



Enterprise risk management and the audit committee

About this document

The Pacific Southwest Audit Committee Network (ACN) is a group of audit committee chairs drawn from leading companies based in the Pacific Southwest 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 new audit environment.

VantagePoint is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, 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 this document may share it 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.

Introduction

The Pacific Southwest Audit Committee Network held its second meeting on December 8, 2005. Discussion focused on enterprise risk management and the role of the audit committee. This document is a synthesis of insights from that meeting.

Members of the Pacific Southwest Audit Committee Network attending the meeting collectively sit on the boards of 12 large-, mid-, and small-cap public companies. Members attending included:

- Tony Anderson, Pacific Southwest Area Managing Partner, Ernst & Young
- Frank Biondi, Audit Committee Chair, Amgen
- David Engelman, Audit Committee Chair, Fleetwood Enterprises
- George Farinsky, Audit Committee Chair, Broadcom Corporation
- Martin Melone, Audit Committee Chair, Countrywide Financial Corporation
- Warren Pinckert, Audit Committee Chair, Pacificare Health Systems
- Bruce Stump, Pacific Southwest Area 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

A number of factors have combined to bring the topic of risk management to the fore: Hurricanes Katrina and Rita most recently; 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 and of how the companies identify, prioritize, and mitigate risk.

Enterprise risk management (ERM) is 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.

At the December 8 meeting, members of the Pacific Southwest ACN discussed a range of practices and shared insights, summarized below. Additional information appears on the pages indicated.

- **Identifying and prioritizing risk is still a difficult process for many companies** (*page 3*)

Companies use a variety of processes, such as formal frameworks (e.g., COSO¹) or the strategic planning process, to surface enterprise risks. Some members were concerned that strategic planning might not identify daily operating risks. Organizations can also learn from extreme events, such as Hurricanes Katrina and Rita, to identify risks to their company, even when the events do not affect them.

- **Management and oversight of risk vary by company and are often determined by the nature of industry regulation** (*page 5*)

Regulated companies are more likely to have a chief risk or compliance officer, and to establish risk committees both within management and on the board. In non-regulated companies, particularly those with smaller boards, the full board often handles risk oversight. Audit committees typically retain oversight of financial risk, but may take on other risk areas depending, in part, on the experience within the committee. Members in non-regulated industries were curious to explore whether certain practices of regulated industries, such as the more common presence of a chief risk officer (CRO), were transferable. Members cautioned against serving on the board of a company whose CEO did not support the risk management effort.

- **Disclosing risk must balance authenticity with concerns over liability** (*page 6*)

Some members said that the list of risks in the MD&A section of their public securities filings is heavily lawyer driven in order to protect the company from frivolous lawsuits. Risks disclosed often include those prioritized in the ERM process, but these may be embedded in a longer list of all possible risks. Other members are making a strenuous effort to ensure that the MD&A is more authentic and discloses only priority risks carefully vetted by top management, directors, and the external auditor.

¹ The COSO framework on enterprise risk management was established in September 2004 by the Committee of Sponsoring Organizations of the Treadway Commission. See Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrated Framework: Executive Summary*, September 2004. Available for download at http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf.



Identifying and prioritizing risk is still a difficult process for many companies

Many members voiced concern over whether they have identified the “right” risks. Sources of risk identified in discussions with numerous audit committee chairs include affirmative action, antitrust laws, compliance with contractual obligations, currency volatility, derivatives, disaster recovery, environmental issues, global operations, health and safety, information security, intellectual property, joint ventures, market timing, the reliability of internal and outsourced systems and processes, and tax risk.

Discussions with audit committee chairs in a number of networks as well as recent business literature suggest that companies, boards, and audit committees rely to different degrees on a combination of tools, frameworks, and a robust strategic planning process to surface risks:

- The **COSO framework** defines enterprise risk management as “a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”²

One member’s firm used COSO along with cross-company committees to identify 4,000 risks, albeit “*many could be two sides of the same risk, and we need to clean them up and prioritize the big ones.*” The process, while exhaustively identifying risks, was not prioritizing them in a way that was meaningful for the audit committee. “*COSO fits all my 4,000 [risks] – but now the audit committee is worrying [about] how to prioritize [them].*”

- Another approach views “**strategic planning** as the engine of the enterprise”³ and uses scenario planning to produce “a set of strategies ... across a broad range of plausible future[s]. The strategic plan becomes the baseline for identifying the most critical risks to the enterprise ... [Management] then disaggregate[s] those risks, assigns responsibility to individual managers for managing them, and also map[s] them to the board and its committees for oversight and governance responsibility.”⁴

A member described the process thus: “*Management identifies the risks to accomplishing the strategic plan and dovetails those with the risk factors listed at the back of public filings. We involve the broader board ... in order to have wider experience, view[s], and expertise. Then we begin to ... deal with the question of how to mitigate the risks.*” Another member felt the strategic plan “*lays the groundwork to understand the business, its strategic drivers, and where there are risks you wouldn’t achieve plan. Then it’s easier to get to the top 10 risks.*” One member, however, wondered “*whether daily operating risks would have trouble bubbling up to the strategic plan.*”

- An emerging comprehensive approach has also been proposed by the Open Compliance and Ethics Group (OCEG).⁵ The **OCEG framework**, which is still being finalized and is relatively unfamiliar to members, aims to “integrate governance, compliance, risk management and integrity into the tangible

² Ibid., 2.

³ James E. Copeland, Jr., “Leveraging information resources and processes to enhance director effectiveness” (presentation, University of Texas, Dallas, TX, October 6, 2005).

⁴ Ibid.

⁵ The Open Compliance and Ethics Group’s framework can be found at www.oceg.org/framework.asp.



practice of everyday business” to provide what it says has been missing: “a structured approach, common language and objective best practice model that organizations of all shapes and sizes could use.”⁶

While each company has its own particular set of risks, members described a “*top strategic risk we all face: [securing] talent. How do you recruit the best people in the world? There aren’t enough.*” A less obvious risk an audit committee might watch for is what a member called “*hubris risk.*” At one company, hubris risk meant that management’s faith in its superior manufacturing ability prevented it from creating a backup plan – until a secondary risk occurred and put operations on hold; a new plant, launched immediately, would take 24 months to come online. Another form of hubris risk is “*M&A hubris – the ‘I and my team can make this [deal] work’ attitude, which puts the board in [an] awkward situation [vis-à-vis] management.*”

Extreme events help companies identify new risks

Events that force analysis of risks can be of the common or extreme variety. “*Financial analysis of any new product, a capital expenditure, an acquisition – they’re one of the few places where we get focused. We’re not just looking at IRR, but at the risks – catastrophic, force majeure – [which become] apparent, and we go back and look to see how wide/deep those risks are.*”

Examining extreme events, such as Hurricanes Katrina and Rita, also spurs organizations to identify risks, even when those events don’t directly affect them. As companies start to build an enterprise risk management process, the first thing they often do is create a detailed disaster recovery plan, because as one member put it, “*If there’s an earthquake or a fire, we’d be out of business.*”

Members see great value in preparing for catastrophic events – whether terrorist attacks or hurricanes or earthquakes – that so far they have been fortunate enough to avoid. “*Get out the list of risks, dust ‘em off, and see what we need to change based on new knowledge from our or others’ recent experiences.*” On the other hand, ameliorating a bad situation may not be the wisest tack, as one member wryly pointed out: “*We’ve made a bet [a natural disaster] wouldn’t happen, but if it did, we’d evacuate, and we have insured the hell out of it. So now we’re better at managing a bad situation, [but] maybe we should look to get out of that bad situation!*” and weigh the pros and cons of vacating a disaster-prone location.

Prioritizing risk

Once the corporation has developed a comprehensive understanding of its material business risks, it must classify those risks and determine their relative priority. Most frameworks prioritize risks according to three attributes: (1) the probability of the risk’s occurring, (2) the potential frequency with which it may occur, and (3) the likely severity of its impact on the corporation. One member added a fourth: “*how close [the risks] are to making a material change in financial statements.*”

Despite the recent popularity of developing a “top 10” priority list of risks facing the company, many audit committee chairs remain unfamiliar with the key risks facing their business. One member suggested that might be because “*what the top risks are may have to be measured in context: ‘depending on what?’*” One audit chair wished he had more insight into “*what keeps the CEO up at night.*” Another member

⁶Open Compliance and Ethics Group, <http://www.oceg.org/about.asp>.



“identifies the ‘single point of failure’ that’s a material risk to the business and could take [the company] down,” and another suggested probing occurrences that could lead to reputational risk, which might be summed up as “the fear of appearing on the front page of the Washington Post.”

Management and oversight of risk vary by company and are often determined by the nature of industry regulation

When the Audit Committee Leadership Network in North America discussed enterprise risk management, *ViewPoints* reported, “There is a strong view that a comprehensive, enterprise-wide view of risk has to be both embraced and driven by the CEO. One audit chair was adamant: ‘You need a CEO who really believes in the process ... I would not serve on a board where the CEO was not committed.’”⁷ Members of the Pacific Southwest ACN agree: *“You’d better have [that support]; otherwise you’d better run from the board! If the CEO wants [risk] to be managed, it will be.”* Another member said, *“Our CEO is ‘chief ethics officer’ and has impact every day through tone at the top: do something wrong and you’re gone. Having that radiate down with the structures in place makes a difference.”*

Although members agreed about the importance of strong leadership at the top of the organization, they also noted the differences between the way companies in regulated and non-regulated industries manage risk. Highly regulated industries are more likely to spread risk management among specific committees, both at the management level and on the board, to focus on, for example, financial, credit, and operations risk. Regulated companies, particularly in financial services, often have a chief risk officer (CRO) as the executive responsible for taking the broad view of enterprise risks.

Perceiving regulated industries’ risk management efforts as *“more sophisticated,”* a member asked, *“Can the CRO model work in other environments? If so, what kind of person do you get for that role, from where?”* While one member questioned whether CROs really have a seat at the table to create change or if events create the change, a member offered the example of a CRO’s power, for instance, to shut down a bank’s trading floor if a situation so warranted.

Other members were concerned that managing and mitigating risk should not just be a case of *“insure it if you can’t get rid of it.”* In one company, *“risk management equals a senior vice president doing insurance management.”* It was unclear to that member how such an approach fits into the ERM process. Another member observed, *“The composition of your management group is key to realizing the fruits [of], or paying penalty [for], [the risk management process]; we’re at [the] mercy of management no matter how good the audit committee is. Better to revisit the role of ERM in the corporation itself, rather than how we deal with it at the audit committee.”*

Another member commented on the situation in many non-regulated companies: *“Highly regulated companies can justify heavy in-house risk management personnel and have board committees to handle them. Other companies [don’t have the resources and] don’t want to add committees, so they say ‘let the audit committee do it’ – it’s like we’re a receptacle at the bottom of a funnel.”* Many members held the

⁷ Audit Committee Leadership Network, “Enterprise Risk Management and the audit committee,” *ViewPoints*, December 22, 2003, 6. Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_Dec03_View3.pdf.



view that ERM should be the responsibility of the entire board to oversee. One member stated, *“You can’t delegate it, but the audit committee can offer an advisory role.”*

Audit committee composition influences the committee’s role

Whether the audit committee takes on the oversight of risk depends on the industry, situation, time, and the ability of the audit committee to look at it. It may also depend in part on the composition of the audit committee. *“While it would be nice to have an expert for each risk, the best proxy is a former CEO who has that mentality, and then you have to know to go outside for expertise as needed.”* Since Sarbanes-Oxley, change is gradually occurring in boards and audit committees: *“As members retire, governance committees may be looking for certain expertise in replacing them, knowing what they need.”*

The level of experience required of audit committee members varies from business to business, but one member suggested trying to assemble a cross section of people who could line up with the serious risks to the business – people who have been in management, such as a CIO or an executive from another function, and ex-attorneys or law partners. *“But you can never cover all the disciplines,”* a member stated. *“If you’re smart and broad ... you can call on experts, versus trying to gather specific areas of expertise [into one committee]. You have to know if you need more information, and where to go to get it.”*

Disclosing risk must balance authenticity with concerns over liability

For many companies, the MD&A section of their public securities filings has developed into a long, difficult document, *“sometimes longer than the financial statements,”* as one member lamented. Members generally deal with the arduous process of reviewing risks for inclusion in the MD&A in one of two ways:

- **Focus on authentic risks.** Some audit committees take a stringent approach to determining what will be on the list of risks in documents such as the 10-Q and 10-K. *“We make sure major risks we’ve identified are among the risks factors we list. We hold a formal meeting that includes our external auditor, directors, and top management, go through all the risk factors, and may add/eliminate [and] informally communicate to move the order.”* Another member also favored a more authentic approach to the MD&A: *“We review everything in the MD&A, and maybe we need to push back on management more if we feel there’s an issue.”*
- **Focus on liability concerns.** Other members say the list of risks in the MD&A is heavily lawyer driven in order to protect the company from frivolous lawsuits. *“You have to mention everything you can think of, and then some.”* The risks disclosed often include the company’s priority list of risks as generated by the ERM process, but these may be embedded in a longer list of all possible risks. Members agreed that lawyers always have the final call: *“The truth is, we all hire lawyers to protect us.”*

Members hope that eventually the process of disclosing risks, rather than being primarily a way of protecting companies from liability, will convey real risk in meaningful ways that investors can more readily understand. One member commented, *“As we develop in the ERM area, some interesting things may fall out of it; maybe [disclosure] will get more real. Idealistically, we’d be able to say, ‘We’ve discovered it, here it is, we’re dealing with it,’ but that’s a long way off.”*



Conclusion

As do members of similar networks of audit committee chairs serving companies in other regions of the United States,⁸ participants in the second meeting of the Pacific Southwest Audit Committee Network use a mix of formal risk frameworks, primarily COSO, and strategic planning to identify and manage risks, as well as approaches grounded in experience and instinct. Many companies are only recently coming to ERM, as Section 404 implementation has diminished somewhat as a key item on the audit committee's agenda. Revisiting the subject of enterprise risk management in a year's time will likely show that companies have learned a great deal more about what to do and when, and that they have achieved greater sophistication in all aspects of risk identification, prioritization, management, mitigation, and disclosure.

The views expressed in this document represent those of the Pacific Southwest 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.

⁸ *VantagePoint* issues covering discussions of the Southeast, Mid-Atlantic, and North Central Audit Committee Networks on this topic are available at http://www.tapestrynetworks.com/net_audit.html.