



Risk management: in search of a practical approach

Introduction

The Midwest Audit Committee Network is a group of audit committee chairs drawn from leading Midwest companies. 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 evolving audit committee environment.

The second meeting of the network was held in Chicago on April 14, 2008, and focused on practical ways for boards and audit committees to effectively oversee enterprise-wide risk management.

This document reflects a synthesis of the key issues that emerged from the meeting. The ultimate value of *VantagePoint* lies in its power to help all constituencies develop their own informed points of view on important issues such as these. Anyone who receives this publication may share it with those in their own network. The more broadly we can disseminate this information to board directors, management executives, and their advisers, the greater the value created for all.

The members of the network present at the meeting, who sit on the boards of 30 large-, mid-, and small-cap companies between them, were:

- Brian Anderson, Audit Committee Chair, W. W. Grainger
- Cheryl Francis, Audit Committee Chair, Morningstar
- Sandy Helton, Audit Committee Chair, Covance
- David Landsittel, Audit Committee Chair, Molex
- Tom O'Neill, Audit Committee Chair, Archer Daniels Midland
- Rich Roedel, Audit Committee Chair, Brightpoint
- David Schwartz, Audit Committee Chair, Walgreen
- Dennis Van Mieghem, Audit Committee Chair, AEGON USA
- John White, Audit Committee Chair, Motorola

Ernst and Young members participating in the meeting included:

- Tony Anderson, Midwest Area Managing Partner
- Kevin Cole, Partner

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

Members of the Midwest Audit Committee Network agreed that existing risk management frameworks are often either too complex or too general, and they are seeking a more practical approach. Members believe that risk management activities are fundamental to a well-run corporation, and they discussed ways in which the board and the audit committee can oversee these activities:

- **Engaging management in the task of risk management** (page 2)

Good leadership, members agreed, is essential for effective risk management. For enterprise-wide risk management (ERM) to be effective, the CEO must be persuaded of its importance. Members identified a number of tangible ways to ensure the commitment of the CEO and management.

- **The governance of enterprise risk management** (page 4)

While members agreed that the full board has the ultimate responsibility for ERM, many questioned whether the full board can play an effective oversight role. Members generally agreed that for the time being, the audit committee can serve as an important catalyst to ensure that risk management processes are developed.

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

Members agreed that the first steps in any risk management process are to identify and prioritize the most significant risks. However, they acknowledged that past efforts have failed to identify certain risks that later caused problems, and many believe that there is much room for improvement. Members described a range of risk management practices, including having business unit leaders aggregate and identify at the corporate level systematic company-wide risks that persist across the organization.

- **ERM in action** (page 6)

Members said risk management should be embedded in management's decision making and strategic planning rather than be a stand-alone project. Boards must approach risk management as a dynamic process.

Engaging management in the task of risk management

Members observed that risk management has increased in prominence in recent years and believe that more time should be spent on discussions of risk identification, minimization, and mitigation. They agreed that boards have struggled to get a handle on risk management and noted that increased interest has not always led to increased clarity. In a discussion before the meeting, one member summed up the general sentiment: *"ERM is a very mystique-driven concept right now, and I'm still really trying to get my arms around it. I've been to numerous seminars, I read a lot, and I talk with a good number folks about it; to say that nobody has the right answer to this is an understatement."*



The importance of the CEO

Members all agree that CEO support is necessary for effective risk management. According to one member, *“If [risk management is] not happening at the top, it’s not happening.”* Another member put it even more strongly, *“The first, second, and third requirement is really the commitment on the part of the CEO.”* In short, *“You can have all the [risk management] systems and procedures in the world, but without senior management buy-in, it’s worthless.”*

Some CEOs hesitate to embrace a formal risk management program on the grounds that it is often difficult to demonstrate a tangible return on investment. As one member shared before the meeting, *“I have a CEO who said to me, ‘When somebody can show me the value that I’m going to get from having a fulsome ERM process and how it’s going to help better run and control my business, I’m ready to do something. I’m not going to spend a lot of time and money until somebody can show me that.’”*

However, members pointed out that return on investment (ROI) is not an appropriate measure for risk management because the substantial value ERM programs offer is often difficult to quantify: *“You cannot just do a quick cost/benefit analysis of risk management.”* One member observed that demonstrating value from ERM is like proving a negative, *“It’s easy to explain when it doesn’t work, but it’s not easy to know when it does.”*

Risk management can also be a catalyst for cultural transformation, and members agreed effective risk management processes often contribute to a more open, transparent corporate culture. One member said, *“It is helpful to have a process that takes the risk and makes it explicit rather than implicit. At the very front end, it helps solidify the fundamental philosophy of the company around risk management.”*

Concrete ways to foster the CEO’s commitment to ERM

Members shared several concrete ways in which audit committees can foster the CEO’s commitment to effective enterprise-wide risk management:

- **Evaluate and compensate the CEO based on ERM’s success.** *“On one of my boards, enterprise risk management is part of the CEO’s compensation. If they don’t reach a particular goal for risk management, then their compensation suffers. As a result, they don’t look at ERM as an expense.”*
- **Provide specific examples of instances in which ERM succeeded.** Members agreed that being able to point to situations in which risk management was successful can help win over the CEO: *“Anything you can do to make it more tangible is better. At [one company] there was a data error, but it served as a wake-up call because it’s a core piece of the business. We’ve [now] improved data [processing] to the point where it’s become a competitive advantage. It was on the list before the error occurred, but when the CEO could tangibly see that ERM created value, it really helped in our overall goals for risk management.”*
- **Do not let the ERM label get in the way.** *“There’s a big fear [on management’s part] that ERM is going to just be a big black hole that you pour money into, and it just becomes a check-the-box mentality as a result. I think it’s really just the labeling that gets in the way. I think if you can overcome*



that, a lot of this is already going on within the business, so it's really just being able to wrap your head around it."

- **Use ERM as a developmental opportunity.** Many members said ERM activities can help embed a strategic risk management philosophy in the organization's culture. One member said, *"Our board found it helpful to tie [risk management] to war-gaming. [A competitor was recently perceived as] a real threat, so we commissioned a team of lower-level management to go through pros and cons and dig into various scenarios. We ultimately concluded that a takeover was not as big a threat as we originally anticipated. In fact, one team ended up predicting exactly [the actual competitive response]."* Another proponent of this approach added, *"I think giving up-and-coming people [risk management] projects, coupled with heavy CEO engagement, is a great idea."*
- **Require the CEO's commitment to ERM.** Members ultimately agreed that the board must simply require the CEO's commitment to risk management: *"Lack of CEO buy-in should not be acceptable to the board. If there's a problem with the CEO taking responsibility for risk management, then I lay that at the feet of the board to handle."*
- **Hire a CEO who views ERM as a top priority.** If the board is at a stage of hiring a new CEO, then hiring one who supports ERM from the start will save time and effort in persuasion later: *"When we did the executive search for a CEO, it was very important that risk management [be] a top priority for [the candidate]."*

The governance of enterprise risk management

Members engaged in a lively debate about the most effective way for boards to oversee risk management. Some asserted that risk management was primarily the responsibility of the full board, while others argued that it was most practical for the audit committee to take the lead.

One member said prior to the meeting, *"I don't think you can delegate [ERM] to one particular committee or group. I think the board as a whole group has responsibility for the oversight of risk management."* Several members disagreed, however, saying that board work is best done in committees. One member argued, *"The heavy lifting really needs to be done in committee. Risk management is complex and requires too much [detailed] thinking, and a board meeting is not the place to do that."* Another member pointed out, *"ERM often falls to the audit committee because it's in most of our charters anyway."*

While appreciating the value the audit committee can add to ERM, several members were unsure about the wisdom of continuing to expand the audit committee's mandate. One member was also worried how others would view the audit committee's involvement in ERM: *"I worry that the audit committee can become a dumping ground, and if the audit committee takes responsibility for risk management, [does] that signal that it is primarily a compliance function?"*

Members recognize the paradox: most believe the full board should lead risk management oversight, yet board meetings are not the right forum for this important work. Although some said the decision to form a separate risk committee is a matter of *"facts and circumstance,"* most (with the exception of those serving on the boards of financial institutions) rejected the idea.



The New York Stock Exchange (NYSE) on the audit committee’s risk oversight responsibilities:¹

- “While it is the job of the CEO and senior management to assess and manage the company’s exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the company’s major financial risk exposures and the steps management has taken to monitor and control such exposures.
- The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken.
- Many companies, particularly financial companies, manage and assess their risk through mechanisms other than the audit committee. The processes these companies have in place should be reviewed in a general manner by the audit committee, but they need not be replaced by the audit committee.”

For many boards, the audit committee will need to serve as a catalyst to get risk management off the ground, even though this may not be the ideal long-term solution: *“I’m still not sure whether or not the audit committee should own the process, but I think somebody just has to get this thing going. By default, it often ends up on the shoulders of the [audit] committee and, while it might not be the ultimate place for it, I think the audit committee can at least get it started.”* Added another member, *“I think there is a danger in expecting nirvana. I think the takeaway here is to just get this thing kick-started, and to do that, it takes a committee. If you try to do that at the board level, everyone just gets really frustrated.”*

Either way, members agreed it is important not to confuse risk oversight with responsibility for managing risk: *“The audit committee should not be driving [ERM]; management should be driving it. I want to be sure the audit committee maintains a meaningful oversight role, but not an active management role.”*

Identifying and prioritizing key risks

Members agreed that the first steps in any risk management process are to identify and prioritize the most significant risks to the business: *“I think the key question for me is, ‘How do you handle a process that is both robust and simple [in a way] that will help you to truly identify the risks that are most important, without making it an over-burdensome process?’”*

Prior to the meeting, several members described approaches they have taken to identify key risks at their organizations. One said, *“Management took all of our risks from the 10-K and laid those out and assigned those risks to the four standing committees of the board.”* However, one member noted that *“the [10-K] and the [10-Q] are not really embedded in the business, and oftentimes that list is created by the company lawyers.”* Another member shared, *“[The board asked] each business leader to list risks for his business unit, and the organization as a whole, based on the percentage of how they would impact the equity and/or*

¹ Commentary from the *Final NYSE Corporate Governance Rules 303A.07(c)(iii)(D)*, <http://www.nyse.com/pdfs/finalcorpgovrules.pdf>.



income.” Although the initial lists were quite long, this member said that when lists were aggregated across the executive team, the final list of frequently named risks was quite short and very useful.

Once the corporation has developed a comprehensive understanding of its material business risks, it must classify those risks and determine their relative priority. As one member pointed out, *“It’s important not to just have your list of the ‘100 horrors’; ... [you should be] able to identify the 20 that can have the most severe impact on your business. I think that’s one of the most important issues – attaching priorities. Then, once risk is identified and you’ve attached the priority, you need to be sure you actually answer the question and know what you’re going to do with this risk.”*

One member shared a practice they found to be effective: *“At my company, we have an interesting process for prioritization. First, we look at the two elements of every risk: likelihood and impact. We then take each risk, and a number of people add their input on whether they believe it is high, medium, or low [for both likelihood and impact], and we ultimately are able to put together a heat diagram. I find it to be pretty effective and simple, and I think we’ve utilized it pretty well.”*

Still, while some members stated that they have found it *“fairly easy to organize, identify, and do the initial prioritization of risk,”* others question whether any companies have developed a truly effective process: *“[At my company], we have been involved in ERM for three or four years, but when I reflect back on the big surprises, not one of them was predicted by our ERM process. We had to take a major charge recently ... and we hadn’t anticipated that at all. It’s so easy to just turn a crank and produce another dashboard and make another list, but the bottom line is, I can’t identify a place where [ERM] has identified or stalled that risk, and a lot of times the board is left to clean up the mess.”* Another member reflected, *“What I worry about is what I don’t know to worry about.”*

Several members said external consultants can provide useful inputs to ERM. One member noted prior to the meeting, *“I think companies are increasingly bringing in external consultants to make sure that they understand everything that’s going on as far out as they can.”* In considering where to turn for external advice, one member said, *“There’s a danger of looking for the ‘Risk Czar’ rather than looking for someone who knows your industry and competitors well.”*

ERM in action

Identifying and prioritizing risks are only the first steps in the ERM process, however. Management must remain engaged when it comes to dealing with the risks that have been identified, and the board must remain engaged in overseeing the process.

The board must ask questions

Members agreed that one of their most important responsibilities as board members is making sure that they are constantly asking questions: *“The questions we ask as a board are important. Both the board and management have a responsibility to really understand the business model, so that our discussion can contribute in a meaningful way.”* Another member added, *“I think as a board we need to constantly be*



asking ourselves, ‘How do we make risk management part of every conversation and make sure we’re reinforcing the tone at the top?’”

One member shared an experience with time-sensitive risks that emphasized the importance of asking questions at the board level: *“When we were [releasing a product], we were dependent on one supplier, and when that was delayed, it cost us millions of dollars. Things like that happen in the supply chain, and sometimes the basic blocking and tackling doesn’t always cover it. I think the questions one should ask at the board level is something we should emphasize. I realize now that I should have been asking more questions.”*

Make sure ERM is not a one-time, stand-alone process

Members agreed that effective risk management is not a one-time project that can be checked off a list; it is an ongoing process that requires continuous review and revision: *“The premise we started on was that we take [ERM] as its own separate issue, and now we have revised that and said that the end game needs to be on a path that is much more integrated.”* Offered another member, *“You need to make sure ERM gets tied into discussions about key processes. If you leave ERM as another stand-alone activity, you’re risking it not being effective.”*

Members described two ways companies can embed risk management into existing processes:

- **Board dinners with management to discuss key risks.** *“[Before] every board meeting, we have a dinner that is broken down into five or six components. Management will start by giving a standard ‘State of the Union,’ and then we talk about the various political and environmental risks we are facing, and it gives us an idea of what we’re talking about. At the very least, it is a good way to educate the board, and I find it very helpful.”*
- **Interviews with business unit leaders.** *“[At my company], management interviews business unit leaders, and then folks at the top identify the highest priority [risk] items. This is done once a year, when we’re already talking about our business strategy.”*

Several members pointed out that it is important to remind management that *“process isn’t a four letter word.”* While some believe process can take away value, in this case, members believe the tangible value of ERM derives precisely from the process. Several members pointed out that management may be more persuaded if ERM is viewed not merely as a set of processes to avoid disasters but as a means to grow the business more thoughtfully: *“I think [risk management] needs to be integrated with the strategic planning process. The whole idea is to develop a strategy that [bolsters the company against] vulnerability to things that could be a major issue.”* Notwithstanding this member’s view, 44% of companies globally do not formally link risk management to business strategy.²

Members agreed that it is also important to determine in advance an appropriate level of risk tolerance: *“It can be hard to know where to stop. How do you figure out when you have done too much?”*

² Ernst & Young, *Companies on risk: The benefits of alignment* (New York: Ernst & Young, 2006), 14. Available at [http://www.ey.com/global/download.nsf/International/Global_Risk_-_Corporate_Survey_Report/\\$file/EY-Risk-Corp-Survey-Report.pdf](http://www.ey.com/global/download.nsf/International/Global_Risk_-_Corporate_Survey_Report/$file/EY-Risk-Corp-Survey-Report.pdf).



Remember that risk is dynamic

Risks are not static; they are dynamic. As one member pointed out, *“Number 20 on the list of risks today might be number one on the list tomorrow, so there needs to be an ongoing dialogue and evaluation process.”* Another audit committee chair said, *“I think about risk a lot, and I worry a lot about what the risks are. I worry about getting caught in a static situation here – in a mechanical mind-set. The state of thinking about these issues [needs to] change. Things can move quickly in even a couple of months.”*

All members struggle with the necessity of dealing with risk management continuously. One member said, *“At the end of the day, finding a way to manage risk on an ongoing basis is what I find to be the real challenge.”* Another member noted prior to the meeting, *“You can’t just have risk management in a glass case on the boardroom wall, with a hammer next to it that you pull out in an emergency. This needs to be an ongoing conversation.”*

Conclusion

A popular Chinese proverb states that “a journey of a thousand miles begins with a single step.” In the quest for a practical approach to risk management, this much is clear: *“ERM is an evolutionary process,”* and companies should not wait until they have a clear road map to set out. The audit committee chair can play a valuable role in ensuring that the company addresses risk in a more systematic manner, considering changes in risk as well as ways to incorporate risk management into the organization’s overall strategic planning process.

Despite many unanswered questions, members believe risk management is a journey worth taking, and they view the future of risk management with confidence: *“Six years ago, we were talking about the difficulty of SOX and [Section] 404, and – you know what? – organizations figured that out. There was a risk that companies would not figure that out, and they stepped up. I think this is the next great frontier, and I think people will figure this out [too].”*

The views expressed in this document represent those of the Midwest 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.