

The CRO's perspective

Introduction

Enterprise risk management is increasingly commanding the attention of both directors and management. Certain sectors, such as financial services and utilities, have historically formalized risk management practices because of their specific regulatory compliance requirements. Now, public companies across all sectors are increasingly formalizing their approach to risk management. To oversee these activities, some companies are instituting a chief risk officer (CRO) role to coordinate enterprise-wide risk management processes. Throughout *InSights*, we use the term CRO to refer to this role rather than to a position with this title.

This issue of *InSights* has been developed to help audit committee chairs gain a deeper understanding of:

- **The evolution of the CRO role**
- **Methods and frameworks for enterprise-wide risk management**
- **The governance of risk management**

In order to better appreciate the CRO's perspective, Tapestry Networks spoke with the executive in charge of risk management in 12 companies across different business sectors. Participants in the research included:

- Carl Berquist, Executive Vice President, Financial Information and Risk Management, Marriott International
- John Collins, Senior Vice President and Chief Risk Officer, Constellation Energy
- Robert Coords, Executive Vice President and Chief Risk Officer, SunTrust Banks
- Mike Gardner, Vice President, Audit Services and Enterprise Risk Management, Textron
- Chris Kite, Senior Director of Global Risk Management, Cisco Systems
- Suzanne Labarge, former Vice Chairman and Chief Risk Officer, RBC Financial Group, and Audit Committee Chairman, Novelis
- Ken LeStrange, Chairman, President, and CEO, Endurance Specialty Holdings
- Mike Milone, Senior Vice President; and James Traut, Director, Enterprise Risk Management, HJ Heinz
- Steve Schaeffgen, Vice President, Enterprise Risk Management, Harrah's Entertainment
- Diane Sheridan, Vice President and Chief Risk Officer, Air Products and Chemicals
- Keith Sherin, Chief Financial Officer, General Electric Company
- Mark Stevens, Senior Risk Officer, Fluor Corporation

This document uses a modified version of the Chatham House Rule whereby names of contributors to the research and their company or organization affiliations are a matter of public record, but the comments made in the conduct of the research are not attributed to individuals.



Executive summary

- **A new and evolving role** *(Page 2)*

The practice of risk management is increasing in importance within public companies. Many companies are formalizing their approach to risk management and developing CRO roles. CROs themselves believe their role to be primarily that of a process leader who ensures that risk is being identified at the senior executive level but managed effectively at the business unit level. CROs say a background in operations, rather than a specialization in risk, helps them understand how risks impact their company's core business lines. It is the CEO who has final responsibility for ensuring that a company manages its risk effectively, and it is critical that the CEO provides active support to the CRO.

- **Using customized frameworks for enterprise risk management** *(Page 4)*

Most CROs report that their companies are still in the early stages of implementing enterprise risk management. CROs are using “homegrown” enterprise risk management methodologies that allow them to tailor risk management practices to specific objectives or issues. They identified unanticipated risk and the sheer magnitude of possible risks confronting their companies as major concerns. An emerging issue is how best to use external expertise to challenge homegrown methodologies.

There were two broad methods for conducting risk assessments, but most of the companies in our discussion used a “bottom-up” approach. Every company used some form of dashboard or top-risk list to identify or rank the primary risks facing the company. Few companies were using quantitative methods for prioritizing risks. Some CROs expressed a desire to use risk management as a vehicle for value creation rather than as a process to manage potential problems. [For a list of good risk management practices recommended by CROs, see page 7.](#)

- **Ensuring effective governance of risk management** *(Page 7)*

The board plays an important role in ensuring that senior management is planning and implementing effective risk management processes. Often the board will delegate specific responsibilities to a standing committee, often the audit committee. CROs say directors are clear in wanting blunt and honest reporting of risk in the senior management presentations. The majority of CROs do not report directly to the full board, but to the committee charged with risk management. This creates the possibility that important details could be omitted, or that the presentation might unfairly skew the board's understanding of the risk priorities toward biases specific to the senior manager presenting. Audit committees may need to take another look at the risk reporting process. [For questions CROs said the audit committee should ask of them, see page 9.](#)

A new and evolving role

Our research participants, chosen from a cross section of industry sectors, agree on two key points: first, the practice of risk management is increasing in importance within public companies, and second, the scope and complexity of potential risks has grown over the past decade to include strategic, operational, and compliance issues. With this increase in corporate vulnerability, the accountability of the executive in

charge of risk has broadened proportionally, as reflected by the attitude of one CRO: *“No one will hold you accountable for a surprise, but [the executive management team] will hold you accountable if you don’t have a plan to deal with it.”*

The responsibilities of a senior risk professional were initially limited primarily to financial risk and insurance coverage. Today, however, the scope of the CRO role continues to expand – but this scope creep has not led to increased role clarity. When asked what the job encompassed, one participant said matter-of-factly, *“I do everything nobody else wants to do.”* Many were daunted by the challenge of the role before finally agreeing to take it on. One CRO who eventually accepted the position said, *“I resisted at first ... [because] ERM is very vague ... It’s boiling the ocean.”*

CROs believe their role is primarily that of a process leader who ensures that risk is being identified at the senior executive level and managed effectively at the business unit level. One CRO was unequivocal about the importance of a strong, company-wide risk management culture: *“My role is ‘risk management’ as a noun, not a verb. In the business units, they are responsible for risk management as a verb.”* Nevertheless, the CRO is the executive ultimately charged with looking ahead at future risks. The same interviewee’s job priorities were outlined as such: *“My main role is to be looking [at risk] across the company, across the industry, across the economy, or across whatever global business we are in and then communicate the findings back to the broader executive risk committee and the board.”*

Our interviews revealed that much of the risk management process takes place within business units. As one interviewee stated, *“risks aren’t in the corporate office; they are out in the business. The real goal is getting [business units] to understand risk.”* There was broad agreement that the more a CRO knew about the various business lines, the more effectively he or she could drive the enterprise-wide risk management process. Additionally, those we interviewed shared the opinion that awareness of risk needed to permeate the broader company culture. When asked who really manages day-to-day risk, one CRO responded, *“If somebody says ‘who manages your risk,’ the answer should be ‘everybody.’”*

Half our interviewees indicated that their role was dedicated exclusively to risk management, while the other half stated that responsibility for risk management was added to already existing roles. Most respondents stated that the CRO benefits more from an operational background, with *“experience across the company,”* than from a traditional finance or internal audit background.

The Audit Committee Leadership Network in North America reached a general agreement that an “enterprise-wide view of risk has to be both embraced and driven by the CEO.”¹ Ultimately, it is the CEO who has final responsibility for ensuring that a company manages its risk effectively. Although CEOs do take the concept and execution of ERM seriously, it is critical that this support is more than lip service. Across our discussions, CROs felt they had the CEO’s support, but one interviewee questioned whether the CEO would maintain the necessary commitment to ensure the ERM program’s success: *“[The] CEO is supportive of having ERM; I’m just not sure he is willing to do the hard work. If we can’t get the CEO aboard, [ERM] won’t work.”*

¹ Audit Committee Leadership Network in North America, “Enterprise Risk Management and the audit committee,” *ViewPoints*, December 22, 2003, 6. Available at: http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_Dec03_View3.pdf

There was a fairly even split among our interviewees between those who report to the CFO and those who report to the CEO. One respondent who currently answers to the CFO said, *“I think [the CRO] should be [reporting] to the CEO and the board.”* All but one interviewee stated that risk identification was primarily a bottom-up activity, but were of the opinion that, to be effective, it needed the attention and support of the senior executive team and the board. Some also mentioned that CEO sponsorship signals to employees the value of risk management as a driver of the company’s success. This increased focus on risk at the very top levels could possibly shift how some companies organize their CRO reporting structure.

Using customized frameworks for enterprise risk management

We were also interested in whether risk management is used to identify opportunities for value creation or simply as a tool to mitigate against potential destruction of shareholder value. Results were mixed:

- **Value creation.** One CRO wondered if their company was playing it too safe: *“There is a higher likelihood that we don’t take enough risks versus not being prepared for something ... we generally spend a lot of time protecting ourselves instead of looking for opportunities.”* Another CRO suggested that the board needed to be part of the equation by asking, *“How do we [the board] know if we are under-managing or over-managing risk? Do we have the right plan in place?”*
- **Value protection.** In contrast, another executive was pleased that their company’s view of risk management was *“more about being prepared for the downside,”* adding that *“85% of risk management is defensive.”*

Some CROs are simply not yet in a position to look beyond building basic risk infrastructure, even when the stated company goal is to use risk management as a vehicle to create competitive advantage. As one said, *“I don’t know how to do that yet.”*

Audit committee chairs frequently report that standardized risk frameworks such as the COSO ERM framework² are overly complex and confusing, and most of the CROs we spoke with agreed.

- **CROs using homegrown frameworks.** Virtually all of the enterprise risk management methodologies from our discussions were homegrown, allowing companies to tailor risk management practices to specific objectives or issues. The majority of CROs interviewed said they had looked at COSO and other frameworks as a starting point, but each then created their risk processes in-house. One interviewee, commenting on COSO’s financial risk focus, said, *“The COSO framework came from accountants, not from people who think about what goes bump in the night.”*
- **CROs using standardized frameworks.** However, five CROs in our discussions found value in adapting pre-existing frameworks such as COSO. Only one CRO used COSO to determine the company’s total risk portfolio; this CRO indicated that it would be used to design a dynamic risk profile to be administered and validated by the company’s internal audit staff.

² Committee of Sponsoring Organizations of the Treadway Commission, “FAQs for COSO’s *Enterprise Risk Management: Integrated Framework*,” D3. Available at: http://www.coso.org/Publications/ERM/erm_faq.htm

Risk identification

In this increasingly complex business environment, the importance of getting risk management right has never been higher. According to the *Economist*, “Managing a company’s risks is no longer optional; it has become a core part of looking after shareholder interests.”³ This sentiment is not lost on those charged with creating and maintaining an organization’s risk mechanisms and infrastructure. One CRO said, “*We believe we will develop shareholder value over the long haul by taking risks effectively.*”

Herein lies the CROs’ greatest fear: unanticipated risk and the sheer magnitude of possible risks confronting their companies. One interviewee shared tips for remaining focused amid such a vast universe of possible risks: “*You need to consider the unthinkable, but you can drive yourself silly. There is plenty of room to identify and improve on basic operational areas. If you do that, you’ll be better prepared to think the unthinkable.*” Another executive pointed to the fluidity of risk, particularly in a globalizing world: “*Risks are always evolving. Geopolitically, the world is more complicated, and we are a more global company than we were ten years ago.*”

Our research supports the finding that most companies have only just created the equivalent of a CRO role and are in the early stages of adopting enterprise-wide risk management processes. A 2005 survey by the Conference Board and Mercer Oliver Wyman indicated that “91% of companies are ‘positively disposed’ or are preparing or developing an enterprise risk management program, but only 11% had fully implemented an ERM program.”⁴ Not surprisingly, half of the CROs we interviewed had been in the role for less than three years.

Many of our interviewees’ companies conduct regular risk assessments to identify risks and then perform a gap analysis to show whether or not those risks are being managed effectively. Who is involved in the assessment varies, but there are two broad approaches:

- **Bottom-up approach to risk identification.** In at least two instances, internal audit departments conducted surveys of senior and middle-level company executives to rank the top 25 risks and the possible outcomes if these risks were left unattended. Another CRO followed a similar procedure, but included interviews with the board and individual focus groups. In that company, the survey resulted in an interesting second-order effect: “*[The survey] helped get people excited thinking about risk because it could help them get more capital allocated to the [risk mitigation] opportunities.*”
- **Top-down approach to risk identification.** One company relied on its institutional expertise by placing the entire responsibility for risk identification (and ranking) with a risk committee of senior management that received input from internal functional risk heads (e.g., health, security, safety, compliance). The CEO looked to the CFO, chief counsel, and functional risk teams to “*shepherd most of the big material-risk items in the company.*” The risk committee regularly collected the best thinking from the company’s top 25 leaders.

³ “Be prepared,” *Economist*, January 22, 2004. Available at: <http://www-personal.umich.edu/~kathrynd/BePrepared.Jan04.pdf>

⁴ Tammy Whitehouse, “Lots of Talk, Still Not Much Action on ERM,” *Compliance Week*, November 22, 2005.

One CRO cautioned against thinking the job was finished once risks were identified, saying, *“Listing of risks is very different than managing risks.”* Another CRO agreed with this observation: *“If you don’t have a process to put [the risk list] into play, then you haven’t really accomplished a whole lot.”* One of our interviewees, sensitive to the need to make risk management more than a theoretical management exercise, *“personally talks with the business units regularly and attends meeting to make sure [business unit heads] can address an issue right away.”*

The question of long-term tracking is also important. One CRO said, *“I do not believe we have a well-defined process for keeping [risks] up-to-date.”* Another CRO stressed the importance of viewing enterprise risk management as an ongoing process rather than a one-time event.

Prioritizing risk

CROs in financial services were more likely to prioritize risk according to quantitative measures and financial modeling, while in other sectors risk prioritization was conducted in a more intuitive fashion:

- **Quantitative methodology.** One CRO used a series of software tools to identify and track risk for every company project. The company first conducts a risk diagnostic that allows them to analyze risks in a format that looks at the probability, the severity, and ways to mitigate a particular risk. They then use a second software package to develop a database of the identified risks. The end result is the ability to place a specific dollar value next to each risk: *“What we’re trying to do is take the 101 risks ... after five to ten years, show the total impact and see what the magnitude of the risk really has been.”*
- **Qualitative methodology.** Companies across all sectors created or are in the process of creating some type of dashboard system to rank and prioritize their risk portfolio, and most companies also have some form of a risk “top ten” list to work from when categorizing enterprise-wide risk. In one company, management’s risk committee relied solely on their personal experience to rank enterprise risks and used no quantitative metrics to rate the probability of a risk’s occurrence or severity.

One CRO was concerned about having the right analytical tools to do a better job of quantifying risk. However, another CRO warned against the potential danger of over-reliance on quantifiable metrics: *“If it were too exact ... we’d fool ourselves into thinking we really understood the risk. We don’t.”*

Avoiding the echo chamber by using external expertise

According to our respondents, risk management is very much an internally focused process. Few of the CROs interviewed regularly use external advice to assist them with their ERM implementation. Some employ “risk-specific” experts during the initial design phase, but many complained that these advisers are often too specialized and are not able to address all their needs. For example, one CRO recounted how the company had hired a security expert to help shape their risk profile, but quickly realized that the consultant *“didn’t address the real risk elements of the business. Risk is much more complicated than security.”* However, external process management expertise is only one possible form of outside help. Other third parties, including external audit firms, strategy consultants, and industry analysts, may also be useful resources.



Now that risk management processes are taking root in companies, a few CROs expressed willingness to engage outside experts to either review the process itself or to help the company think strategically about risk in terms of competitive advantage. One CRO said, “[We have had] no significant interaction with the strategic planning process. This is where the use of an external group would give us the biggest bang.”

An important question for audit committees is whether homegrown risk methodologies catch all the risks that threaten the company. Additionally, how can audit committees ensure that management doesn’t end up locked into an echo chamber as a result of relying solely on these internally developed methodologies, with only internal input and no external review or validation? One CRO, commenting on the risk of an echo chamber effect, said, “I don’t think we are missing any big pieces, but what may become an echo chamber is what we are saying [to ourselves] about [the identified risks].”

Good risk management practices recommended by CROs

- Develop a method of prioritizing and categorizing risks, e.g., a risk pyramid with the hardest-to-manage risks at the top and the easiest-to-manage at the bottom. Develop a database of top risks to be tracked over time to determine the real impact of risks as opposed to estimated likelihood and impact.
- Set up a corporate risk committee with members drawn from senior leadership; have it meet frequently to ensure support and focus from the top and to bring leadership and experience to risk management on an ongoing basis.
- Conduct a broad survey of management at all levels in the company to get bottom-up input on the biggest strategic and operating risks to the company from the perspective of those operating “in the trenches” every day.
- Embed risk professionals within the business units and have them report to the risk management organization to ensure buy-in at the business level, with wider accountability.
- Develop a limited but clear set of operating policies and procedures, with clear ownership, to ensure risk management is embedded in corporate culture.
- Look for best practices from outside highly regulated industries, because the best of those companies are probably pursuing effective risk management to achieve competitive advantage rather than simply to satisfy regulatory compliance requirements.

Ensuring effective governance of risk management

The board plays an important role in ensuring that senior management is planning and implementing effective risk management processes. Often the board will delegate specific responsibilities to a standing committee. In most instances, the audit committee oversees the risk management process and has specific oversight of financial risk – and sometimes of all risks that have been identified. However, other board committees may have oversight of a specific risk area (e.g., the investment committee may oversee emerging markets and investment strategy risk).



What is the audit committee’s role in risk oversight? NYSE listing rules state:⁵

- “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.”

There is also variation in the level of person presenting the risk analysis to the board or board committee. In some companies, the CRO leads the presentation to the audit committee. At other companies, only the CEO or CFO reports on risk. Almost all the CROs interviewed said that board agendas cover a subset of overall risks, which they rotate for each successive board meeting or alter depending on current market or geopolitical conditions. One interviewee said that *“management lives and breathes the business everyday, so the board should ask them, ‘What are you doing to navigate the top risks?’”*

Directors are clear about what they want from the presentation. More than one CRO said, *“The committee wants me to be blunt. They don’t want any surprises.”* This poses the challenge of determining what level of detail is useful to the board or committee. One interviewee characterized this balancing act thus: *“The challenge is getting communication with the board that is at a macro enough level, but still gives them enough insight to fulfill their fiduciary responsibilities. The devil’s in the details ... it’s not an insignificant problem.”* This is especially true given that the cost of getting it wrong can be substantial: *“If you add up the dollar value of some of the risks we are assuming, our board members would have a heart attack ... How do they get comfortable without knowing all the underlying mitigations?”*

Another consideration for board members is to understand the degree and type of filtering that necessarily takes place as information is aggregated and summarized for the board. Since the majority of CROs do not report directly to the full board, there is the possibility that important details may be omitted or that the presentation might unfairly skew the board’s understanding of the risk priorities toward biases specific to the senior manager presenting. One CRO suggested that an executive session with the audit committee would benefit the company by allowing the CRO to speak uninhibitedly: *“There are questions that may need to be asked that would be better answered without other management present.”*

We asked respondents if the board or a committee had been involved in their selection in the way that, for example, many audit committees are involved in selecting the chief audit executive. Most did not know how involved directors had been in the process, but believed there would be more involvement when their

⁵ Commentary from the *Final NYSE Corporate Governance Rules* 303A.07(c)(iii)(D). Available at: <http://www.nyse.com/pdfs/finalcorpgovrules.pdf>



successors are appointed. One CRO told us, *“I think the recommendation should come from management, but the board should have veto power if they [don’t] think the person [has] the qualifications.”*

Questions CROs said the audit committee should ask of them:

Identifying risks

- What keeps you up at night? What are the key material risks to the company? How have you been talking to us about these risks throughout the year?
- How have you identified the top risks to the company? How do we know we are not missing major, material risks to the company?
- Are the appropriate people involved in making risk decisions? Has a third party weighed in on identifying and evaluating risks?

Managing risks

- How do we know if we are under-managing or over-managing risk? How do we know we have the best plans in place?
- What infrastructure do you have in place to mitigate major risks?
- Is risk management taken seriously within the company? Where aren’t you getting cooperation? Do you have the staff and resources you need?

Creating value

- How do the company’s risk management efforts pay off for shareholders? How can we use risk management to create competitive advantage?

Conclusion

Enterprise-wide risk, and how companies organize to manage it, is a crucial issue. Companies are uniformly concerned about the size of the challenge, but diverge on how best to position their organizations to deal with it. How centralized, how formal, how bottom-up, and how quantitative should the process be? The CRO role also remains a work in progress. There is no consensus on whether a company should have a CRO role, and indeed, the roles of many executives given that title are not yet fully defined. What is certain is that active oversight, inquiry, and engagement from the audit committee, working with senior management, can help companies resolve these issues and develop effective risk management processes, to the benefit of the company and its shareholders.

InSights

FOR AUDIT COMMITTEE MEMBERS



About this document

InSights is produced by Tapestry Networks to provide assessments of key issues of interest to audit committees. Initially, *InSights* will be distributed to members of audit committee networks sponsored by Ernst & Young and orchestrated by Tapestry Networks, who, in turn, will share it with colleagues on audit committees and boards, and their advisers. It will be distributed by Ernst & Young to its partners. Anyone who receives *InSights* may share it with those in their own network. The ultimate value of *InSights* lies in its power to help all constituencies develop their own informed points of view.

The views expressed in this document represent those of the individuals who participated in the research. 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.