



Leading risk management practices

On January 11, 2010, members of the Southeast Audit Committee Network (SEACN) convened in Atlanta for their 15th meeting. Network members, who sit on the boards of more than 25 large-, mid-, and small-cap companies between them, discussed leading risk management practices. Members were joined by Jim Traut, director of enterprise reputation and risk management at H. J. Heinz Company. Over dinner, members were also joined by Michael Smith, a partner at King & Spalding, to discuss director liability as it relates to risk management. This document summarizes the key points raised during the meeting, along with some additional perspectives that members shared before and after the meeting.¹ For a full list of participants, see Appendix 1, on page 11.

Executive summary

Members agreed that understanding and benchmarking specific risk management techniques across a broad range of companies and situations would help directors fulfill their risk oversight responsibilities. Members shared examples of effective practices in a spirit of appreciative inquiry. The discussion covered five broad areas:

- **Designing an effective enterprise risk management (ERM) process** (*Page 3*)

Meeting participants distinguished two primary approaches to the design of risk management processes. The first is a bottom-up approach, whereby risk management is embedded in the operations of the company. The second is a top-down approach, whereby risk management is initiated by executive management and the board through the strategic planning process. The strengths of the one are the weaknesses of the other: the bottom-up approach does not always fully integrate risk management with strategy, while the top-down approach often struggles to operationalize ERM in the company. Members differed on what constitutes an appropriate role for the internal audit function, with some questioning whether their internal auditors can overcome their reputation as policemen and others saying that internal audit plays an invaluable role as the key drivers of the process.

- **Identifying and prioritizing key risks** (*Page 5*)

Members agreed that an effective risk management program should identify and assess a comprehensive list of all significant risks. Ways of identifying them include building on the risks listed in the 10-K, brainstorming risks during the annual strategy off-site meeting, holding risk workshops, and conducting scenario planning. Members reported that more often than not, risk identification is *“much more qualitative than quantitative.”*

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. The meeting guests have given permission for their remarks to be attributed. Quotes in italics are drawn directly from comments made by SEACN members during and after the January 11 meeting. Mr. Traut’s remarks are not italicized.



▪ **Mitigation and reporting** (Page 7)

Meeting participants agreed that identifying risks is much easier than mitigating them. Members repeatedly emphasized that the most effective mitigation tactic is to ingrain risk management in the day-to-day functioning of the business. Beyond the standard heat chart and probability matrix, members expressed discontent with the fact that it often feels like they are being “*reported to death.*” Members pointed out that the audit committee can play a role in making sure these reports are more helpful.

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

While all members agree that the ultimate responsibility for risk management oversight lies with the full board, a handful of members stated that they are still struggling to engage the full board. Regardless of the level of full board engagement, members acknowledge that detailed risk management oversight work is done in committees. From there, members described four different approaches to handling risk at the committee level: the audit committee drives the process and monitors risk; the audit committee monitors financial risks and allocates responsibility for other risks to the other committees; a stand-alone committee is formed to take on the primary risk related to the company’s business (such as a technology and quality committee spearheading the effort at a medical devices company); or a separate, stand-alone risk committee may be established to oversee risk. The last option was not a popular choice for non-financial businesses.

▪ **Evolution of risk management** (Page 10)

Meeting participants concluded their discussion by reflecting on the future of enterprise risk management. Members pointed out that risks do not occur sequentially and raised questions about the challenges of handling multiple, simultaneous risks. Members also highlighted the need for board directors to keep up with the risks and opportunities created by the rapid pace of change in technology.

Appendix 2, on page 12, includes a list of questions related to risk management practices for audit committees to consider.

Introduction

Recent studies have found risk management programs wanting. In a 2009 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 Another survey, also conducted in 2009, revealed that 85% of corporate executives believe an overhaul in risk management is required if the lessons of the economic crisis are to be used to improve business results.³

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.⁴ Given that “*there is no Holy Grail for any of this,*” members recognized the practical

² Ernst & Young, *The future of risk: Protecting and enabling performance* (Ernst & Young Global Limited, 2009), 1.

³ Accenture, *Managing Risk for High Performance in Extraordinary Times* (Accenture, 2009), 8.

⁴ Ernst & Young, *The future of risk: Protecting and enabling performance*, 2.



value of sharing, in a confidential setting, risk management approaches from the companies on whose boards they sit.

Designing an effective enterprise risk management (ERM) process

An effective risk management program involves understanding risk, assigning organizational responsibility, linking risk with strategy, and adopting processes to operationalize management. 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.⁵

Two primary risk management models

Companies take a number of approaches to assigning responsibility for risk management, including identifying a centralized risk leader, such as a CRO, creating a small senior risk team, establishing a management-level risk management committee, or alternatively, decentralizing risk responsibility to operating management. Two prominent models for driving the risk management process emerged during the January meeting discussion:

- **Bottom-up, operational approach.** Mr. Traut described H. J. Heinz Company’s decentralized approach to risk management design: “We initiated our process by doing a risk assessment with the functional area leads and ultimately ended up identifying our initial list of risks. We then assessed those risks, based on likelihood and impact, before doing a deep dive into the primary areas we identified – roughly five. We tried to think through from a policy and ways of working perspective how we could guide this process through the 25 different business units. I felt strongly that this should not be a [Sarbanes-Oxley]-like, compliance-heavy process. Instead, we focus on how functional leaders can drive the business from the ground up.” One member concurred: *“If you are going to get a risk management program to work, you have to get input from someone who has a great deal of operational experience and knows where all the bodies are buried.”*

One member whose company implements a similar approach pointed out that this can make it difficult to bridge the gap between operations and strategy: *“We do not get a lot of detailed reports at the audit committee level on the intricacies of the ERM process because most of it is done at operating levels. It was good that they were operationalizing it, but on the other hand, it’s not [providing] quite the same transparency at the audit committee level, where we’re discussing overall planning and strategy.”*

- **Top-down, strategic approach.** When this approach is implemented, oftentimes it is driven by a centralized risk leader. *“Risk management is all driven through [the CFO’s] office because it is all part of strategy. We work with all the business leaders to develop risk management from a market perspective, and we always make it part of the strategic planning discussion.”* Added another member,

⁵ *Ibid.*, 9.



“Our CFO headed up our ERM practice because he was already so familiar with the process and is able to more effectively make it part of everyone’s job responsibility. He might not have the title of CRO, but he performs that role.”

However, as one member pointed out, *“Sometimes focusing too much attention on your own culture and strategy can sow the seeds of your own demise. [At one company] we got so mechanized and were so busy thinking about how far we were out on the tail and trying to include it in the strategic planning, but it became too controlling. We had to back up, look at [our risk management process] separately, and then find a way to put it back in and operationalize it within the business.”*

Members point out that one approach’s strength is the other approach’s weakness: the bottom-up approach does not always fully integrate risk management with strategy, while the top-down approach often struggles to operationalize ERM in the company. Consequently, members were quick to agree with the member who said, *“I think every company has its own [approach], and you have to do what’s right for that company.”* One member warned against making risk management a perfunctory task: *“Risk cannot be a task where you just check the box and then it goes on a shelf. In order to make sure your company is addressing the biggest threats to the business, [risk management] needs to be a living, breathing part of the everyday strategy.”*

Differing views on how best to utilize internal audit

The discussion regarding the role of the internal audit function in the risk management process was the source of some disagreement amongst members.

- Many members, particularly those whose companies are still in the early stages of establishing an ERM process, reported that their internal audit function has played a key role: *“At my company, internal audit is viewed as very much part of the collaborative process. It’s not seen as a ‘gotcha’ function. We’re working together.”* One member had said prior to the meeting, *“I have total confidence in our internal auditor. Granted, [at my company] the head of internal audit is a broad-based business leader, not a career internal auditor, and I wouldn’t have it any other way. You need someone with that business sense.”*
- Other members differed. One member remarked, *“For what it’s worth, I think having ERM in internal audit is the worst possible thing that you can do ... Internal audit is [often] viewed as these people that run around and try to find something that you’re doing wrong. That does not create the kind of environment that you want.”* Some members also questioned the extent of internal audit’s involvement, given their other responsibilities: *“I think sometimes you can stretch [a role] too much ... I, for one, would hate to see the basic responsibilities of internal audit diluted by giving them too much.”*

Seeking external advice

Several members reported that external third parties can be a helpful guide during the initial development of a risk framework and processes: *“We brought in an [independent audit firm] to help formulate our process*



and coordinate meetings and documentation. It's important to have a defined process and [to make] sure that you're following through on what's identified, and they were very helpful in that effort."

Prior to the meeting, one member shared that external advisers have been useful in pointing out areas of weakness in risk management processes: "We had someone come in and walk us through our strategic plan and challenge us and make sure we'd thought of everything. Doing that dry run to see if we thought of everything and providing a new perspective to test the plan was really beneficial for us."

Mr. Traut emphasized to members that regardless of who is driving and contributing to the process, "The one word I would use that is critical to ERM is *communication*. [As a driver of risk management], I can only be effective if there is total transparency and everyone is trying to get things out on the table."

Identifying and prioritizing key risks

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines risk assessment as "the identification and analysis of risks to the achievement of business objectives. It forms a basis for determining how risks should be managed."⁶ Identification and prioritization of risks is often one of the first areas in which companies focus their risk management efforts.

Yet the dynamic nature of risk means that even though many companies report benefiting from their efforts to identify and understand key risks (58% of the executives surveyed by Ernst & Young said their organization receives a high to very high benefit from this effort),⁷ there is always plenty of room for improvement (84% of respondents in the Ernst & Young survey say they will invest in improving their risk assessment, aiming for a more comprehensive view of risk and an enhanced ability to anticipate risks).⁸

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 high-impact, enterprise-wide risk areas.

Pre-meeting conversations and discussion at the meeting itself revealed a number of ways to identify those key risks:

- **Hold annual strategic deep-dive off-site meetings.** *"We identify risks as part of a risk strategy off-site that we have every year. We discuss all the different risks and how we're going to deal with them."*
- **Start with the 10-K.** *"We begin the process by looking at all the risk factors that have been identified in the 10-K and mak[ing] sure any of those that have been identified are being represented in our assessment."*
- **Implement risk workshops.** *"We now conduct risk workshops across all different business units across North America and Europe. It's an all-inclusive and really meaningful process to identify the key risks in*

⁶ Institute of Internal Auditors, "Applying COSO's Enterprise Risk Management – Integrated Framework," PowerPoint presentation, slide 33.

⁷ Ernst & Young, *The future of risk: Protecting and enabling performance*, 4.

⁸ *Ibid.*, 9.



the company. At each workshop, different representatives from the business units get in a group and come up with different risk scenarios and then draft a strategy to address [them].”

- **Conduct scenario planning.** *“The other side of identifying various disaster scenarios is talking about what the ripple effect of that disaster would be. How many of our business units would be impacted? It’s helpful to trace the production process to identify how many potential ways you can be impacted because often it’s the ripple effects you don’t think about.”*
- **Survey buy-side analysts.** *“We invited analysts to come in for conversations around risk. Also, when we presented updates to the annual plan and three-year plan, there was always a section operators addressed around risk, and we asked everyone to look ahead and consider potential risks.”*
- **Brainstorm with futurists.** Some members use external consultants, with one reporting *“bringing in futurists at the board level”* in an effort to brainstorm around potential longer-term risks. One member noted, *“Last year, at every board meeting we would have some expert come and make a presentation ... anyone to get us thinking.”*

Assessment and prioritization

Ultimately, members agreed that more often than not, risk identification is *“much more qualitative than quantitative.”* As a result, members point out that the prioritization of risks becomes more important. Still, as one SEACN member remarked, *“One of the greatest challenges we have – and I suppose every company has – is how do you quantify and assess what the impact of these risks will be?”*

Mr. Traut shared with members the value he has found at Heinz using real-time survey tools to assess key risks: *“After we get a sense of the top elements we need to address, we sat with the functional area leads in real-time sessions to vote on the likelihood, impact and level of control of the top risks by functional area.”* Prior to the network meeting, one member, who had tried a similar survey process, said it was *“very revealing and told us a lot about how different people within the company understand our risks and how they’re mitigated,”* but another member reported that *“we’re not doing [the survey] again because we found it ultimately not very actionable.”*

Mitigation and reporting

Risk mitigation is arguably the most difficult aspect of any risk management program. The COSO framework 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.⁹

Company practices for risk mitigation vary depending on the nature of the risks: while some may simply necessitate the preparation of backup plans, others may warrant modifying operating practices or designing specific programs tailored to mitigate the risks. Risk reporting may entail separate processes designed for that task or may be embedded in business planning, decision making, and financial forecasting processes.

At the meeting, members repeatedly emphasized that the greatest mitigation tactic possible is getting to the point where handling the risk is ingrained in the day-to-day functioning of the business – as one member put it, *“baked into the strategic planning process.”* Prior to the meeting, one member described doing this by assigning risk ownership to individual management team members: “There are basically six categories of high-priority risks, and they break down into specific sub-risk areas. Those all get mapped to a specific management person who has the responsibility for ensuring those risks are being properly addressed and mitigated.”

When it comes to reporting risks, many SEACN members reported some use some form of either a *“heat chart”* or a *“matrix that highlights the probability and impact of all primary risks.”* Beyond this, members said there is a risk of being *“reported to death,”* and therefore they cautioned against overdoing the reports that are meant to serve as updates on the status of risk management. Members said that the audit committee can play a role in making sure these reports are optimal.

Mr. Traut said that at Heinz, he and his team report the salient points to the board and the audit committee: “[The report] should be a simple document. We’ve now color coded it to deal with the positive side of risk – value creation versus value protection. We report to the audit committee, other committees, and the full board on a regular basis.”

Ensuring effective oversight of risk management

The allocation of risk oversight responsibility across the board and its committees has been a popular topic of discussion for audit chairs in the United States in recent years. Previous network meetings have discussed the issue of allocation, but at the January meeting, SEACN members chose to address how the board and its committees work together to ensure risk is well managed.

Under the increased government and regulatory attention that the financial crisis has triggered, some boards are considering the addition of a risk committee at the board level, though other directors oppose such a move. Members pointed out that in August 2009, for example, two Hershey directors resigned from the company’s board, citing its creation of a finance and risk committee and objecting to the duties of the full board being transferred to a committee.¹⁰

⁹ Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrated Framework: Executive Summary* (Committee of Sponsoring Organizations of the Treadway Commission, 2004), 4.

¹⁰ [“Two Hershey directors resign over new committee.” Reuters, August 13, 2009.](#)



Reducing director liability

Over dinner, members of the SEACN were joined by Michael Smith, a partner at King & Spalding, who pointed out that a director's fiduciary duties include oversight of the corporation's legal, financial, and operating risks. Case law suggests that without evidence of "sustained and systematic failure of oversight – such as a failure to attempt to assure a reasonable reporting system exists," the courts are unlikely to hold individual directors liable for a company's inability to manage risk effectively. Further, the recent CitiGroup case set a precedent that directors cannot be held liable for "bad business decisions or being unable to predict the future."

Nonetheless, the plaintiff's shareholder class action bar is a highly specialized, well funded, and adroit group. Anytime share prices drop 15% or more, the directors are exposed to legal action. Directors can, however, take steps to reduce their personal liability exposure:

- Ad hoc attendance/participation by a board member in committee meetings of which he/she is not a member can increase the non-member's litigation risk regarding actions taken by the committee.
- Board members should prepare for meetings by reviewing information reasonably necessary to reach informed business judgments. Corporations should achieve a balance between providing directors unrestricted access to information, while not deluging them with so much data that they do not focus on the most important material.
- Develop and maintain a clear understanding of your D&O insurance policy and coverage. Review and ensure that the insurance includes Side A coverage, in particular, to provide additional protection against personal liability in circumstances where the corporation cannot or will not provide indemnification.
- Regardless of individual committee assignment, review thoroughly 10-Ks and 10-Qs, particularly the relevant risk factors to assure a thorough and accurate discussion of the material risks faced by the enterprise. Generally, limit committee meeting participation to committee members. Make committee pre-meeting materials available to all members of the board, but do not proactively send all committee pre-meeting materials to all board members.

Yet despite the increasing external focus on risk management, some SEACN members say that they continue to struggle to keep the full board engaged: *"The thing that I'm still scratching my head over is that our audit committee is very active in the area of risk management, but we're grappling with what to do with the board in total. We need to make this a board-level conversation and not just an audit committee issue."*

Regardless, they acknowledge that that detailed risk management oversight work is done in committees. At the meeting, SEACN members described four different approaches to handling risk at the committee level:

- **The audit committee drives risk management for the board.** In these cases, *"the audit committee is responsible for reviewing the design, processes, and implementation of risk [management]. They also serve as the point of contact for the management team on all risk-related matters."*



- **The audit committee oversees financial risks and allocates remaining risks to other committees.** For example, *“the compensation committee will address all risks related to employee matters, and we will be responsible for all financial and compliance-related risks – the risks that logically fall within our purview.”*
- **A stand-alone committee is formed to take on the primary risk related to the company’s business.** One member reported, *“I have seen in examples of medical devices companies, the safety committee will spearhead the risk management effort.”* Likewise, at a consumer products company, the quality committee might provide detailed oversight, while at a chemical company, the environmental committee will take on the responsibility.
- **A separate, stand-alone risk committee handles risk.** With the exception of boards of financial institutions, no members’ boards have proactively chosen to establish a separate risk committee – although most have considered it, they reported that many boards are often too small to sustain an additional committee and therefore in most cases the work is being covered by the audit committee or another committee of the board.

Evolution of risk management

As one member pointed out, *“Too often we’re looking in the rearview mirror. One of the problems with boards is we’re too busy looking at the last crisis and making sure that’s not going to happen again rather than looking at what’s happening ahead of us.”* Members took time to reflect on what the future might hold for enterprise risk management. In particular, they highlighted:

- **The possibility of multiple risks occurring at once.** *“I’m not sure I have a good idea of the correlation between various risk factors. That’s where there’s greater risk, but it’s just not as obvious. Too often we think of risk in silos, but what if a domino effect occurs? What are those things that can come together to create a big thing, where multiple problems could be happening at once?”*
- **The risks and opportunities posed by the advance of technology.** *“The pace of change when it comes to technology is so dramatic that I think it’s going to force risk management to become ingrained in everyone’s way of thinking.”* Moreover, as members were quick to point out, more often than not boards are not well connected to this environment and therefore are particularly vulnerable to falling behind the pace of change.

Conclusion

Members agreed that ERM *“is very much an evolutionary process and one that continues to evolve every day. I’m not sure any of us will ever reach the finish line.”* In the meantime, members are committed to making sure risk-related issues stay at the top of the board agenda. SEACN members benefited both from sharing risk practices in use at their companies and from the discussion that ensued. The success of their dialogue highlights a clear need for more positive, leading-practice sharing as a corrective to the prolonged focus on what has gone wrong with enterprise-wide risk management.



About this document

The Southeast Audit Committee Network is a group of audit committee chairs drawn from leading North American 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 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 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:

- Eddie Adair, Audit Committee Chair, Tech Data
- Denny Beresford, Audit Committee Chair, Kimberly-Clark and Legg Mason
- Renée Hornbaker, Audit Committee Chair, Eastman Chemical
- Doug Ivester, Audit Committee Chair, SunTrust Banks
- Claude Lilly, Audit Committee Chair, FairPoint Communications
- Andy McKenna, Audit Committee Chair, AutoZone
- Dean O'Hare, Audit Committee Chair, H. J. Heinz Company
- Vicki Palmer, Audit Committee Chair, First Horizon National Bank
- Jim Robbins, Audit Committee Chair, DSW
- Carol Tomé, Audit Committee Chair, UPS
- Erik van der Kaay, Audit Committee Chair, RF Micro Devices
- Bunny Winter, Audit Committee Chair, Wellesley College

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

- John Farrell, Audit Committee Member, Lender Processing Services
- Edwina Woodbury, former Audit Committee Chair, R. H. Donnelley

Ernst & Young was also represented by:

- Steve Konenkamp, Southeast Assurance Managing Partner
- Karole Lloyd, Vice Chair and Southeast Managing Partner
- Chuck Seets, Principal



Appendix 2: Selected questions audit committee members might ask 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? Is there an individual designated to lead risk management activity at your company? Why was that person selected? Do risk professionals garner the respect and attention they need? 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 does your approach to risk identification compare with those outlined in this document? How is your list of risks generated? What screening criteria are applied? Who participates in the identification process? What sources does your company turn to for risk identification (e.g., line management, external expertise, industry benchmarks)?
- ?** What methodology is used to prioritize the list of potential risks? What quantitative and qualitative factors are taken into account? Are your company’s risks aggregated centrally so as to allow for a company-wide view?
- ?** Do you feel your company approaches risk mitigation effectively? What tools does management use to mitigate material risks once they are identified?
- ?** Is there sufficient risk expertise in your business areas to ensure that risks are properly addressed? How is this expertise developed and shared with new staff?
- ?** How does the full board support the risk management activity? Have you made any changes to the role and remit of any board committees? What might you like to change?
- ?** 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? What is the nature of the risk management discussions between the board and management?
- ?** What risk oversight practices has your audit committee or full board taken on that you feel are particularly useful or innovative?