, on October 18, 2005. Discussion focused primarily on managing enterprise risks and on the audit committee's role in:

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

This document reflects a synthesis of key issues arising from that meeting. In addition, in an unstructured open session, members raised matters of current concern that included year two of Section 404, the emerging expectations gap audit committees must deal with, and the future of the accounting profession.

The members of the network present at all or part of the meeting, who sit on the boards of nearly 25 large-, mid-, and small-cap public companies among them, were:

- Eddie Adair, Audit Committee Chair, Tech Data Corporation
- Kermit Campbell, Audit Committee Chair, SPX Corporation
- Joe Cegala, AABS Managing Partner, Ernst & Young
- Jim Copeland, Audit Committee Chair, Equifax
- John Farrell, Audit Committee Chair, Fidelity National Financial
- Tom Hough, Area Managing Partner, Ernst & Young
- Doug Ivester, Audit Committee Chair, SunTrust Banks
- Max Lennon, former Audit Committee Chair, Duke Energy
- Dean O'Hare, Audit Committee Chair, Fluor Corporation
- David Rickard, Audit Committee Chair, Harris Corporation
- Jim Robbins, Audit Committee Chair, Dollar General Corporation
- Peter Wood, Audit Committee Chair, Eastman Chemical Company

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

Risk management is not about eliminating business risks, but rather about creating a process to identify and address risk. In order to fulfill their duties to shareholders, directors must have a comprehensive understanding of their companies' risks. Many companies are beginning to pursue enterprise risk management (ERM), a methodology that views risk in the context of business strategy rather than looking at individual hazards. Members of the Southeast Audit Committee Network believe there is no "one-size-fits-all" ERM process; *"every company has different risks, so the risk assessment process must differ."* The insights of members are highlighted below, with more detailed discussion on the following pages:

- **Risk management derives from the strategic plan** (Page 3)

How a company manages risk depends on the sector in which it operates, the culture of the organization, and the experience of the board and audit committee. Nevertheless, commonalities of approach exist. Members of the Southeast Audit Committee Network agree that the risk management process begins with strategic planning. They observed that enterprise risk might well be defined as the risk of *"not achieving the strategic plan."* Risk management must be part of the corporate culture. Members feel the COSO framework¹ for enterprise risk management is a useful, tactical tool to help management ensure they have identified all the risks in the strategic plan.

- **Learning from extreme events** (Pages 3-4)

No company can anticipate every risk, but members advocate scenario planning, crisis management planning, and contingency planning to address *"the broadest number of plausible futures."* Actual incidents become opportunities to review and refresh the company's risk management process.

- **The board's role: ensuring the process is robust** (Pages 4-5)

SEACN members seek a clear division between what management is charged with and the board's role. Since risks are identified by the strategic planning process, network members said a director's responsibility is to ensure that there *is* a management process of high-quality that the board understands and with which they are comfortable. Which board committee then oversees risk management, or discusses particular risks, is less important.

- **Management's role: running the process** (Page 5)

Most members say risk in their company is devolved to line management, although some companies – particularly in financial services – delegate risk management to chief risk officers. Members found value in having a risk committee with company-wide representation coordinate the process. Most members agree that internal audit has an important role to play in risk management, particularly for assessments of the risk management process.

- **Risk disclosure: balancing transparency for investors with protection for directors** (Page 5)

Members would welcome a return to meaningful disclosure that represents the risks to the business. Most audit committees regularly review the MD&A to amend it for current conditions. Aware that

¹ Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrated Framework: Executive Summary*, 5. Available for download at http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf



some companies review competitors' disclosures, members also debated whether it is better to "out-disclose" or disclose less than the competitor, but most saw over-disclosure as disadvantageous.

Risk management derives from the strategic plan

The complexity of today's environment is leading many enterprises to take a more systematic, integrated, and holistic approach to managing risk. Members said they use the development of the strategic plan – a process that "*needs to be more than 'base case plus or minus 10%'*" – to surface the major enterprise risks their business faces. One member said, "*There is a real danger in separating risk management from the strategic planning process. Risks should be implicit in the strategy, otherwise you may end up focusing too much on little things, rather than the big ones.*"

Board directors, a member suggested, have the responsibility to question whether the strategic plan is highlighting those risks. "*We cannot generalize about risk, [hence] the importance of thoughtfully questioning the strategic plan. Curiosity and asking questions, not being satisfied until we get answers, are the most important attributes of a board member.*" Members agree that "*an absence of understanding on the board's part suggests there may not be such a process [to highlight risks as part of the strategic plan].*"

While the majority of a business's risks tend to be quite similar each year and "*don't grow up overnight,*" refreshing the list of risks periodically keeps an organization prepared to respond to most eventualities. "*It's important to review the strategic plan over the course of several [board] sessions, not just at one meeting, to understand the evolution of the thought process.*"

One company had each division or business unit identify their top risks, which are then aggregated. "*It may not raise every single risk, but you have confidence that this is the best educated guess.*" The COSO framework is seen as a useful, tactical management tool, a "*root map to trigger thoughts that might identify risks,*" as one member put it, noting that in his company, "*the audit committee has to constantly be sure that someone, whether it's internal audit or a chief risk officer, goes through COSO, but then the committee must focus debate on the four or five biggest risks ... each year.*"

Learning from extreme events

No company can anticipate every risk, but members advocated scenario planning, crisis management planning, and contingency planning to address "*the broadest number of plausible futures.*" Learning from other companies' experiences in crisis situations helps an organization prepare for unexpected situations that might arise. "*The improbable can and will happen. If we analyze every extreme event – Hurricane Katrina, 9/11, 18 inches of rain in the northeast – and ask 'how would we react?' we're doing what a board member should: constantly evaluating whether management is doing its job, asking, 'Are we in good shape if this happens to us?'*"

One member noted that because his company had the foresight to develop a crisis plan following the February 1993 bombing at the World Trade Center, it was able to avert a far worse outcome when the attacks of 9/11 came, although the company "*still lost something because [the plan] was about 25% degraded and obsolete.*" Similarly, a member said his audit committee reviewed its disaster planning around a New



York City transit strike and Y2K and found “we had technology and logistics in good shape, but hadn’t spent enough time on the people side: how are we going to keep going if people can’t get in to work?” The company beefed up the risk management plan to address this issue. Another member said that in observing how the financial services sector manages risks, he found approaches that were transferable to his own industry.

Members also reflected on their own responsibility to learn from extreme events. One described a graduated “scale of increasing concern to where, as an audit committee chair and board member, I am very active and responsive to what I hear. I’m on the phone with the CEO immediately if there is a crisis, and I’m not so sure that would have been true a few years ago.”

The board’s role: ensuring the process is robust

The board, or one of its committees, must ensure the risk management process is robust. SEACN members seek a clear division between what management is charged with and the board’s role. A number of members cited efforts – some by management – to “almost pull the board into management. The board must be vigilant about our [respective] roles.” Being clear on who has oversight of risk management was more important to SEACN members than who the responsible party ultimately is.

Still, many audit committee chairs remain divided about whether risk is the responsibility of the audit committee, the full board, or another board committee:

- **The audit committee.** Some members prefer to see ERM reside with the audit committee, since “ultimately all risk has financial statement impact.” 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.² The NACD Blue Ribbon Commission on Risk Oversight states, “Experienced audit committee members generally agree that the scope of the committee goes beyond oversight of financial reporting, and ... includes oversight of financial risk and legal compliance.”³ Another member said, “My audit committee gets at the largest issues.”
- **The full board.** One member felt strongly that “risk is not an audit committee issue, but a full board issue: our list of risks is so long, we would be overwhelmed.” His organization also split its former audit committee in two, creating a risk committee with its own charter and staff. For another member, “there is nothing uniquely financial about ERM. The audit committee should do the financial stuff, otherwise it’s a whole-board issue.”
- **Another board committee.** Members agree that enterprise risk can just as effectively be overseen by the governance committee or a risk committee of the board. One member said, “ERM was pushed on the audit committee [by the New York Stock Exchange] because the last crisis was financial.” Had it been environmental, he believed, another committee would have risk oversight responsibility.

² Final NYSE Corporate Governance Rules 303A.07(c)(iii)(D), <http://www.nyse.com/pdfs/finalcorpgovrules.pdf>

³ National Association of Corporate Directors, *Report of the Blue Ribbon Commission on Risk Oversight: Board Lessons For Turbulent Times* (Washington, DC: National Association of Corporate Directors, 2002), 33.



Beyond these oversight options, members are clear that the full board needs to be an integral part of the process. *“Whoever oversees this, the board must devote some significant part of at least one meeting per year to ERM,”* said a member who serves on multiple boards. *“My boards’ [annual] strategic planning meetings go for a couple of days, and we get into ERM for at least two hours.”* Members said that the risk management process also enabled the board to determine the quality of management. *“Every part of the business presents to the board, which helps us understand the operational and financial risks and lets the second tier of management show off.”*

Management’s role: running the process

Most members say risk in their company is devolved to line management. One member commented, *“The CEO is the ultimate chief risk officer,”* but while *“the CEO knows all the risks, they have to be put out there in a way that the board can react to. If it’s keeping the CEO awake at night, [the audit committee chair] may as well be awake, too.”* Some companies delegate risk management to chief risk officers. Financial services institutions, which are highly regulated, and companies with large financial divisions were more likely to have a chief risk officer.

Whatever framework or process emerges to identify and manage risk, it needs to become embedded within the company’s culture, and there must be a group to manage the risk process across business areas. *“The risks can be mapped to management, to ensure responsibility is assigned for each risk.”* Several members recommended use of a special risk committee with company-wide jurisdiction, which would *“[tap] the diverse experiences of management ... and [offer] comfort that the majority of risks will be surfaced.”*

Most members agreed that internal audit also has a role to play in risk management, particularly in assessing the risk management process, and that it should have a seat on the committee that deals with risk management. One member commented, *“Internal audit is inevitably involved. Risk management comes at so many levels.”* Another company relies on the head of internal audit to educate the board on the risk plan. Eager for help assessing their risk management process, members are looking for *“an independent view of the job our people did – did we get everything? Have we missed anything?”*

Risk disclosure: balancing transparency for investors with protection for directors

The SEC is advocating increased transparency in corporate disclosures and has called for more thorough management discussion and analysis (MD&A) sections in corporate filings. SEC Commissioner Cynthia Glassman said, *“The purpose of MD&A is to provide a sense of the quality of a company’s earnings and cash flow. To do that, companies must understand risks to performance going forward and an ERM process is a way to do that.”*⁴ Regardless of whether the audit committee takes on responsibility for risk management, it must nevertheless sign off on the itemized list of business risks included in the both the 10-K and the 10-Q.

One member pointed out, *“The audit committee is required to look at the MD&A because we review the [10-K and] 10Q before it’s filed; we can’t avoid that responsibility.”* This member stressed that, given the seriousness of disclosures, if an audit committee member is not reading the MD&A, *“you need to make sure*

⁴ Joanne Sammer, “Pressure Grows to Disclose ERM Information in MD&A,” *Compliance Week*, January 2005, 6.



they are, or kick them off the committee.” Another member said the list of risks should be “reasonable and indicate the risks to the business.” In his company’s MD&A, directors ensure that the risks listed include “things that could cause important financial effects” if they occurred.

Members said they clean up the MD&A list of risks regularly. *“We look at what’s on the list, what’s still serious. We don’t call out per se the top five risks that emerged from the strategic planning process, but they’re on the list.”* Another member stressed, *“We need to be sure the risks listed [in the MD&A] are the most meaningful and have emerged from a thoughtful process, not just 10-K boilerplate.”*

Committees wrestle with which way to err. Disclosing too little may leave investors in the dark. Disclosing too much, out of concern over legal action for omitting a risk, means *“disclosure hype has taken ‘annuals’ that used to have meaning and express[ed] management’s feel for the business to where everyone writes their annual to avoid being sued.”* Another member said, *“It’s not so much about informing the investor; it’s about protecting ourselves, so we can say, ‘Yes, but we told you that could happen’ – but at some point, listing too many risks obscures the true risks.”*

Conclusion

Network members acknowledge the additional workload that ERM responsibilities add to an already burdensome audit committee agenda. However, they approach ERM from a highly strategic perspective. Indeed, members’ main concern appears to be finding the best logical home for ERM efforts, be it the audit committee, the full board, or some other committee, such as governance or a special risk committee. The ultimate objectives appear to be a thoughtful and thorough assessment of the risks facing the organization, to ensure that responsibility for overseeing risk mitigation is clearly assigned, and to disclose risks using judgment and reasonableness.

About this document

The Southeast Audit Committee Network (SEACN) is a group of audit committee chairs drawn from leading companies based in the Southeast 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.

The ultimate value of *VantagePoint* lies in its power to help all constituencies develop their own informed points of view on important issues. Anyone who receives this publication may share it with those in their own network. The more board directors, 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 Southeast 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.