



## A deeper dive into risk management practices

### Introduction

The Midwest Audit Committee Network (MWACN) held its sixth meeting on October 15, 2009, in Chicago. Network members, who sit on the boards of more than 25 large-, mid-, and small-cap companies between them, used the meeting for a deep 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.<sup>1</sup> For a full list of participants, see Appendix 1 on page 9.

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% of respondents believe their risk management programs could be improved.<sup>2</sup> 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.<sup>3</sup> Given that there are few commonly agreed-upon best practices in risk management, members recognized the practical value of sharing, in a confidential setting, specific risk management approaches from the companies on whose boards they sit.

### Executive summary

In order to fulfill their risk oversight responsibilities, members agreed it would be beneficial for directors to understand and benchmark specific enterprise risk management (ERM) 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 organizational approach to enterprise risk management** (*Page 2*)

Audit committee chairs reported that even the basic step of defining risk appetite is difficult, and they warned that companies could become too risk averse. Specifically, several members thought the term “*enterprise opportunity management*” better reflected the presence of “*game changing*” strategic opportunities resulting from the economic crisis. Meeting participants noted a diversity of approaches to the design of risk management processes at the organizational level. Some companies assign risk management to an individual, often the chief risk officer (CRO). Others have formed a management committee to coordinate risk management efforts. Members agreed that the internal audit function can play an important role in the initial development of a risk management program, though some members said this capability might be migrated over time to the group responsible for strategy.

<sup>1</sup> *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 MWACN members during and after the October 15 meeting.

<sup>2</sup> 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).

<sup>3</sup> *Ibid.*, 2.



▪ **Drawing on all resources to identify and prioritize risks** (Page 4)

Members agreed that an effective risk management program must identify and assess a comprehensive list of material risks. Processes that members highlighted for identifying those key risks include building on the risks listed in the 10-K, interviewing business unit leadership, reviewing competitors' risk disclosures, discussing correlated risks, brainstorming risks during the strategic planning session, and fostering board curiosity. Given that management can often be *"too close to the trees"* in their awareness and understanding of risk, members agreed that external advisers could add value by providing fresh perspectives and *"stress testing"* the company's process for identifying and assessing risks.

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

Meeting participants agreed that identifying risks is much easier than mitigating them. While a *"fortress balance sheet"* is often the best form of risk mitigation, this comes at a significant opportunity cost. One member reported that it is important to be attuned to early warning signals and remain *"agile, flexible, and adaptive"* in order to better navigate economic cycles. Members also said individual risk accountability *"is a form of mitigation in itself."* Another member described a *"comprehensive loss report"* that documents operational failures along with mitigation plans. While many risks cannot be easily measured, almost all members said that their companies use some form of heat chart or probability/impact matrix to track and report key risks.

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

Members discussed whether the ultimate responsibility for ERM should reside with the full board, the audit committee, or an independent risk committee. While some members question the board's ability to dig deeply into key risks, many members thought the ownership risk needed to belong to the full board. Still, the audit committee can play a valuable role by overseeing the process and ensuring the board focuses on the highest-priority risks. Participants agreed that corporate culture is a critical piece of the risk management program and encouraged their fellow directors to ensure risk management practices are embedded into all business processes.

For examples of questions audit committee members and other board directors might ask themselves about enterprise risk, see Appendix 2 on page 10.

## Designing an effective organizational approach to enterprise risk 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.<sup>4</sup> MWACN 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 first step is a difficult one. As for risk ownership, members noted a range of trends in assigning risk responsibility at the organizational level.

---

<sup>4</sup> Ibid., 9.



## An actionable definition of “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.”<sup>5</sup>

While this definition is helpful, members agree that it is difficult to define an optimal level of risk: “*We did one round of discussions on risk appetite, and I think to get it right you really need to go through two to three iterations of that discussion, where everyone is comfortable that they’re speaking the same language and they have enough choices. The primary benefit of doing the exercise is beginning the dialogue,*” remarked one. Another said, “*Risk appetite is something we still struggle with. The notion is that you’re not going to be successful if you’re unwilling to assume some risk, but how you define that appetite is very difficult.*”

Indeed, some have tried to set strict parameters, but without success: “*We set very specific boundaries around how much risk to take on and never went beyond [those boundaries]. Then the [economic crisis] occurred, [which] no one could have anticipated. By the time we would have put the brakes on, it would have taken five months [to make a difference]. After that, we struggled with how, as a board, you say, ‘This is our risk appetite.’ We thought we had strict parameters, but it didn’t matter.*”

One member pointed out that risk appetite might vary based on the quality of the people responsible for those risks: “*You might find risk appetite ebbs and flows in particular areas depending on who is leading the efforts. [In] an area where you have a superstar, you might be willing to take on more risk, as opposed to an area with someone who is new and unproven.*”

Despite the ongoing challenge of effectively defining risk appetite, members agreed that directors need to remember not to be “*too risk averse,*” since companies need to take risks to make money: “*All too often we worry about the death of the enterprise, rather than net future value. We’ve become so risk averse that a lot of good opportunities are being overlooked.*” Moreover, as one member pointed out, “*It should be called enterprise opportunity management. There will never be a better time for game changers. Everyone has gotten so risk averse, but it’s the perfect time to make changes and seize opportunities.*”

## A range of approaches exist for risk management at the operational level

Members acknowledged that “*each industry has different challenges, so you can’t just pick one [approach] to risk management and [say] that’s the way it goes for everyone.*” Still, when members described their companies’ risk management organizations, four primary approaches emerged:

- **Assign risk management to an individual risk executive.** Some companies assign responsibility for managing risk to a single individual. For many companies, this individual is the CRO, in role if

<sup>5</sup> 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](http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf).



not in title: *“Specific risks are divided across different committees and individuals, and they all report back to the CRO. They focus on various risks as they bubble up, and the CRO sits in on all of those meetings.”*

- **Assign risk management to the internal audit group.** *“I wouldn’t be apologetic about having risk management in internal audit – particularly [for] mid-market [companies]. [Internal audit personnel] understand risk, mitigation of risk, and also have an enterprise-wide perspective and enterprise-wide relationships. Obviously it depends on the quality of the group, but if they’re good, I think there are some advantages to internal audit taking a leadership role ... I think it’s pretty effective.”*
- **Assign risk management to a management committee.** *“Every business unit in the company is represented on the committee, and they meet on a monthly basis. They’re the ones that sign off on the heat risk map, and they’re the ones who debate it and report to the full board.”*
- **Assign risk management to the strategic planning group after incubation in internal audit.** *“ERM has always been part of internal audit, and we recently moved it to the strategic planning group. In fact, we took the person in internal audit and moved them to the strategy group.”* Another member pointed out, *“Internal audit is a good place to nurture and incubate risks, but over time, I think [risk] should find its way into the strategy group.”* A third member agreed: *“Risk management belongs side-by-side with strategy.”*

Meeting participants agreed that regardless of the approach, committed leadership is essential for effective risk management. Management – particularly the CEO – must ultimately drive the process: *“Our CEO would say he’s the chief risk officer. We have a CRO, but ultimately the buck stops at the CEO’s desk. Many CEOs see this as a line function and not as something integral to their jobs, and it’s our job [as directors] to not let that happen.”*

## Drawing on all resources to identify and prioritize 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.<sup>6</sup>

### 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.

---

<sup>6</sup> Ernst & Young, *The future of risk: Protecting and enabling performance*, 9.



Members described several processes for identifying those key risks:

- **Start with the 10-K.** *“We always initiate the process by taking a look at the risks we have reported in the 10-K.”*
- **Encourage internal audit interviews with senior leadership.** *“There are some risks that require in-depth analysis. Internal audit has interviews with select board members and senior leaders around the world to help identify a broader range of these risks.”*
- **Review competitors’ risks.** *“We make sure to review and do a deep dive into our competitors’ key risks as well.”*
- **Consider how risks are correlated.** *“When we’re looking at total risk at the board level, we talk about what would happen if the ‘perfect storm’ of multiple risks happened at the same time.”*
- **Brainstorm during the strategic planning session.** *“At one company, they have a strategic plan, but not much of a strategic planning process. Management is going to have a retreat and a facilitator and manage it more than [has been the case] the past. We are also going to use that time to identify the key risks and integrate those into the strategic plan.”*
- **Encourage board curiosity.** Meeting participants pointed out that *“pure curiosity on the part of the board is important.”* One said, *“The board is straddling the inside and outside, and yet outside, they serve on other boards and have outside perspectives.”* Another pointed out, *“I think there’s a behavioral challenge, in that people get overconfident and say, ‘This risk won’t happen here,’ or they don’t think through thoroughly enough about a broader range of risks. I think trying to pique the curiosity of the board enriches the discussion.”* Members said that foreign site visits and visiting with executives are two ways in which this curiosity could manifest itself.

### External advisers

Members agreed that companies *“are typically not great assessors of their own risk”* and said third parties could help with *“stress testing”* the company’s process for identifying and assessing areas of vulnerability: *“I’ve found that having that core group of people who understand [our risks] is important, but having that one external person who’s not involved is just as important. They ask and challenge [management] with good questions and usually bring an inquisitive viewpoint.”* Although members note that *“management can be reluctant to bring in outsiders that are out of their control,”* several members concurred that *“having that fresh external perspective that forces you to think outside the box is important.”*

Members acknowledged, *“The greatest risk is the one we haven’t thought of yet,”* and further, *“We will always miss something. We’re never going to get it exactly right.”* And yet, although many report that they are *“only in the second or third inning of this process,”* they are confident that *“over time, we’ll develop better ways for identifying and processing these risks.”*



### Risks that typically require board attention

A member of another network of audit committee chairs summarized the risks discussed in that network that should be of particular interest to directors:

- 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 audit committee chair observed 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 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.<sup>7</sup>

### A range of 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 a strong balance sheet is the most effective mitigation tactic.

---

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



Other mitigation approaches raised by members include:

- **Managing through troughs by monitoring early warning signs.** *“Trough management has been a big objective for us. We’ve been through multiple recessions now, and we’ve learned to anticipate that these troughs are coming every six years or so. We discuss at length in our strategy meetings what we can do to stay profitable. We have to get production married up with [demand], and we’ve done that by monitoring triggering events that serve as early warning signs.”*
- **Holding management accountable.** *“Holding people accountable is a form of risk mitigation in itself.”* Another member elaborated, *“You always need to ask if something passes the smell test. If you get a sniff and say something to the CEO, executives have to understand that if they do nothing and [the issue] comes back, [they] can be doomed.”*
- **Reviewing unanticipated events.** *“Two years ago, we started listing all of the ‘loss events’ that took place each quarter. Management asks, ‘What happened during the quarter that could have been avoided?’ What’s important is that they formalized a procedure for monitoring these losses, and it’s allowed us to ask, ‘What are you going to do to prevent it again in the future?’ It definitely helps you mitigate [operating risks] going forward.”* Another member observed, *“[This practice] would definitely push management more to reflect on the lessons.”*

In the Ernst & Young survey, 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.<sup>8</sup> Members agreed that one of the board’s oversight responsibilities should be to encourage appreciation of risk management: *“Our view is that risk management ought to be embedded in the business.”* One member shared an optimistic vision of the future in which risk is embedded in the corporate culture: *“Everything we’ve done has been to embed risk management into the business units and culture. I’m hoping a couple of years from now when we’re talking about this, we’ll be talking about it with the business managers in a business context, rather than as a [stand-alone] risk [discussion].”*

### **An emerging consistency in risk management reporting**

One audit committee chair noted, “Reporting on risk management is much more qualitative than quantitative.” Another observed, “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 MWACN 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.”

Members agreed that when it comes to risk mitigation, *“the only thing you can do is be agile, flexible, and adapt.”* As one member pointed out, *“The companies that were not flexible or agile [in the current financial crisis] are not around anymore. You need to adopt somewhat of a ‘what doesn’t kill you makes you stronger’ type of mentality.”*

---

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



## Ensuring effective oversight of risk management

Participants acknowledged that governance of enterprise risk management continues to be an ongoing topic of board discussion. Specifically, many continue to debate whether ultimate responsibility for ERM should reside with the full board, the audit committee, or an independent risk committee. Those who advocate for the audit committee or a separate risk committee argue that *“nothing ever seems to get fully addressed at the board level.”* As a result, some say that giving ownership of risk to the board *“is like kicking it up to the attic”* whereas *“having a separate committee handle this makes it much more actionable.”*

Nevertheless, several members felt that the full board should have the ultimate responsibility for oversight of enterprise-wide risk management, while granting that the audit committee can still play an important role in ensuring that risk management processes are developed: *“At the end of the day, it’s definitely a full board responsibility, but when you peel back the onion, the audit committee should be responsible for understanding the process and assessing the effectiveness [of the risk management program].”*

## Conclusion

Members agreed ERM is an evolutionary process and that companies will undoubtedly go through multiple iterations. As the process evolves, many are committed to making sure risk-related issues stay at the top of the board agenda, and several members asserted that they will press for greater candor: *“I’m taken by the dynamic of this [network] meeting. How do we get this dynamic and energy into a board meeting?”* Members were pleased to observe that slowly and surely, progress is being made: *“We’ve been talking about this issue of risk [as a group] for several years now, and I think our sophistication around this topic has improved dramatically. There’s a ways to go, but we’re definitely moving forward.”*

## About this document

The Midwest 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 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 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:

- Dave Burritt, Audit Committee Chair, Lockheed Martin
- Brenda Gaines, Audit Committee Chair, Office Depot
- 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

The following members were not able to attend the meeting but took part in post-meeting discussions:

- Howard Carver, Audit Committee Chair, Assurant
- Cheryl Francis, Audit Committee Chair, Morningstar
- Sandy Helton, Audit Committee Chair, Covance
- Olivia Kirtley, Audit Committee Chair, U.S. Bancorp
- David Landsittel, Audit Committee Chair, Molex
- George Off, Audit Committee Chair, Telephone and Data Systems
- Al Smith, Audit Committee Chair, Simon Property Group

Ernst & Young partners participating in the meeting included:

- Tony Anderson, Midwest Area Managing Partner
- Rich Bonahoom, Midwest Accounts & Business Development Leader
- Jim Logothetis, Global Client Service Partner



## Appendix 2: Questions audit committee members and other board directors might ask themselves about enterprise risk

- ? 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?