European Audit Committee Leadership Network

March 2019

EACLN

VIEWPOINTS

Board oversight of risk

Enterprise risk management (ERM) has seen a renaissance in the last 10 years, driven first by the financial crisis and then by mounting concerns over issues such as cybersecurity, privacy, and fraud. In response to demands from investors, regulators, and other stakeholders, companies and boards have strengthened their focus on the processes used to identify and mitigate the wide array of risks.

According to members of the European Audit Committee Leadership Network (EACLN), ERM systems are now considerably more mature than they were before the financial crisis. Yet they see room for improvement, especially in the board's oversight of risk, and they are asking questions that continue to defy easy answers. For example, how should responsibility for overseeing risk be allocated among the board and its committees? How can emerging risks be spotted before they seriously threaten a company? How can the board ensure that risks are being managed effectively and in accordance with the company's risk appetite?

Executive summary

On 5 February 2019, members of the EACLN met in London to discuss aspects of risk oversight that continue to challenge boards and audit committees:[1]

- **Which committee should take the lead?** *(page 2)*

  Most EACLN members, especially those on boards in industries other than financial services, reported that their audit committees are responsible for the risk oversight process. The audit committee also typically oversees some subset of specific risks, delegating the rest to appropriate committees. However, members acknowledged the benefits of a dedicated risk committee that can focus its time and effort on the complexities of risk oversight.

- **How can the board enhance the risk identification and prioritization process?** *(page 4)*

  Members reported extensive interactions with senior members of management to identify and prioritize risks. They mentioned the use of dashboards or risk maps as a way of assessing and comparing risks in a systematic way. They also noted that field trips to business units can be helpful for understanding risks. To avoid being surprised by significant emerging risks, members also suggested more imaginative scenario planning, including stress testing.

- **How are key risks managed?** *(page 6)*

  Boards review how key risks are managed, interacting with all three lines of defense—the business units, the risk management function, and internal audit. While they see value in keeping these lines separate, they acknowledged that a strict separation is not always

enforced. They also see room for improvement in the articulation and application of the company's risk appetite to determine if residual risks are acceptable. Even financial services companies sometimes struggle to specify their risk appetite for operational risks, though they tend to be further along in applying the concept of risk appetite.

For a list of members attending, see Appendix 1, on page 9. For a list of discussion questions for audit committees, see Appendix 2, on page 10.

Which committee should take the lead?

Risk oversight activities—identifying risks, assessing their probability, tracking them, mitigating their impact, and assessing whether residual risks are compatible with the organization's risk appetite—permeate the entire enterprise. Effective oversight thus requires substantial board activity, including interactions with management and thorough assessments of the company's approach. This raises the question of how risk oversight responsibilities can best be allocated among the board and its committees.

While the full board is ultimately responsible for risk oversight, especially at the strategic level, board committees typically lead the risk oversight process and supervise efforts related to specific risks. In the financial services sector, regulators in many jurisdictions require boards to have a separate risk committee to ensure adequate attention. In the EU, for example, the Capital Requirements Directive IV requires that larger, more complex financial institutions separate the audit and risk committees.[2] In other sectors, corporate governance guidelines and stock exchange listing requirements often assign risk oversight to the audit committee, but they may permit a board to establish a risk committee instead.[3]

Most EACLN members, especially those on boards in industries other than financial services, reported that their audit committees are responsible for the risk oversight process, and they discussed how this arrangement typically works. However, they also considered the benefits of having a risk committee, even absent a regulatory requirement.

The audit committee as the leader

When the audit committee is responsible for risk oversight, EACLN members said, it typically oversees both the company's overall process and some subset of specific risks. One member explained: *"The oversight process resides with the audit committee, in terms of risk management, internal controls, and internal audit. We map the risks, look at mitigation, prioritize risks, etc. Then, at the end of the process, we allocate risks among committees. Not surprisingly, about 50% of risks that would have an important financial impact, including operational risks, stay with the audit committee, but the others go to other committees such as human resources or sustainability."*

Another member described a similar process and added, *"We delegate, and then they follow the risks on a day-by-day basis and come to the audit committee for the final review."* In all circumstances, the full board is kept informed: *"The most important issues are brought to the board at least once a year."* One member saw room for improvement in the interactions among committees and the full board: *"I'm not satisfied with the way it's reported back to the audit committee or to the full board. Each committee is responsible, but they don't report."*

Some members also warned that, as the audit committee assumes more responsibility for risk oversight, it may take on risks that it is less well-equipped to handle than those related to financial reporting and internal controls. Without a clear and explicit understanding on the board regarding the scope of the audit committee's responsibilities, this scope can easily grow broader and broader.

The risk committee as an alternative

In financial institutions and some other companies, boards have established separate risk committees to deal with the growing burden of risk oversight. A 2018 Spencer Stuart survey of the largest 150 companies in the Financial Times Stock Exchange rankings, for example, found that 19.3% of boards had a separate risk committee, with more than 85% of these in financial services.[4]

Experts point to several advantages of having a dedicated risk committee.[5] A risk committee can focus all its time and effort on the complexities of risk oversight, and it can be composed of members with expertise in risk management. Such a committee may be able to go much deeper in its oversight. Separating risk committees and audit committees is an approach that acknowledges the importance of and distinction between risk management and financial reporting.

EACLN members acknowledged these benefits. One member said, *"I'm going to advocate that big companies have a risk committee and nominate members with a background to work on it."* Another member agreed and suggested that the audit committee's typical relationships and resources might not be sufficient for risk oversight: *"The audit committee doesn't have risk experts reporting to us or external audit helping us assess risk somewhere. The CFO is different than the risk organization, and internal audit looks at institutional control."*

Yet the audit committee's core duties may also present challenges for separating risk oversight and assigning it to a different committee. One reason the audit committee is often seen as the home for risk oversight is that there are tight interlinkages between risk oversight and the audit committee's work. As a member noted in a pre-meeting conversation, *"There is a risk of overlap between the risk committee and the audit committee. Mitigation is about strategy and controls, which is what the audit committee does. Yet the risk committee looks at risk mitigation. You need to ensure that topics are properly shared."* Another member remarked, *"The audit committee has a big influence on how risk is handled, even if it's not formally allocated to it."*

A member explained in more detail how one board addressed this overlap: *"The way the risk committee and I [as audit chair] articulated it is that the risk committee is responsible for understanding the inherent risk in an area, seeing what level of residual risk we will tolerate, and understanding the mitigation we need. The audit committee's responsibility is to dig into whether the design of the controls is effective and to ask whether those controls have been implemented and are working. If not, the audit committee has to let the risk committee know so they can decide if the residual is acceptable or has to be fixed."* Another member summed it up: *"The risk committee focuses on outcomes, and the audit committee focuses on controls. We manage the overlap by having some members sit on both committees."*

The need for expertise

EACLN members raised the question of whether there is enough risk expertise on the board and the committees assigned to oversee risk. For some members, the answer is clear: more expertise is needed, particularly in certain challenging areas of risk management. *"Let's be frank,"* one member said. *"When you talk about risk appetite, board members' eyes get huge. They don't have the background."*

Audit committees that take the lead on risk oversight must balance risk-related skills against the skills required for the committee's other duties. One member said, *"I'm curious about committee skills— audit is a very demanding committee. The ability to engage is highly important … There is a question about the capability."*

Members observed that risk committees, especially in financial services companies, seek directors with specialized skills and experience in risk management; in fact, regulators may criticize a financial services firm if its risk committee members lack a technical risk background. One recalled asking, *"How are you qualified to manage some of these risks? Do you have detailed modeling experience, for example?"*

How can the board enhance the risk identification and prioritization process?

A critical aspect of risk oversight is identifying the most important risks and prioritizing the company's risk mitigation efforts. Given the multitude of risks any company faces, the board cannot discuss all of them. EACLN members described the processes by which management and the board, working together, determine the most significant risks to the company.

Interactions with management

Members reported extensive interaction with senior members of management to discuss and prioritize risks. One said, *"We have a chief risk officer with a dedicated team, including actuaries and top-level people. We have them in to the board four or five times a year, and we have decided on a dashboard with assessments of the top risks."* Another member said, *"We have meetings with the head of internal audit five or six times a year."*

Several members at the meeting pointed out that examining indiscriminate or random aggregations of risks will not suffice. One member explained, *"In my view, the company has to have a framework of some sort. You can't just pick risks here or there. You have to have a framework that brings the risks to you, so that there is proper risk identification in a measured fashion."*

Members elaborated on the use of dashboards or risk maps as a way of comparing risks in a systematic way. One said, *"Basically, the committee at least once a year does a risk map. One of the things that I always complain about is that it's hard to go through all the risks. It takes a*

year, so I ask once a quarter for an update." Another reported, *"The audit committee spends a full session to review in detail the risk map. And then there is a presentation to the board of the same map, but we take 15–20 minutes reviewing it there."*

One member mentioned assessing the accuracy of the risk map retroactively: *"We've had risk maps for five or six years, but I've now asked for back testing. Over the last five years, have the risks on the map occurred? If yes, why? If not, why? The result was that the high-probability risks did occur, which demonstrated that the risk map was correct. However, another risk had not been captured in the risk map."*

Members also talked about going beyond reliance on senior management by venturing out across the company and its operations. *"One great mechanism is site visits, where you visit certain subsidiaries. There's a more casual atmosphere, and a lot comes out. It's about getting people away from the board table,"* a member said. In previous conversations about risk oversight, audit chairs in other networks have recommended field trips to business units as an excellent way of learning about the company's risks and building relationships with those in charge of managing them.[6]

The challenge of emerging risks

New—and potentially surprising—risks are always a concern, members noted, and the board needs to be sure that management is not ignoring or underestimating such risks, even if they are more speculative. *"Emerging risks are like other risks—they need to be identified, and people need to be made accountable. You can't just talk about them. The role of the audit committee or the board is to challenge management on whether new things are emerging,"* said one member. Another commented, *"We know we are going to lose a certain amount of money to fraud every year, but that's not the issue. That's just one element of operational risk. I think more about the events that haven't hit the company in the past but could cause substantial harm."* One member suggested that this approach might be new to some audit committees: *"As an audit committee, we are mostly backward looking. Risk assessment needs to be forward looking."*

Looking for lessons from the financial services sector, one member commented on the value of stress tests to help the board more fully appreciate systemic risks: *"The risk practices in financial services institutions may be moving into other industries. For example, do you reverse stress-test? What combination of factors would it take to break this business? I've found it hugely informative to help to identify risks that could really bring the business down."*

Members mentioned scenario planning more generally as a helpful tool, perhaps facilitated by outside experts. *"For tail risks, which are low probability but high impact, we are looking into scenario planning,"* one member said. *"You can't eliminate these risks, but you have to understand the potential impact. What's plan B?"* The member added that trying to identify these risks means going beyond routine exercises: *"It requires imagination. We are looking at a few scenarios, getting external help to think outside the box. You have to be creative but not outrageous."*

How are key risks managed?

Once the risks that the board should track are identified, boards can focus more closely on managing them. In a pre-meeting call, a member described one approach: *"We ask if there are risk owners, responsible parties. Are there mitigation plans in place in case the risk occurs? Is everything that must get done on track, or does the business need to remediate the plan? We figure out what needs to be solved, and we have a dashboard of things we have to solve, things that need action."*

At the meeting, a member described a similar process: *"We have to ensure to the full board that they can trust in the underlying process that risks are identified in a structured way, that we've got mitigation of risks, that plans are happening, and it's all been documented and followed up on."*

Deeper dives on some risks may be necessary. *"We decided that one of the audit committee members, the former deputy CEO of a company, and I would do a deep dive,"* a member said. Such deep dives may involve more extended discussions with managers responsible for specific risks. Discussions with internal audit are helpful, too. In some cases, outside experts are brought in to provide fresh perspectives and additional knowledge, including benchmarks based on other companies' experiences.[7] *"Since risks are very polymorphic, I think that entails different solutions given the various kinds of risks,"* a member noted.

Coordinating with all three lines of defense

Members also discussed the board's relationships with the different functions within the company responsible for providing three lines of defense. Under this framework, the first line of defense is the business units, which own and manage the risks during the course of their day-to-day operations. The second line is the risk management function itself, which develops and promulgates consistent policies and practices across the company. Finally, the third line is internal audit, which provides independent assurance that the two other lines are performing as required.

Members mentioned the value of a separate risk function that provides the board with an integrated, holistic view of risk management efforts. They like hearing from a dedicated chief risk officer (CRO) who can spot trends across the organization and provide a consolidated view. At the same time, members said it is essential for the board to hear from the executives who actually own the company's most critical risks. And some members noted that a robust second line is not ubiquitous yet: *"Outside of financial services, I've had limited experiences with true second lines of defense, i.e., an independent function that challenges management. They haven't been required to do so."*

Some members felt that it was best to keep the third line, internal audit, separate from the other lines, despite the temptation to leverage its expertise and resources more directly. One explained, *"There used to be a mind-set that internal audit does a lot with risk management. Now that businesses are more mature, we know risk management should be embedded in the management [of the business]. It's clear that risk management has nothing to do with internal audit, which is supposed to be your internal assurer, and there would definitely be a conflict of*

interest [if it were involved]." However, a clear separation is not always enforced, as was clear from one member's description: *"When the CRO identifies risks, he informs internal audit. Now internal audit and risk are integrated and report to the same executive."*

Linking with risk appetite

Understanding the risks, the mitigation plans, and ultimately the residual risk leads to another thorny question: Is the residual risk acceptable? Does it match the level of risk the company is willing and able to take—in other words, the company's risk appetite? *"There needs to be a decision by the board about its risk appetite for key risks. For non–financial services boards, this is often a more generic approach. But every board needs to be explicit about its risk appetite,"* said one member.

One member noted in advance of the meeting that when it comes to incorporating risk appetite, *"industrial companies are far behind financial institutions."* This member continued, *"The financial companies I worked for clearly had a definition of risk appetite which considered correlations between major risks. In my industrial company, there is no definition of risk appetite or a computation of the correlation between the 15 to 20 top risks."* Determining how various risks might be correlated is critical for calculating their aggregate impact—the impact if multiple risks materialize simultaneously—which is in turn necessary for understanding how the company's risk profile compares with its overall risk appetite.

Yet calculating and comparing certain kinds of risks is difficult because some are more quantifiable than others. Members noted that it is much harder for companies to calculate the impact of an operational risk (such as a storm that shuts down a major supplier) with the kind of specificity that is possible with a financial risk (such as a credit risk for which data is readily available). *"I still think that even in financial services risk committees, they are only just getting a grasp on operational risk,"* a member reflected. Another member has seen a variety of approaches to risk appetite within one company: *"I've found that every division does great things, but differently. We need a more uniform approach to risk appetite. I'd like guidance and brainstorming, and there's work to be done everywhere."*

Other members suggested that a key aspect of risk appetite—the choice to accept a certain level of risk rather than just minimize the risk—rarely comes into play. One observed, *"The focus has been on identification and mitigation, not so much residual risk. The task is always to drive that risk downward. Considering whether to accept more or less risk would mean sometimes accepting more. The board is more focused on whether there is a solid mitigation plan and that it's working."*

At the same time, members asserted that some risks should in fact be driven to zero. *"For some compliance issues, the board needs to declare that there is zero tolerance,"* said one member, citing money laundering and food safety as examples.

Conclusion

Despite the increasing maturity of ERM and its oversight, EACLN members identified several aspects of the board's role in risk management that could be improved. In some areas, lessons from the financial services sector are applicable. For example, while most members reported

that the audit committee takes the lead on risk oversight, they recognized the benefits of a separate risk committee, especially if the two committees coordinate their responsibilities effectively.

Identification of risks, including emerging risks, remains an important challenge. To tackle the task, members engage in extensive interactions with multiple levels of management and employ dashboards and even stress tests similar to those used by banks. In the area of risk mitigation, members see the value of regular board interaction with all three lines of defense. They also stressed a desire for a clearly articulated concept of risk appetite, but they acknowledged that in both these areas, industrial companies still lag their financial counterparts.

About this document

The European Audit Committee Leadership Network is a group of audit committee chairs drawn from leading European 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.

Appendix 1: List of participants

EACLN members and alumni participating in all or part of the meeting included the following:

- Mike Ashley, Barclays
- Aldo Cardoso, Bureau Veritas
- Carolyn Dittmeier, Generali
- Eric Elzvik, Ericsson
- Edgar Ernst, TUI
- Renato Fassbind, Nestlé and Swiss Re
- Byron Grote, Tesco, Akzo Nobel and Anglo American
- Liz Hewitt, Novo Nordisk
- Arne Karlsson, Mærsk
- Dagmar Kollmann, Deutsche Telekom
- Helman le Pas de Sécheval, Bouygues
- Richard Meddings, Deutsche Bank
- David Meline, ABB
- Marie-José Nadeau, ENGIE
- Erhard Schipporeit, SAP and RWE
- Carla Smits-Nusteling, Nokia
- François Thomazeau, Bolloré
- Isabel Torremocha, Repsol

EY was represented in all or part of the meeting by the following:

- Hywel Ball, Managing Partner, Assurance, United Kingdom and Ireland
- Andrew Hobbs, Partner, Europe, the Middle East, India, and Africa (EMEIA) Public Policy Leader
- Jean-Yves Jégourel, EMEIA Assurance Leader

Appendix 2: Discussion questions for audit committees

- ? Which committee on your board takes the lead on risk oversight? Has your board considered a dedicated risk committee? Why or why not?
- ? How are different risks delegated among various committees and the full board? How are excessive overlaps or gaps avoided?
- ? How is director expertise in the area of risk taken into account when staffing committees or selecting new directors for the board?
- ? What is the board's role in identifying and assessing risks? What methods does the board use to assist the company with this crucial aspect of risk management?
- ? How does the board approach the problem of unexpected risks? What techniques are used to identify them? Have preparations been made to deal with a significant event that has not been identified in advance?
- ? What sorts of outside experts are helpful in risk identification and assessment? In what ways can they help?
- ? How do the board and its committees interact with management to understand how key risks are mitigated? Who meets with the board, and how often?
- ? How are dashboards, risk maps, and other tools used to enhance the board's understanding? What kind of reports does the board get from management?
- ? How is the assessment of risk identification and mitigation linked to the company's risk appetite? How does the board weigh in on risk appetite?

Endnotes

[1] The European Audit Committee Leadership Networks comprise audit committee chairs of leading global public companies with over $10 billion in revenue. This document 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.

[2] European Parliament and Council of the European Union, "Directive 2013/36/EU of the European Parliament and of the Council on Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms, Amending Directive 2002/87/EC and Repealing Directives 2006/48/EC and 2006/49/EC," *Official Journal of the European Union,* June 27, 2013, 379.

[3] Financial Reporting Council, *The UK Corporate Governance Code* (London: Financial Reporting Council, 2018), 10.

[4] Spencer Stuart, *2018 UK Spencer Stuart Board Index* (Chicago: Spencer Stuart, 2018), 35.

[5] See, for example, Protiviti, *Should the Board Have a Separate Risk Committee?* Board Perspectives: Risk Oversight (Menlo Park, CA: Protiviti, 2015).

[6] Audit Committee Leadership Network, *Leading Practices in Enterprise Risk Management*, ViewPoints (Waltham, MA: Tapestry Networks, 2015).

[7] Ibid., 7.