AUDIT COMMITTEE LEADERSHIP NETWORK
IN NORTH AMERICA
ViewPoints

April 13, 2015

TAPESTRY NETWORKS, INC · WWW.TAPESTRYNETWORKS.COM · +1 781 290 2270

Leading practices in enterprise risk management

On March 10-11, 2015, members of the Audit Committee Leadership Network (ACLN) convened in New York for their 29th stand-alone meeting. On March 11, one session focused on leading practices in enterprise risk management (ERM). The goal of this session was to share examples of ERM practices that ACLN members have found to be innovative or especially effective.

This *ViewPoints* presents a summary of the key points, along with background information and selected perspectives that members and subject matter experts shared before and after the meeting.[1] For further information on the network, see "About this document," on page 9. For a full list of participants, see Appendix 1, on page 11.

Executive summary

ACLN members shared ideas and practices on three main topics in their discussion of ERM:

- **Leadership and organization** *(page 2)*

  Members noted that effective ERM requires an engaged CEO who establishes priorities and galvanizes action on critical cross-company risks, such as cybersecurity. At the same time, accountability for ERM should extend through the business, with managers of the various business lines taking responsibility, supported by the staff of the risk function. Internal audit can assist the risk function with thought leadership and skills related to the ERM process, or it can provide independent assurance on the ERM system, though allowing it to perform both these roles could compromise objectivity.

- **Tools and techniques** *(page 4)*

  ACLN members brought up the benefits of desktop exercises to evaluate how the company would respond if certain risks materialized. In pre-meeting discussions, they described the use of broad-based company surveys to identify risks, which can then be analyzed and prioritized Recognizing that business opportunities often entail risks, however, members also argued that the ERM system should enable risk taking by both mitigating risks and evaluating residual risks against the company's risk appetite.

- **Board and audit committee practices** *(page 6)*

  In order to be effective, the board must work with the CEO to prioritize the risks it focuses on. It should also get out into the field, spending time with business leaders and their employees, and it should conduct deep dives on key risks. Delegating some oversight of specific risks to committees other than the audit committee may make these responsibilities more manageable, and paying attention to the mix of experience and skills on the board may also be helpful.

For a list of discussion questions for audit committees, see Appendix 2, on page 12.

[1] *ViewPoints* 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 are not attributed to individuals or corporations. Italicized quotations reflect comments made in connection with the meeting by network members and other meeting participants.

Leadership and organization

ACLN members pointed out that the organizational aspects of the ERM system are critical to its effectiveness, yet they noted that some companies are still falling short. One member said, *"The amount of bureaucracy in ERM is huge."* Members described three approaches to improving the organizational foundation of ERM and turning it into a strategic enabler as opposed to a box-ticking exercise:

- Engaging the CEO
- Assigning responsibility throughout the organization
- Leveraging internal audit

Engaging the CEO

In advance of the meeting, several members noted that the CEO plays a major role in ensuring that the ERM system is not just a bureaucracy. One member said, *"Where the CEO owns or sponsors or is very involved in ERM, that's when ERM works best. I have seen it have a big, big impact."* Others elaborated: *"It wasn't until the CEO personally owned the process that it got jumpstarted. That was really important – tone at the top ... the CEO became the chief risk officer. Whenever it was discussed, he was involved … He led the conversation on prioritization. The organization could see he was engaged."*

The importance of the CEO emerged again at the meeting. A member contrasted two companies in the same industry whose CEOs had differing approaches and styles: *"The CEO at one company was a bit of a risk-taker. His approach to risk put the company at risk. The CEO at the other company owned the process, in contrast. He took risk management seriously. He did the best job I've seen of really identifying big-ticket risk potentials. He got the company well positioned from a capital structure standpoint, which was a big risk in 2008–2009. As a result, the company weathered the downturn better than any other."*

Another member described how a company finally made progress on the difficult issue of cybersecurity by engaging the CEO: *"We weren't getting anywhere with cybersecurity. We still had intrusions, still lost data we shouldn't have. The CEO took charge and has a group of five people meeting with him monthly. They grind on this stuff and measure themselves against standards from the government and others. They come out with timelines and standards that are auditable, and they will be accountable. By that example, business leaders got the message."*

Assigning responsibility throughout the organization

While the involvement of the CEO is key, members also repeatedly stressed that responsibility and accountability for risks should extend throughout the organization. They noted that ERM ultimately has to be integrated into the business in such a way that the business itself is responsible. Under the "three lines of defense" approach to ERM advocated by the Institute of Internal Auditors (IIA) in a January 2013 position paper, the first line of defense is operational management, which is "responsible for maintaining effective

internal controls and for executing risk and control procedures on a day-to-day basis."[2] A member emphasized the importance of actively involving operational management as opposed to relying on directives developed by a separate risk function: *"We create all these processes and books, but we don't feel the lines of business are as involved as we'd like them to be. They're the ones that have to confront these crises, and they may not remember that there's a book back there on the shelf that tells you what to do."*

A small risk function can support and oversee the efforts of the business lines, ensuring that consistent risk management processes are in place across the organization. The risk function may include individuals devoted exclusively to risk areas that are especially important, as one member suggested: *"Touching the government is like touching the third rail … We hired an individual who concentrates on nothing but government contracts and compliance."*

Another member described the role that can be played by a chief risk officer (CRO) who assists the CEO in spearheading the overall effort: *"One thing that has been positive is the designation of a CRO. All that the individual does is look at risks across the business lines. It's different for different business lines and products, so it's about making sure that there truly is a focus on what needs to be looked at in each area."* This individual has a thorough understanding of ERM, but his or her expertise goes beyond risk: *"Whoever is driving the process has to have a deep understanding of the business in order to be credible with the business. It can't be someone who just has a risk background."*

Given the diversity of risks and their often-technical nature, one member noted that a good deal of attention must be paid to the capabilities of the staff in the risk management function, particularly the IT staff. The member said, *"There's a more detailed review today of how talent is matched against risks. What talent acquisitions do we need to focus on?"* The escalation of cybersecurity threats has been an especially strong driver of concerns about the technical expertise of the risk management function. Another member made a more general point about staffing and its fundamental importance for all aspects of risk management: *"You can set up a process, but it still depends on the people and how they behave."*

Leveraging internal audit

Members mentioned a role for internal audit in both implementing and assessing the ERM process. Internal audit can be a useful source of information about risks and risk mitigation and an important component of the ERM process. At the same time, the auditing capabilities of internal audit can be brought to bear on the assessment of the ERM process itself, even providing formal assurance on its integrity.

However, members also highlighted a dilemma stemming from these two roles. As a member noted in a pre-meeting conversation, *"There has been a lot of confusion regarding the role of internal audit … Internal audit is often on both sides of the line, a provider of information and also an auditor."* The member noted that a dual role could compromise the objectivity of internal audit in its assurance role. At the meeting, other members agreed: *"You can't audit your own work. It may be that internal audit has a skill set to help establish a better process, but eventually it needs to extract itself. One problem is that they get looked to as*

[2] Institute of Internal Auditors, The Three Lines of Defense in Effective Risk Management and Control (Altamonte Springs, FL: Institute of Internal Auditors, 2013), 3.

the owner, and that needs to change. They can't be the third line of defense – the backstop – if they are the first- and second-line executors as well." Under the IIA's "three lines of defense" approach, the auditing role of internal audit is indeed situated in the third line of defense, independent assurance,[3] though there has been debate recently about whether that role necessarily precludes participation in the second line, the risk function.[4]

Tools and techniques

Previous ACLN discussions of ERM practices identified measures such as surveys of both internal and external stakeholders, scenario planning, and methods of promulgating the company's culture to overseas staff.[5] Some of these measures also came up in the conversations associated with the March 2015 meeting, as ACLN members described several approaches that their companies found useful for identifying risks and crafting the right responses to them:

- Running desktop exercises
- Using data analytics and company surveys
- Factoring in risk appetite

Running desktop exercises

One member said, *"I believe strongly in desktop exercises. You take a couple of significant risks and create a real-life exercise for each of them … It's role playing with real people, not just consultants, and it helps you think through who would do what … We came up with where steps were missed – it's very powerful, if done well."* The member noted, *"Complacency in companies is the biggest enemy. Issues only come to the fore in real crises or simulated crises."*

Managers who have found value in desktop exercises, also known as tabletop exercises, noted that such exercises can be an economical way of exploring real-life scenarios and identifying weaknesses in how a company would respond.[6] A recent article about using desktop exercises to analyze responses to security incidents offered a number of tips from security managers, such as communicating the objectives and scope of the exercise clearly to participants, using guidance from industry groups and the government, and making the scenario as realistic as possible.[7]

Injecting realism into a scenario can be challenging if the company has never experienced anything like the event in question, yet companies may want to understand certain unlikely but potentially devastating scenarios. One member described a variant of scenario analysis that is designed to explore such possibilities: *"We take a huge event, like a huge earthquake in 1989, and put it in a scenario for today. What would be*

---

[3] Ibid.

[4] See, for instance, Institute of Internal Auditors Netherlands, *Combining Internal Audit and Second Line of Defense Functions?* (Naarden, the Netherlands: Institute of Internal Auditors Netherlands, 2014).

[5] Audit Committee Leadership Network, *Leading Risk Management Practices,* ViewPoints (Waltham, MA: Tapestry Networks, 2009).

[6] Bob Violino, "6 Tips for Effective Security Tabletop Testing," *CSO Online,* October 27, 2014.

[7] Ibid.

the impact of such an event today? We have data on the impact at the time, and we build a scenario based on that."

Using data analytics and company surveys

Advanced data analytics, including tools for analyzing the vast and dynamic aggregations of data known as "big data," are beginning to gain traction. One member said, *"There is a lot more use of big data by the internal audit group. They have hired experts to use big data to find problems."* A survey by EY on the use of forensic data analytics to manage the risks of fraud, bribery, and corruption found that companies using techniques going beyond spreadsheets and databases reported significant benefits, such as improved results and recoveries (11% more than others) and earlier detection of misconduct (15% more than others).[8]

At the same time, the survey suggested that companies are still early in the process of adopting more advanced tools. Only a minority use tools such as forensic analytics software (26%), visualization and reporting applications (12%), statistical analysis software (11%), and big-data technologies (2%).[9] The report on the survey concludes that many companies are "missing important opportunities to leverage more sophisticated tools."[10] In a pre-meeting conversation, Matt Polak, a partner with Ernst & Young LLP and an expert on risk management, noted that US companies also do not utilize the technologies available to them for risk management more broadly.

However, companies continue to gather and analyze data on risks in systematic ways, a practice that ACLN members discussed at length in a 2009 meeting on ERM practices.[11] In advance of the March 2015 meeting, a member described how his company regularly undertakes a formal survey to prioritize risks: *"The company takes a survey of 250 officers in all areas across the company – out in the field, in finance, in IT, etc. Not all are at headquarters; they are selected across sectors. They are asked to identify what risks they have and what risks the whole company faces. Then we slice and dice and, among the many risks, find the 20 most mentioned. We try to say which were the 5, 10, 15 highest risks. And from the people out in the field, what were the 5 highest."*

The breadth and depth of the survey builds confidence that all important risks have been flagged: *"I now have a comfort level that through these surveys, the issue has been raised and the hard questions have been asked. It keeps us from overreacting. We take things very calmly … knowing what your true risks are and how to respond – knowing the bigger picture. Let the people throughout the system let you know."*

Factoring in risk appetite

ACLN members also argued that the ERM system must take into account the company's risk appetite, underscoring the fact that risk is an unavoidable element of business strategy. Risk management is not just about avoiding risk but about helping the company take certain risks, through both mitigation of risk and

[8] EY, *Big Risks Require Big Data Thinking: Global Forensic Data Analytics Survey 2014* (London: EYGM Limited, 2014), 4.
[9] Ibid., 3.
[10] Ibid., 1.
[11] Audit Committee Leadership Network, *Leading Risk Management Practices.*

assessment of residual risk against the company's risk appetite.[12] One member explained, *"Risk has a negative connotation, but risk management forces you to look at it both ways. Why have risk? To seize opportunity. [At one of my companies], risk management has a heat map that shows opportunities and not just reds and greens. As they establish the budget, they say, 'Here are all the risks, but here are these opportunities that can make up for these risks.'"*

A member noted that after the leadership of the company has established the company's risk appetite, it becomes the anchor for the ERM system: *"The executive management then has to take that risk appetite and set out all the controls and the operational budget and drive the culture to operate within it. Then the operations people need to execute their business within those parameters. And then the internal audit and control groups need to make sure everyone stays within those parameters."*

Board and audit committee practices

ERM is a critical concern for boards and audit committees, and ACLN members highlighted five board practices that can improve oversight:

- Prioritizing risks
- Taking risk-related field trips to business units
- Utilizing deep dives on specific risks
- Establishing a risk committee or other committees that focus on a specific risk
- Balancing tenure and diversity

Prioritizing risks

While reflecting on the board's responsibility to address the risks faced by the company, some members noted that the board needs to help the CEO set priorities. A member said, *"We flailed at ERM for a long time because we had too many so-called enterprise risks. So we sat down with the CEO and asked, 'What are the risks that could have a material impact, that could blow the company up?' There weren't many. There is no one but the CEO who can set these priorities."* Another member pointed out that publicly disclosed risks cannot all be addressed by the board: *"There are going to be more things in the 10-K than the board is asking about and working on. If the board has a risk that it thinks is important, it better be in the 10-K … but it doesn't necessarily flow the other way around."*

This observation echoed the point made by ACLN and LDN members in 2013 that boards should focus on strategic risks, such as disruptive technologies and new business models that could pose an existential threat to the company, sometimes with little warning. In that meeting, members underscored the difficulty of spotting such risks but recommended that boards, like management, seek insights from a diversity of sources,

[12] Some critics have argued that the "three lines of defense" approach is too much about avoiding risk and not enough about taking appropriate risks. See Joe Mont, "What Critics Say on Three Lines of Defense," *Compliance Week,* February 10, 2015.

including technology innovators, entrepreneurs, younger employees, and other "possible dissenters from the company's established strategy."[13]

Reflecting on how difficult it can be to spot a strategic risk, one member brought up the example of supply chain risks: *"We had a flood in Thailand that wiped out a supplier to our supplier. We thought we were okay because our supplier was in China, but its suppliers were not. You need to audit critical components of suppliers' suppliers."* EY's Matt Polak noted that it is easier to focus on strategic risks if the company has adopted efficient processes and technologies that reduce the cost and effort spent on preventable or compliance risks.

Taking risk-related field trips to business units

A member noted how helpful it has been to get the members of the board out into the business: *"We have board members go visit a site, and we construct it as an ERM visit. At the site, it's the business leaders – no CEO, no CFO, no general counsel. It's the board members meeting with business leaders and their reports to talk about risk in the business and the mitigation strategy. We follow up with a town hall meeting of employees."*

The member elaborated on the benefits: *"It lets them know we care, and it helped us to hear directly from them about risk and how they are addressing it. For five years we did it, and then we asked if we should continue. The answer was, 'This has been very helpful for employees and engagement.' We did away with one board meeting and made this mandatory."*

Other members also brought up the relationship with people in the business. A member said, *"As a board member, you need to get really comfortable with people and skills. You do that by interacting with them and challenging them in a constructive way and spending time with people."* If there is an incident, line management can be summoned to the audit committee. Getting closer to the business may be a way of ameliorating a problem observed by EY's Matt Polak: a gap between what the board wants to know and what management communicates.

For audit chairs, as one member explained, it is also about evaluating when an issue is serious enough to escalate: *"I like to have low-key questions and conversation with management and key operations people – have they heard about this, is this an issue? It's about getting yourself comfortable with an issue and how it is handled before taking it to the other board members."*

Utilizing deep dives on specific risks

Several members mentioned that their audit committees and boards conduct in-depth sessions on specific risks. One member said, *"We routinely have risk management deep dives, allocating time on our agenda. We bring in outside experts. It's open to any board member. It allocates time and brain power to focus on that area and allows us to see if we are falling behind."* Members noted that deep dives are often planned out at the beginning of the year, and while some audit committees do one or two of them per year, others carve out time for deep dives in every meeting.

[13] Audit Committee Leadership Network, *Risk Oversight,* ViewPoints (Waltham, MA: Tapestry Networks, 2013), 3.

While conferring with the individuals in management responsible for specific risks is likely to be an element of these deep dives, several members also mentioned using outside experts to provide fresh insight and deep knowledge in specific areas. Outside experts can also assist with in-depth evaluations of the ERM system as a whole. One member reported, *"Every few years, we bring in external advisers to evaluate how ERM is doing. The auditor looks at it, too. Are we best in class?"* Another member said some of the outside input came in the form of benchmarking against other companies on whose boards the member serves.

Establishing a risk committee or other committees that focus on a specific risk

The New York Stock Exchange listing requirements state that the audit committee should "discuss policies with respect to risk assessment and risk management."[14] While this suggests that the audit committee must ensure that an ERM process is in place and that responsibility for various risk areas has been assigned, it is generally not interpreted to mean that the audit committee is responsible for all risk oversight. ACLN members have often discussed how the responsibility for oversight can be distributed among several committees and the full board.

A few members said that the responsibility for overseeing risk management ultimately led their boards to establish separate risk committees. In a pre-meeting conversation, one said, *"We spun off risk to a new committee because it was so time consuming."* Board risk committees are still rare outside of financial services and other regulated sectors, but some observers believe factors such as the current wave of cyberattacks and the comment by Securities and Exchange commissioner Luis Aguilar on the helpfulness of risk committees may lead to an upswing in their creation.[15]

However, not all risk committees will be called risk committees, especially if they focus on a particular category of risk, such as environmental or compliance risk. A member remarked, *"To balance the workload, we don't have a risk committee, but we have a compliance committee that really handles the risk. In another company, we shifted the load to the governance committee by making it the governance and compliance committee."*

One member noted that the need for risk committees might be a reflection of the challenges boards are facing during the transition to better ERM: *"I like to think that over a number of years, there won't be a need for risk committees because the processes will have matured to the point where they are not needed."*

Balancing tenure and diversity

ACLN members also touched on the issue of board composition as a factor in risk oversight, including the question of when long-standing board members should be ushered off the board to make room for new members with fresh perspectives. Among S&P 500 companies, the average director tenure is 8.4 years.[16]

---

[14] New York Stock Exchange, "Audit Committee Additional Requirements," in *Listed Company Manual* (New York: NYSE Euronext, 2011), 303A.07.

[15] Priya Cherian Huskins, "New Kid on the Block: The Risk Committee," *InsideCounsel,* November 1, 2014.

[16] Spencer Stuart, *Spencer Stuart U.S. Board Index 2014* (Chicago, IL: Spencer Stuart, 2014), 5.

Some institutional investors, including State Street Global Advisors, have adopted policies that address average board tenure relative to peers to test board independence.[17]

Members tended to be skeptical of term or age limits: *"Leveraging talent is not about a formula."* One member supported the idea of monitoring average tenure, thereby allowing some flexibility in terms of departures. One member argued, *"In a company as big and complicated as ours, there is a real advantage to having a subset of board members who know what they are doing, who have been around awhile. There needs to be change on the board, but we also need to keep experience on the board."* Another member said, *"You can't tell if [a board member] is good or bad just on the basis of age or time on the board."*

Another member said that the issue was ultimately the responsibility of the board chair. As in previous discussions of board composition, members mentioned the use of a skills matrix to assess the board and its needs.

Conclusion

ACLN members have seen progress on risk management over the last several years. One member said, *"In general, it's something I feel much better about in all my companies than in the past. Six to eight years ago, I felt I was a voice in the wilderness. Everyone takes this more seriously now. You don't have to worry about getting anyone's attention anymore."* At the same time, members see room for improvement in many areas. Involving the CEO more closely can have a huge impact, though risk management should ultimately be embedded in the operational management of the various business lines. Desktop exercises, data analytics, and surveys can help identify risks and evaluate response plans, but some risk taking is desirable, and ERM should always take that into account.

The board can play a critical role in guiding the ERM system, especially if it can help the CEO focus on the most important risks, interact directly with those who are managing risks, and delegate responsibilities across board committees effectively. The experience of board members is an important asset. One member concluded, *"This is an area where directors can be the most helpful to companies because we do see this across a range of companies. CEOs often want to do the right thing but don't always know what to do."*

About this document

The Audit Committee Leadership Network is a group of audit committee chairs drawn from leading North American companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is organized and led by Tapestry Networks with the support of EY as part of its continuing commitment to board effectiveness and good governance.

ViewPoints 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 *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

[17] Rakhi Kumar, "Board Refreshment and Director Succession in Investee Companies," *Harvard Law School Forum on Corporate Governance and Financial Regulation* (blog), May 25, 2014.

Appendix 1: Participants

Members participating in all or part of the meeting sit on the boards of 45 public companies:

- Aldo Cardoso, Audit Committee Chair, GDF Suez*
- Tim Flynn, Audit Committee Chair, Wal-Mart Stores
- Raj Gupta, Audit Committee Chair, Hewlett-Packard Company
- Dick Harrington, Audit Committee Chair, Aetna and Xerox
- Michele Hooper, Audit Committee Chair, PPG Industries
- Olivia Kirtley, Audit Committee Chair, U.S. Bancorp
- Mike Losh, Audit Committee Chair, Aon and TRW Automotive
- Heidi Miller, Audit Committee Chair, General Mills
- Guylaine Saucier, Audit Committee Chair, Wendel*
- Tom Schoewe, Audit Committee Chair, General Motors
- Sandy Warner, Audit Committee Chair, General Electric Company

EY was represented by:

- David Kane, Americas Vice Chair of Professional Practice
- Frank Mahoney, Americas Vice Chair of Assurance Services

* Member of the European Audit Committee Leadership Network

Appendix 2: Questions for audit committees

- How is your CEO driving risk management into the processes used to run the business?
- Is line management accountable for ERM, or has responsibility been shifted to a staff function?
- How is your company prioritizing risks and treating them differently based upon the necessary response?
- Who should lead the ERM function? What are the advantages and disadvantages of having a dedicated CRO? What is the CEO's role?
- How should internal audit be utilized? How can conflicts involving its assurance role be resolved?
- What staffing challenges does ERM entail? Has ERM changed the way your company hires?
- Has your company introduced any other new ERM practices in recent years? What are some challenges that might be addressed with new tools or techniques?
- If your company has run desktop exercises to test its response capabilities, what factors make such exercises more helpful?
- If your company has used surveys to identify and prioritize risks, what kinds of surveys have worked well?
- How much is your company using advanced data analytics for ERM, including tools for analyzing big data?
- How are the issues of strategy and risk appetite integrated into risk management?
- What new practices has your board and/or audit committee introduced to improve or facilitate the oversight of ERM? What are the biggest challenges for the board in overseeing ERM?
- How does your board decide what risks to focus on? How are strategic risks identified?
- Does your board visit business units to get a better sense of how risks are being managed? What other practices can provide more information about the business to the board?
- How does your board drill down on specific risks? What kind of outside experts do you bring in?
- What changes (e.g., establishing a dedicated risk committee) has your board made recently in how it allocates responsibility for risk oversight?
- In what ways is risk oversight a consideration when reviewing board composition?