

Emerging best practices in risk management: a network compendium

Introduction

Compliance with Section 404 of the Sarbanes–Oxley Act afforded companies across all industries the chance to reevaluate and reshape the ways in which they manage risk, and even though the compliance effort is now embedded, members of the Audit Committee Leadership Network and other audit committee networks continue to have a robust appetite for information concerning best practices within the risk management arena. Over the last few years, we have discussed risk management in many conversations with audit chairs, and it has been the topic of a host of network meetings.

This summer we asked members in several audit committee networks to identify their companies' risk management best practices. Though members were often reluctant to go so far as to designate their corporate procedures best practices, a wealth of ideas and initiatives came to light. Audit chairs also asked us to include the risk management practices that other network members and practitioners in the field – such as the 12 chief risk officers (CROs) featured in the previous issue of *InSights* – have shared.¹

This issue of *InSights* answers those requests through exploration of the following topics:

- **Risk management frameworks and guidelines**
- **Specific practices for overseeing, identifying, prioritizing, and managing risk**
 - Case study: Benchmarking risk parameters – lessons from the hospitality industry
 - Case study: Tone at the top – one CEO's perspective on risk management

A bibliography of network discussions on risk-related topics is included on pages 7-8.

This document uses the Chatham House Rule whereby comments made in the conduct of the research or during network meetings are not attributed to individuals.

Risk management frameworks and guidelines

Audit chairs recognize that while many companies are increasing their focus on risk management, they are “all doing [it] somewhat differently.” Multiple audit committee chairs commented on the fact that there are no established frameworks that companies can easily apply to their enterprise risk management efforts. As one audit chair pointed out, “Each company has to take the broad frameworks and see how they fit with their company.”

Then too, many audit chairs feel that although generalized frameworks such as COSO² offer useful guidelines, adhering to them slavishly can inadvertently force a company's risk management efforts to become somewhat narrow and rigid. As one audit chair put it, “We're far less wedded to a prescriptive use of COSO, which can become mechanistic ... you end up losing sight of the forest for the trees.”

¹ Ernst & Young and Tapestry Networks, “The CRO's perspective,” *InSights*, June 30, 2006, 5. Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_June06_InSights.pdf.

² More information on the COSO framework is available at http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf.

Given that all off-the-shelf frameworks need modification, which framework a company picks may be less important than simply picking one. One audit chair advised using “any framework to get the conversation started.” A number of audit committee chairs recommended resources – some industry specific – that are helping them consider appropriate parameters as they build their own frameworks. These include the Open Compliance and Ethics Group (OCEG) and the Committee of Chief Risk Officers (CCRO).³

Virtually all of the enterprise risk management methodologies mentioned during discussions with CROs were homegrown, which allowed companies to tailor them 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.⁴

Specific practices for overseeing, identifying, prioritizing, and managing risk

Numerous practices for overseeing, identifying, prioritizing, and managing risk have emerged from network meetings. Below are summaries of practices that many audit chairs have endorsed, as well as descriptions of other, more singular methods.

Risk oversight

- The audit committee may have responsibility for some areas of risk, but the full board is ultimately responsible for the enterprise-wide risk management effort.
- The division of risks is such that at one company, the full board is responsible for dealing with succession, sourcing and suppliers, competition, and political risks, while the audit committee deals with financial reporting and regulatory compliance, ethics, legal matters, and disaster recovery.
- The audit committee can play a facilitation role, making sure an adequate risk management process exists and that management is using it. Likewise, the CRO or other senior executive responsible for risk management should not “own” all enterprise-wide risks, but should instead be responsible for ensuring that an effective risk management process is in place and functioning smoothly.
- The audit committee will often have specific oversight of financial risks and may share oversight of other specific enterprise-wide risks with other board committees.
- A number of CROs suggested that boards meet with the CRO in a private session because, as one CRO pointed out, “There are questions that may need to be asked that would be better answered without other management present.”⁵

Risk oversight remains the element of enterprise-wide risk management that most concerns audit chairs. One audit chair asked, “Is there a magic bullet for dealing with risk? How do we get our arms around the subject of risk?” Another audit committee chair feels appropriate ownership of overall risk – at the board

³ Their websites are <http://www.oceg.org/> and <http://www.ccro.org/>, respectively.

⁴ Ernst & Young and Tapestry Networks, “The CRO’s perspective,” 5.

⁵ Ernst & Young and Tapestry Networks, “The CRO’s perspective,” 8.

level – still has to be decided: “The big question of ‘where does this fall?’ remains. Is it an audit committee issue or a board issue? Right now I think it’s pretty squishy.”

Risk identification and prioritization

- When identifying risks, questions to ask include: (1) What risks “keep the CEO up at night?” (2) Is there a ‘single point of failure’ that could take the company down? (3) What are the key reputation risks that could harm the company?
- Some companies assess the ways in which other organizations identify and manage their risks, then use those benchmarks to help flesh out their own risk management procedures and parameters. One CRO said, “We reach across industries – especially those that are not regulated – because we think they are doing [risk management] for competitive advantage.” See page 4, “[Benchmarking risk parameters – lessons from the hospitality industry.](#)”
- Multiple, formal inputs on risk can be illuminating. Several companies try to get a 360-degree view of risk by soliciting perspectives from their external auditor, internal auditor, and management. Some companies have engaged outside consultants (primarily risk specialists) in their initial risk-identification phase. One CRO said that the lack of an external perspective might lead to the danger of management efforts becoming something of “an echo chamber,” bouncing around the ideas and assessments with which senior executives feel most comfortable.
- Some companies use a top-down approach. In one company management conducts an annual executive survey within the company and board, asking all respondents to list the top 25 risks they feel the company is facing. Then respondents are asked, in the words of one audit chair, “Without regard to control, how significant is the risk? How well are we managing it? Where are the gaps?” One company holds a quarterly review with the CEO, COO, and 20 or so senior managers to “take the pulse of the company on things that concern each of the business lines.”
- An audit committee chair described how, at one company, “Business unit heads talk to the audit committee about risks they are facing and how they are dealing with them.” Though he noted that the information imparted was generally not surprising, “it’s comforting and educational to hear how managers think about risk in the business.”
- Extreme events such as Hurricane Katrina can help companies identify risks and learn important lessons in risk management. One audit chair noted, “We all support just-in-time manufacturing, but post-Katrina, companies found if they had a major supplier in the area, they had no inventory.”
- Letting history be the guide can help companies focus on the risks they are most likely to face. One audit committee chair felt it was all about “pattern recognition” and “defining your universe.” He pointed to risk management processes within the financial services industry and noted that they were the result of experience and past mistakes. “Good judgment comes from experience, and experience comes from bad judgment,” he said.



- One CRO prepares a report on the company's most compelling risks approximately seven times a year "to inform the board and management team of material risks." This report includes a dashboard that categorizes such risks as the company's credit portfolio, plant operations, financial liquidity, environmental compliance obligations, and regulatory concerns. The report then codes risks red, yellow, or green to show whether a risk is trending up or down over both the short and long term. The report includes both an explanation of the risk and the mitigating activities surrounding it. This company also uses quadrant analysis to plot individual risks on a four-square grid according to anticipated severity and likelihood of occurrence.
- Another company uses a "significant-risks radar," a report that shows the dollar value of a risk under current mitigation and the possibility of its occurring. Depending on the industry and the size of the company, the dollar value at which a risk becomes worth mentioning will vary.

Benchmarking risk parameters – lessons from the hospitality industry

Several audit chairs and CROs mentioned wanting to know how businesses in other industries manage risk. Businesses within the hospitality industry face some of the broadest and most potentially damaging types of risk. One organization whose CRO we spoke with has a highly detailed series of risk-related processes and procedures in place that are worth examining. "Our biggest risk is always brand risk," noted the CRO, "since our name is on every door."

Their risk management process begins with a set of wide-ranging policies that spell out detailed procedures for 85 types of potential risks, "everything from disbursement approval to governance to identity security for customers to protecting the brand." Each policy is vetted by internal audit, which also makes sure the policy is being followed. The company's legal department approves and monitors legal policies. In general, the board must approve the policies before they can be implemented. "There's an owner for every policy, and risk management within the business lines flows from each policy." Once risks are identified, they are broken down into four broad categories: strategic, operational, financial, and compliance.

"One critical policy [relates to] business continuity," said the CRO. "Every department must have a written plan that defines how they'll carry on, even under extreme adversity. And each plan is tested every year." The company's risk management group also includes a scenario planning expert, whose job "is to make sure we've covered all contingencies via scenario planning that she initiates," the CRO explained.

Another policy calls for all company accounts to be internally certified as being reconciled for each of the company's quarterly financial reports. This policy was adopted because "risk in financial reporting is often buried within the organization. You may have a problem and not know it. This nips it in the bud."



Risk management

- Audit chairs continually point to CEO leadership as perhaps the most significant factor for managing enterprise-wide risk and establishing “tone at the top.” One audit chair, who is also a CEO, said, “You may have a CRO, but at the end of the day, you’re the captain of the ship. It’s not an accountability you can delegate to anyone. I view this as one of my principle responsibilities at the company.” This individual further noted, “If people see risk being delegated to the back room, the cue will be picked up immediately, throughout the organization, and people will do the bare minimum. They’ll be more inclined to do what’s sexy.” Another audit chair commented, “The CEO driving the process is the most effective way to develop a strong risk management culture.” [See page 6, “Tone at the top – one CEO’s perspective on risk management.”](#)
- One approach is to establish a corporate risk committee, with members drawn from senior leadership. It should meet frequently to ensure support and focus from the top and to bring leadership and experience to management on an ongoing basis.
- A number of companies use a matrix approach. As one audit committee chair described it, this involves “having the board create a matrix of different risk areas.” The matrix shows “how responsibility is allocated organizationally for each of these areas, how this is communicated to the rest of the company, [and] which part of the board has oversight of this area. This has been effective in giving us something to talk about.”
- Another approach is to embed risk management in existing processes for managing the business. One audit chair observed, “Management [is] trying to embed risk management in the strategic planning process to drive managers to think about it explicitly. A separate antiseptic activity won’t work.”
- Companies can also manage risk at the operating-group level. One CRO mentioned that the various operating groups within the company must sign quarterly statements certifying that they are managing and mitigating divisional risks. This is then reported to the CFO and CEO.
- One CRO said, “Think about risk within three lines of defense. The first line is the business line. They own the risks and are responsible for managing them. The second line of defense is the risk management organization, which is responsible for developing policies and procedures around risk and for understanding the business lines and the roles of the people in them. The third line of defense is the external auditor and the audit committee.”
- The audit committee should ask four questions: (1) Is the company looking at interdependencies among risks? (2) How is the company working to mitigate, prevent, or “wear” the risk? (3) Is risk being looked at as an opportunity? (4) Is the company becoming too risk averse?
- Management should brainstorm potential crisis scenarios and come up with a crisis management plan in advance of any actual disaster; the audit committee must ensure that crisis plans are specific in nature and deal with identifiable threats, rather than generic ones.



Tone at the top – one CEO’s perspective on risk management

This case study focuses on a CEO who has a unique range of experiences. Formerly, he was employed in the financial services sector; currently, he heads a company that has both regulated and unregulated lines of business, and he is also an audit committee chair for another public company.

“Many companies look at operational risk only,” the CEO notes, “while some only look at financial risks and don’t take operational risks into account. In my opinion, companies must take a more sophisticated measurement of all their risks. I integrated the financial, physical, operational, and credit risks all in one place.”

From his first day on the job, he took steps to show how much importance he attached to enterprise-wide risk management: “On day one of my tenure as CEO, I appointed a CRO in order to make sure that risk management [would] be perceived as a critical priority throughout the company.”

To ensure that risk management remains a priority, this CEO chairs “a weekly risk committee meeting ... It’s the first meeting of the week at 7 a.m. every Monday.” The meetings are attended by his direct reports, all heads of businesses that have P&L risk, and the CFO and CRO.

This CEO believes that “risk is an inherent board issue, and it is management’s number one responsibility to build awareness at the board level of the business model and the risks faced by the enterprise.” He has recommended how frequently the board and audit committee should review risk. “Ultimately, we decided to give a risk update at every [board] meeting, with the audit committee getting a much deeper overview. I also had to [develop the confidence of] the board that the CRO was someone who could be trusted to drive the process.”

Conclusion

Though everyone agrees on the need for and value of enterprise-wide risk management, audit committee chairs continue to grapple with which methodologies are appropriate for individual companies. There is consensus, however, across all networks, that open and honest communication between the audit committee, the board, management, and the external auditor is necessary if appropriate risk management plans are to be developed and implemented across company lines.

One CRO summed it up thus: “No one will hold you accountable for a surprise, but they will hold you accountable if you don’t have a plan to deal with it.”



Bibliography

While most meetings of audit committee networks in North America inevitably touch on risk management, the following documents are dedicated to specific aspects of risk management:

Audit Committee Leadership Network

1. “IT risks and governance.” Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_July06_View13.pdf
2. “Pension obligations: a deep dive into one area of risk.” Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_July06_View14.pdf
3. “Risk management / Compliance and ethics.” Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_May06_View12.pdf
4. “Transaction risk: a role for the audit committee?” Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_Mar04_View4.pdf
5. “Enterprise Risk Management and the audit committee.” Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_Dec03_View3.pdf

Mid-Atlantic Audit Committee Network

6. “Risk management: in search of a practical approach.” Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_MidAt_ACN_May06_Van.pdf
7. “Enterprise Risk Management and the audit committee.” Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_MidAt_ACN_Mar05_Van.pdf

North Central Audit Committee Network

8. “Risk management: in search of a practical approach.” Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_NC_ACN_June06_Van.pdf
9. “Enterprise Risk Management and the audit committee.” Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_NC_ACN_Mar05_Van.pdf

Southeast Audit Committee Network

10. “Enterprise risk management and the audit committee.” Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_SEast_ACN_Oct05_Van.pdf

Pacific Southwest Audit Committee Network

11. “Enterprise risk management and the audit committee.” Available at http://www.tapestrynetworks.com/documents/Tapestry_PacSouthwest_ACN_Dec05.pdf



For directors who sit on the boards of global companies, whether listed in the U.S. or elsewhere, the meetings of the European Audit Committee Leadership Network that focused on aspects of risk management may also be of interest:

European Audit Committee Leadership Network

12. “IT governance.” Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_Euro_ACLN_May06_View8.pdf
13. “Major emerging markets risk.” Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_Euro_ACLN_May06_View9.pdf
14. “Preventing, detecting and investigating fraud / Insuring against risk.” Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_EuroACLN_Mar06_View.pdf

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 network members 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 individual leaders cited. They are not the views and do not constitute the advice of all audit committee network members, 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.