



A deeper dive into risk management practices

Introduction

The Pacific Southwest Audit Committee Network (PSWACN) held its 14th meeting on October 14, 2009, in Santa Monica, CA. Network members, who sit on the boards of more than 25 large-, mid-, and small-cap companies between them, used the meeting for a deeper dive into current risk management practices. This document reflects a summary of the key points raised during the meeting, along with selected perspectives that members shared before and after the meeting.¹ For a full list of participants, see Appendix 1 on page 10.

In a recent survey sponsored by Ernst & Young, the Economist Intelligence Unit found that the average Fortune 500 company spends about 4% of its revenues on risk management activities, yet 96% believe their risk management programs could be improved.² Furthermore, risk is on the rise: 52% of executives said financial risks have increased over the last 12 months, with 42% seeing increases in strategic risk, 40% seeing increases in compliance risks and 39% seeing increases in operational risks.³ Given that *“there is no bible for any of this,”* members recognized the practical value of sharing, in a confidential setting, risk management approaches from the companies on whose boards they sit.

Executive summary

In order to fulfill their risk oversight responsibilities, members agreed it was important for directors to understand and benchmark specific risk management techniques across a broad range of companies and situations. Members shared examples of effective practices, in a spirit of appreciative inquiry. The discussion covered four broad areas:

- **Designing an effective enterprise risk management (ERM) process** (Page 2)

Audit committee chairs reported that even the basic step of defining risk appetite is difficult, and they cautioned against becoming too risk averse in the current economy. Meeting participants noted a diversity of approaches to the design of risk management processes at the organizational level. Some companies assign risk management responsibility to an individual, oftentimes the chief risk officer (CRO). Others have formed a management committee to drive risk management efforts. Network members shared experiences of using external advisers, concluding that such advisers can offer useful tools and frameworks to support initial risk management design.

¹ *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. Quotes in italics are drawn directly from comments made by PSWACN members during and after the October 14 meeting.

² Ernst & Young, *The future of risk: Protecting and enabling performance* (Ernst & Young Global Limited, 2009), 1. Available at [http://www.ey.com/Publication/vwLUAssets/The_future_of_risk/\\$FILE/The%20future%20of%20risk.pdf](http://www.ey.com/Publication/vwLUAssets/The_future_of_risk/$FILE/The%20future%20of%20risk.pdf).

³ *Ibid.*, 2.



- **Identifying and prioritizing current and future risks** (Page 4)

Members agreed that an effective risk management program should ultimately strive to identify and assess those risks that could “*crater the enterprise.*” Processes that members highlighted for identifying those key risks include building on the risks listed in the 10-K, reviewing the risks inherent in balance sheet line items, surveying executives across business units, brainstorming risks that emerge from the strategic planning process, and forming committees deep inside the company to identify and prioritize risk. Members acknowledged that “*the past year-and-a-half has changed the risk landscape a great deal,*” and noted that boards are now focusing much more attention on catastrophic, “long-tail” events, new and emerging risks, and risks that could ultimately threaten the relevancy of the business model.

- **Mitigating and reporting risks** (Page 6)

Meeting participants agreed that identifying risks is much easier than mitigating them. While a solid balance sheet is often the best form of risk mitigation, this comes at a significant opportunity cost. Members identified other mitigation practices, including developing techniques to avoid single points of failure, scrutinizing counterparties more closely, establishing a disaster recovery plan, and tailoring programs to mitigate specific risks. While many risks cannot be easily quantified, almost all members said that their companies use some form of heat chart or probability/impact matrix to track and report on key risks. Meeting participants agreed that the reporting process must be dynamic and that companies must not adopt a “*check-the-box*” mentality.

- **Ensuring effective oversight of risk management** (Page 8)

While members agree that “*there’s no ducking the fact that risk truly is a board oversight responsibility,*” many believe the audit committee can play an important support role. While few members believe a board risk committee is necessary, one member said such a committee could provide focus while the risk management program was being developed. This member described a model for migrating responsibility from the risk committee to the full board according to a set timetable. Participants agreed that corporate culture is a critical piece of the risk management program and noted that one can evaluate a company’s risk culture by the frequency of risk discussions outside formal risk management presentations.

For selected questions audit committee members and other board directors might ask themselves about enterprise risk, see Appendix 2 on page 11.

Designing an effective enterprise risk management (ERM) process

When executives in the Ernst & Young survey cited earlier were asked where they plan to commit more resources to strengthen their risk management capabilities, 85% said they intended to improve the alignment of their risk management approach with their business strategy, and 72% intended to redefine risk ownership roles, processes, and structure.⁴ PSWACN members observed that understanding the organization’s risk appetite is a fundamental step in aligning the risk management approach with business strategy, and yet this

⁴ Ibid., 9.



first step is a difficult one. As for risk ownership, members noted two trends in assigning risk responsibility on the organizational level.

Defining risk appetite continues to be a challenge

According to the Committee of Sponsoring Organizations of the Treadway Commission (COSO), “Enterprise risk management is 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.”⁵

While this definition is helpful, members agree that it is difficult to define an optimal level of risk. One said, *“I’d say the consensus on my boards is that there’s not a static definition of risk, nor is there a static management system for risk. In some respects, I think we’ve almost tried to stay away from defining it. Risks that are ‘bet-the-company’ in one environment might not be the case in another.”* Another member added, *“Risk appetite has changed over the past 18 months. It’s more conservative for now, but it’s an evolving and moving target.”*

Given the changeable nature of risk, members agreed that directors must not be *“too risk averse,”* since companies need to take some reasonable amount of risk to make money: *“It’s the board’s job to manage with a steady hand, and although it can be our tendency to overreact and be risk averse, we need to make sure we’re not avoiding risks altogether.”* Moreover, as one member pointed out, *“a critical component to mention is that on the opposite side of the biggest risk is the biggest opportunity. We need to see the risks with eyes wide open rather than closed.”*

Two dominant approaches exist for risk management at the operational level

A member remarked, *“The board needs to make sure management is taking ownership for risk and that they’re not just hearing about risk when it’s being discussed in an annual [risk] report.”* When members described their companies’ risk management organizations, two primary approaches emerged:

- **Assign risk management to a management committee.** *“The committee is made up of the CEO’s direct reports. When the company first initiated the [risk management] process, we engaged [a third party] to walk them through how to design the process and to help map out risk. We went through and identified the top risks and their likelihood and assigned each risk to an owner. Since we started, there have been quite a few ‘a-ha’ moments, with lots of places to dig in further. We do not present the whole risk report to the full board, just the top 12 [risks].”*
- **Assign risk management to an individual executive.** Some companies advocate an internal “quarterback” who takes responsibility for operationalizing risk processes. For many companies, this individual is the CRO in role if not in title: *“We made the head of internal audit the CRO, who is*

⁵ Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrated Framework: Executive Summary* (Committee of Sponsoring Organizations of the Treadway Commission, 2004), 2. Available at http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf.



responsible for managing risk. The board needed someone to own all of this. [The] internal audit [function] has a solid line to the audit committee and a dotted line to the CRO.”

Meeting participants agreed that regardless of the approach, the CEO’s support is essential: *“The CEO needs to own the process and get behind it 100%.”*

External advisers can be useful in the early stages of risk management design

Almost all members agreed that third parties can help with the initial risk management framework: *“We used an [independent audit firm] to do a survey of our risk management function. They also brought a process that informed if we needed a risk committee. Depending on the company, there’s always going to be a different view on risk and how you approach it.”* Another member said, *“We put ERM under a senior officer, and they oversee a committee of internal folks. Initially, they went out and got two law firms who helped guide them through their first pass. It gives people a good template.”*

Identifying and prioritizing current and future risks

Members agreed that the first steps in any risk management process are to identify and prioritize the most significant risks to the business. Still, this continues to be an issue companies struggle with: in the Ernst & Young survey, 84% of executives said they are investing in risk assessment to provide a comprehensive view of risk and better enable the anticipation of risks.⁶

Useful identification processes

Most companies are exposed to hundreds if not thousands of specific risks: compliance, financial, operational, competitive, strategic, and reputational. However, as a practical matter, senior management must focus on a smaller number of significant enterprise-wide risk areas. To help with the identification process, members agree that they first need to define which risks they will be assessing: *“We focus on risks that could crater the enterprise, not all risks in the enterprise.”* Another said their risk management efforts are designed to identify *“any risks that can deliver a body blow.”*

Pre-meeting conversations and discussion at the meeting itself revealed a number of processes for identifying those key risks:

- **Start with the 10-K.** *“We have an official statement of risks in the 10-K, so we use that as a template.”*
- **Review the balance sheet.** *“We go through the balance sheet every year and identify the risks inherent in each account.”*
- **Survey business unit leaders.** *“Each business head is responsible for identifying major risks in their business, and those are then reviewed by the CFO and presented to the board. It’s always the business units that [identify risks] initially. Lots of [risks] filter up across the company that way that the board might not have come up with [on their own].”*

⁶ Ibid.



- **Brainstorm during the strategic planning session.** *“We dedicate several hours at the [annual] strategic planning session to brainstorming areas of risk. Management has done a good job preparing material in advance ... The goal is to ask, ‘What are we doing to identify risk? Do we have people who are responsible for those risks?’”*
- **Form committees for risk identification.** *“Management formed several committees focused on identifying emerging risks. These committees, which go pretty far down in the organization, hold [periodic] brainstorming sessions to bubble up issues to senior management.”*

Polling a wide group of senior managers on those risks they see as most important and contrasting them with the risks identified by the board serves as a good feedback loop for gauging the effectiveness of the ERM process. One network member who implemented such an approach agreed that the broader base of insight is helpful but pointed out the importance of following up on the results: *“We did a poll [of the company], but we never saw the report back on how closely aligned [the board’s view of risk] was with [that of] management.”*

Prioritizing and assessing risks in a new environment

Network members agreed that prioritizing risks is at least as important as identifying them in the first place. While they recognize that companies face a multitude of risks, members highlighted two categories of risk that demand more focused attention:

- **Catastrophic, long-tail events.** *“We need to acknowledge that the financial crisis has caused a sea change. We’re now all thinking about catastrophic risk. If you go back to August 2008, we wouldn’t be talking about [catastrophic events], but now there is this new acknowledgement that big, bad things can happen.”* One member offered an extreme example: *“What if a bomb goes off and kills your entire board and management? What would you do?”* Another member said in response, *“We used to have a laminated card of the next pecking order [of executives]. Those kinds of conversations don’t happen often, but they do raise your antennae about catastrophic scenarios.”* A third observed, *“This discussion on the long-tail, improbable events [is important]. There are things we can do at low cost to mitigate some of them.”*
- **Emerging risks.** Members were concerned about the dynamic nature of risk, particularly risk that impacts a company’s fundamental business model. *“The key challenge today is identifying the new and emerging risks. You can start with the 10-K to get the old risks, but the new and emerging [ones] are the most difficult to get your arms around. Focusing on those is the most challenging, but also the most critical.”* Another member pointed out, *“The hardest risks to see are the ones that develop over time. They creep up on you.”* As an illustration, one member shared an anecdote about a senior executive’s behavior driving away talent to a competitor. Over time, the company was forced to make an acquisition to regain strategic capabilities it had lost.

Members also noted that risks unfold at different rates: *“[Assessing] the timing of risks is important – what could kill us today versus what could hurt us in 20 years. How much is near term versus emerging?”* A near-term risk could potentially include a shifting management dynamic: *“Any time you get a new CEO in*



place, it's important to understand the team dynamics. The quality of executive management is one of the greatest business risks out there.”

Members point out that longer-term risks, such as demographic shifts and the use of technology, often cut to the essence of the business model: “The biggest [long-term] risk for us is the relevancy of the business.” Added another member, “We’re not worried about how to grow, we’re worried about what’s going to jeopardize the enterprise down the road. Our problem could be our business model.” Ultimately, most members agreed with the audit committee chair who said, “You have to make sure you’re always looking at both [immediate and long-term] risks.”

Risks that typically require board attention

One member summarized the risks that members highlighted during the meeting. This list of board-level risks included:

- Single points of failure (e.g., supply chain rests on one vendor, production dependent on one factory)
- Major catastrophes (e.g., a dirty bomb in Manhattan)
- Loss of management team and/or board
- Emerging trends that pose a threat to the business model (e.g., technology changes)
- Strategic planning risk (i.e., decisions you do and do not make)
- Significant operating risk
- Loss of reputation
- Loss of liquidity

Mitigating and reporting risks

One member observed prior to the meeting that the “timing [of mitigation] is crucial. It’s not clear what to do when you know you have some exposure. If [things are] going well, it’s hard to significantly change policies on the gamble that something bad is going to happen.”

Indeed, risk mitigation is arguably the most difficult aspect of any risk management program. The risk framework developed by the Committee of Sponsoring Organizations of the Treadway Commission articulates three components of risk mitigation and reporting:

- Risk response – avoiding, accepting, reducing, or sharing risk and developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.
- Control activities – policies and procedures that are established and implemented to help ensure the risk responses are effectively carried out.



- Information and communication – the identification and capture of relevant information in a form and time frame that enable people to carry out their responsibilities.⁷

Mitigation tactics

Some risks can be mitigated through insurance or self-insurance; however, many important risks (market, competitive, technology, strategic) are uninsurable. Members agreed that protecting and reinforcing the balance sheet is the most important and effective mitigation tactic: *“There’s no process that’s bulletproof, but a fortress balance sheet certainly helps.”* Other mitigation approaches members mentioned include:

- **Avoiding single points of failure.** Many companies have vulnerabilities that result from sole manufacturing or sourcing arrangements. In some cases, these risks can be mitigated with additional supply or production capacity. However, where redundancy is impossible or financially unattractive, management may need to pursue other mitigation strategies (e.g., increasing buffer stock).
- **Scrutinizing counterparties more closely.** One member said, *“We asked [management to] go through and identify their significant counterparties ... They did that exercise begrudgingly, and probably thought, ‘Ohhh, here’s another thing the audit committee wants.’ They hadn’t really thought about it until they went through the systematic approach – it had been very much ad hoc before. As a result of that process, we’ve had a very eye-opening experience. They identified some serious vendor risk. They developed some good back-up plans as a result.”*
- **Establishing a disaster recovery plan.** *“I have always championed a disaster recovery plan. These [recessions and traumatic events] have been going on for decades. We need to think about the fourth standard deviation from the norm.”*
- **Learning from historical lessons.** *“We don’t spend enough time looking in the rearview mirror. [There are] a lot of old lessons we should have been looking at relative to our industries.”*
- **Creating programs tailored to mitigate specific risks.** In a pre-meeting conversation, one member said, *“[Management] concluded that product quality and returns was an issue that was not being adequately addressed, so they developed a risk mitigation program.”*

An emerging consistency in risk management reporting

Several members noted that *“reporting on risk management is much more qualitative than quantitative,”* and one said, *“You [can] get yourself very rapidly into a statistical probability exercise that turns into ‘how many angels can dance on the head of a pin?’ You can over-engineer this thing so badly, and that’s one of my greatest concerns about this. Don’t over-complicate it.”* For their part, almost all members shared that they use some form of either a *“heat chart”* or a *“matrix that highlights the probability and impact of all primary risks.”*

⁷ Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrated Framework: Executive Summary*, 4.



Regardless of what type of reporting process they use, members agree that it needs to be dynamic. One member said, *“We have little arrows next to each mapped risk, moving left or right to indicate how each one is [changing].”* Meeting participants stressed that establishing an effective reporting system is not a onetime goal that can be achieved and checked off; it is an ongoing process that requires continuous review and revision: *“When you get a matrix in place, it’s easy to think you have it covered. It’s incumbent on directors to make sure you keep that list fresh. Don’t just check the risks on the current list and move on.”* Moreover, *“You need to make sure the list you have is the right list. You could leave one risk off, and it would be catastrophic. You need to have a rigorous kicking around of this issue – the risk of omission is a big one.”*

Ensuring effective oversight of risk management

Participants acknowledged that boards continue to debate where responsibility for oversight of enterprise risk management should lie. Many agreed that the full board has the ultimate responsibility for ERM: *“At the end of the day, the buck stops [with all the directors]. You want the full board to be involved.”* Added another member, *“The full board needs to be responsible so you can have more people thinking about risk. There are a lot of great minds at work [on the board], and you need to structure [risk oversight] in a way that has the greatest chance of getting people thinking broadly and deeply.”*

While members agreed that the full board has the ultimate responsibility for risk, participants pointed out that the audit committee can still play an important role in ensuring that risk management processes are developed: *“The audit committee is responsible [under Sarbanes-Oxley] for reinforcing the process and making sure the company has done the job.”*

Although few members said their companies planned to create a permanent board-level risk committee, one member described a recent decision to establish a temporary risk committee while the risk management framework is developed and refined. After three years, the risk committee’s responsibilities will be migrated to the full board and the risk committee will be disbanded.

In the Ernst & Young survey cited earlier, 61% of executives said their companies needed to commit more resources to promoting a “risk culture” – a company culture that recognizes the importance of managing risk.⁸ Members agreed that one of the board’s oversight responsibilities should be to encourage a positive attitude toward risk management. Members described a simple way for directors to gauge the degree to which risk is embedded in the corporate culture: *“The real test is whether risk comes up when business proposals are being done. That’s the real proof in the pudding that your risk management process is working.”*

⁸ Ernst & Young, *The future of risk: Protecting and enabling performance*, 9.



Conclusion

Members agreed that ERM is an evolutionary process and that companies will undoubtedly go through multiple iterations. As ERM evolves, members are committed to making sure risk-related issues stay at the top of the board agenda. One said, *“I’m going to continue to press for this discerning and candid type of discussion at the board level.”* Moreover, members reiterated the importance of seizing the opportunities that will emerge from the financial crisis: *“I fear the events of the past couple of years will make companies overly conservative, but that is bad for the economy overall. We need to remember, ‘nothing ventured, nothing gained.’”*

About this document

The Pacific Southwest Audit Committee Network is a select group of audit committee chairs from leading companies committed to improving the performance of audit committees and enhancing trust in financial markets. 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 committee 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 *VantagePoint* 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.

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 US 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.



Appendix 1: Participants at the network meeting

The members of the network who participated in the meeting were:

- Frank Biondi, Audit Committee Chair, Amgen
- Henry DeNero, Audit Committee Chair, Western Digital
- Ray Dittamore, Audit Committee Chair, Life Technologies
- David Engelman, Audit Committee Member, Fleetwood Enterprises
- Lou Lavigne, Audit Committee Chair, BMC Software
- Roger Molvar, Audit Committee Chair, CapitalSource Bank
- Stephen Page, Audit Committee Chair, Lowe's Companies
- Sue Redman, Audit Committee Chair, The Apollo Group
- Orin Smith, Audit Committee Chair, The Walt Disney Company
- Dean Yoost, Audit Committee Chair, Pacific Life

The following members took part in post-meeting discussions but were unable to attend the meeting:

- Richard Dahl, Audit Committee Chair, DineEquity
- Bala Iyer, Audit Committee Chair, IHS
- Marty Melone, Audit Committee Chair, Internet Brands
- Paul Unruh, Audit Committee Chair, Symantec

Ernst & Young partners participating in the meeting included:

- Mark Borowski, Pacific Southwest Sub-Area Assurance Managing Partner, Assurance Services
- Abdul Lakhani, Pacific Southwest Area Professional Practice Group Leader



Appendix 2: Selected questions audit committee members and other board directors might ask themselves about enterprise risk management

- ? How effective are the organizational and process components of your company's risk management programs?
- ? Does your leadership team support a company-wide emphasis on the importance of risk management? What mechanisms might executives adopt to ensure risk management is embedded in the corporate culture?
- ? Who (or what group) has been designated to lead the risk management activity? What prompted this choice? What supporting organization is required? How is the risk management group supported by the organizational culture and by the audit committee?
- ? What sources of external expertise does your company rely upon for risk management? What value do they bring?
- ? How is risk appetite defined at your company? Are the measures qualitative or quantitative?
- ? How does your approach to risk identification compare with those outlined above? How is your list of risks generated? What screening criteria are applied? Who participates in the identification process?
- ? What methodology is used to prioritize the list of potential risks? What quantitative and qualitative factors are taken into account?
- ? What unexpected results emerged from the risk identification and prioritization process?
- ? What tools does management use to mitigate material risks once they are identified?
- ? How does management report the status of the risk management effort? How frequently are these reports prepared? To whom are the reports distributed, and how are they used? How do companies ensure that risks are reported up through the organizational hierarchy without being filtered?
- ? How is the risk management framework used to support management decisions?
- ? How does the full board support the risk management activity?
- ? What is the nature of the risk management discussions between the board and management?
- ? Have you made any changes to the role and remit of any board committees?