



*Article originally appeared in*

**POINT of VIEW**

A SPECIAL ISSUE FOCUSING ON TODAY'S BOARD & CEO AGENDA

# The growing role of the board in risk oversight

KEVIN M. CONNELLY, *Chicago*

CAROLYN C. EADIE, *London*

VALERIE R. HARPER, *Stamford*

The oversight of financial risk is a well-established responsibility of the board. But as recent crises faced by companies such as Toyota and BP show, boards today are being held accountable for an ever-more diverse range of risks that can include safety, environmental, technological, regulatory and reputational risks, among others.

To gain an insider's perspective on the evolving role of the board in risk oversight, Spencer Stuart recently conducted several confidential interviews with the audit and risk committee chairs of leading multinational corporations in the industrial, life sciences, banking and financial services sectors headquartered in Europe and the United States. These executives shared their insights on the board's role in risk oversight, the skills the board requires to fulfill that role effectively, the pros and cons of creating a separate risk committee, and the steps the board should take to enhance risk management throughout the organization. We also heard their views on the role of the chief risk officer and its relationship with the board of directors.

With this article, we are not attempting to provide definitive answers to all of the questions boards have about risk oversight, but to offer a firsthand view from the boardroom on how leading companies and their board directors are reassessing risk.

“Effective risk oversight is about courage — the courage of swimming against the tide when there’s momentum for something, whether it’s a new product or innovation or an M&A opportunity. And part of the courage is to accept that you’ll have false positives and will be engaged in a degree of apology, but you won’t be deterred.”

## Greater accountability

The directors agreed that the expectation that boards have a broader responsibility for risk oversight is not entirely new. It is instead a continuing trend that has merely attained greater prominence of late in the wake of the financial crisis and recent high-profile corporate missteps. In today’s digital society, these missteps are much more visible, are transmitted more quickly and are more likely to affect the personal reputations of board directors in a negative way.

“Twenty years ago, it was unthinkable that individual directors would be profiled the way they are today, with their curricula vitae scrutinized in the press if something went badly with an organization,” said one risk committee chair. “But today directors take a huge personal risk. Directors have to learn that they will be blamed for things that they didn’t have an earthly chance of preventing or diagnosing.”

Board directors are also confronted with a world in which the number and scale of risks they must examine have multiplied. In an increasingly global environment, this growing complexity of risk results from factors such as lengthening supply chains; expansion into emerging markets and the segmentation of existing ones; new regulations; more frequent joint ventures, mergers and acquisitions; and product lines of growing complexity and diversity.

## The board’s role: management or oversight?

In this complex environment, the directors we spoke with agree that risk can’t be managed from the board level, but only overseen. A key responsibility for the board, then, is to set the company’s risk appetite and culture. Taking risks — the right level and kind of risks — is critical to running a successful business. “I’m on the board of a reinsurance company,” said one director. “There, a very valuable distinction is drawn between the risks the company is in the business to manage and the risks it has to manage if it wants to stay in business.”

Once the board has decided upon the appropriate level of risk for its company, it should also communicate this risk appetite throughout the organization and oversee the creation of controls that keep the company operating within these established boundaries. “The board must set up a precise risk profile and risk tolerance, communicate it loudly and clearly to the business units, make sure that the business units remain within it, and see to it that the monitoring process captures any meaningful deviation from the profile and tolerance accurately and in a timely fashion,” said one audit and risk chair.

According to directors, this is best accomplished by ensuring that there is an ongoing review of risk performance across the different categories of risk (credit, market, operational and compliance) and across the business units. Regular assessment of the strength of existing risk management systems and contingency plans is also important, from the company’s accounting platforms to its technology, reporting and business continuity procedures.

The board cannot conduct these reviews itself, but is responsible for seeing that these review processes are in place. For example, one leading industrial company has a risk database that catalogs each of the 200 to 300 risks that have been

identified for the organization. Each risk is assigned to a front-line person who is responsible for mitigating, managing and watching that risk. The internal auditor who reports to the audit committee, in turn, accesses that system to prepare his risk-related reports and analysis to the board.

In addition to seeing that the risk appetite is identified, supervised and monitored, the board can also play a role in ensuring that employee incentives are designed to reinforce the established risk culture, as opposed to rewarding risks by individuals that fall outside the desired risk profile.

## Board skills for effective risk oversight

According to the directors we interviewed, the boards — and risk or audit committees — that are most effective at risk oversight possess a mix of skills. It is particularly helpful to have directors on the board who have a background in the company's industry. "It's very difficult to fully appreciate the risk management challenges a company faces without that understanding of the business," said one risk committee chair. "Risk is very different than leadership on the audit side, where it's primarily about financial reporting and financial controls — things that are to some extent generic across industries."

That being said, directors note that financial expertise is itself an important requirement in a board hoping to achieve effective risk oversight. For example, the audit chair of one multibillion-dollar industrial company explained that the value of his company's pension plan is equal to the company's market value, making financial risk an enormous component of the organization's risk portfolio.

### Risk oversight: A checklist for the board

- Define the company's risk appetite and culture.
- Make sure that risk expectations are communicated to the organization.
- Determine the appropriate risk oversight structure, including the role of the full board and audit committee and whether a dedicated risk committee is needed.
- Ensure that there is an ongoing review of risk performance across the risk categories (credit, market, operational and compliance) and across the business units.
- Make sure that the strength of risk management systems and contingency plans are assessed regularly.
- See that each risk is assigned to a front-line person who is responsible for mitigating, managing and monitoring that risk.
- Ensure that employee incentives are structured to support rather than undermine the risk profile.
- Consider the appropriate mix of board expertise: knowledge of the business, financial expertise, technical knowledge or outsider perspective.

Some directors argue that the addition of an outsider's perspective also can be important to help boards think about risk in a new way. "The board should include people who are capable of understanding the different dimensions of the business, but who come from another world, be it through adding someone from a public sector background or someone who has worked in other countries," said one risk and audit committee member. "There has to be a possibility of having a different sort of discussion on the board about risk from what you have on the management team."

Sometimes, it can be helpful if this diversity of perspective even extends to having board directors who may be viewed as counter to the company's prevailing culture. As one risk chair said, "Effective risk oversight is about courage — the courage of swimming against the tide when there's momentum for something, whether it's a new product or innovation or an M&A opportunity. And part of the courage is to accept that you'll have false positives and will be engaged in a degree of apology, but you won't be deterred."

The political difficulty of sustaining such a position is one reason many risk and audit chairs in the U.S. believe it is best to keep the board largely independent, with only one insider — the CEO — on the board. Those feeling this way believe that other insiders are compromised by their overall reluctance to have a difference of opinion with their CEO at the board level.

In some particularly complex businesses, however, the knowledge another internal executive can bring may be worth tolerating this dilemma. For example, in the pharmaceutical industry, the proliferation of biotech medicines has resulted in products that are becoming increasingly complicated to produce, with some pills containing more than 50 elements. To deal with the inherent complexity of the industry today, the board of one pharmaceutical company includes two directors with a science background in addition to three internal directors: the CEO, CFO and head of R&D.

Overall, effective risk oversight requires the board to have increased technical ability — in understanding the business and numbers as well as the stress tests and other measurement tools that can provide a fair picture of the company's major risks. "The trouble with risk oversight is that you have to up the intellectual stakes on the board to be able to do it," said one risk chair. "It can't be accomplished by a board in which the directors sit around and joke about all the confusing numbers that are brought to them."

## Risk versus audit

While risk oversight is a responsibility of all board directors and is handled in some companies at the full board level, it is typically owned by either the audit committee or a dedicated risk committee. And while the audit and risk committee approaches can both be effective, the nature of the organization and the kinds of risks the business faces can significantly influence which approach makes the most sense for a specific company.

"The more a business is dependent upon the proactive taking of risk in a dynamic way, the more likely it is to be better served by a risk committee separate from audit," said one director. "If the risk profile changes very infrequently and is

“ The trouble with risk oversight is that you have to up the intellectual stakes on the board to be able to do it. It can't be accomplished by a board in which the directors sit around and joke about all the confusing numbers that are brought to them. ”

essentially around strategic and operational considerations, I think it's plausible that an audit committee can handle that in addition to its regular duties."

Those who argue against separating risk oversight responsibility from the audit committee note that the internal control system that the audit committee provides must still deal with risk assessment even if a risk committee is formed. This can create a weak boundary between the two committees, a strong risk of overlap and the possibility that issues could fall between the cracks of the two committees. Those who favor a structure centered on a powerful, global audit committee also argue against the formation of a separate risk committee because it can dilute this power.

Even those directors who favor the oversight of risk by the audit committee acknowledge that it is a time-consuming task, however. One audit and risk chair from the banking industry argues that at least half of the audit committee's time should be devoted to risk monitoring. Another risk chair who favors keeping risk under the audit committee believes that separating the two committees can create a structural problem, but also admits that tackling every risk issue from the audit committee can mean day-long meetings for that committee.

As a result, one potential problem associated with keeping risk under the audit committee is the danger that risk will become a lower priority. "The problem is that so much of the audit committee's traditional agenda is time-sensitive," said one U.S. risk committee chair. "If you're going to oversee risk within audit, it requires discipline to ensure that the risk elements of the agenda do not become displaced due to the time constraints associated with quarterly earnings releases, 'Q' filings, Sarbanes-Oxley reviews and executive sessions."

For some companies, the extensive commitment already required by committee members just to fulfill traditional audit committee tasks may be the best argument for creating a separate risk committee. This is particularly the case for financial services companies, which are required by law in some countries to have a separate risk committee, and in some nations even to get regulator approval of the risk committee's composition. "For companies that are in the business of intermediating financial risk, I think it's very hard to argue that they wouldn't be well-served by having a separate risk committee, because the workload of the audit committee is already so overwhelming," said one risk chair for a financial services company.

## The role of the chief risk officer

As more boards create a separate risk committee to oversee enterprise risks, more organizations are also instituting a chief risk officer (CRO) role on the management team. While directors may disagree on whether the role is necessary, nearly all of the directors we spoke with believe that the appointment of a CRO should not influence the responsibilities of either the board or the CEO in regard to risk, though the CRO may help them in those tasks.

"It's easy for directors to sit there and look at dense pages of technical information, but that's not what boards are supposed to do," said one audit and risk committee member. "They're supposed to get their minds on the big questions and extract big messages, and that's where a good CRO can help. If you don't have analytical underpinning for these discussions, they are hot air. You've got to have both the intuitive and the analytical, and risk professionals help you hugely on the analytical side. The business judgment, imagination and life experience of the board members come into play on the intuitive side."

What the CRO should not do in many organizations is take on responsibility for risk management. "It's inconceivable to me that a CRO could handle the product and engineering complexity that we have," said the audit chair of one industrial manufacturer. "Responsibilities for those risks need to be embedded in the businesses, and if you're not going to listen to the employees in the trenches and hold them responsible for the risks they take, you will not have good risk management."

“ You’ve got to have both the intuitive and the analytical, and risk professionals help you hugely on the analytical side. The business judgment, imagination and life experience of the board members come into play on the intuitive side. ”

According to the same director, the CRO role is most effective when he or she instead is responsible for making sure that there is a risk management system in place in each business that includes effective risk-control mechanisms as well as information systems that flow up to senior management. According to another director, the CRO can also help shape the risk principles and policies of the company, determine analytics and methodologies to evaluate how much risk is being taken, track the capital risk capacity of the company, define who is responsible for managing the specific risks within the organization, and provide a framework for judging the effectiveness of risk-taking.

But while the CRO should have high visibility to the board and to the risk committee if there is one, the CRO does not function as the internal auditor does for the audit committee. Instead, as most directors we spoke with agree, the CRO is part of the management team, ultimately acting independently of the board and of the individual business units as the CEO’s highest-level representative on risk.

## A primary responsibility

The risk and audit committee chairs we spoke with agreed that risk oversight is one of the board’s most integral responsibilities. It is also one of the trickiest, since risk by its very nature can never be reduced to a science. Things that no one could have predicted do happen, and in those cases, the board’s role is to respond to the crisis in a sensitive, effective and comprehensive way.

But other risks are more predictable, and boards need the knowledge to determine the likelihood of risks, the impact if they occur and the company’s appetite for taking those risks relative to its ability to absorb those impacts. By defining the company’s risk appetite; ensuring that risk-taking is visible, appropriately monitored and evaluated throughout the organization; and creating employee incentives that support rather than undermine the selected risk profile, boards can largely fulfill their role in risk oversight. At the same time, following these steps can also help board directors mitigate their personal reputational risks associated with board service — and embrace the benefits of serving on the board of a world-class, well-governed organization.

### ABOUT THE AUTHORS

Kevin M. Connelly is chairman of Spencer Stuart and has client-facing responsibilities as a member of the Board Services, Financial Officer, Financial Services and Private Equity practices. Carolyn C. Eadie is chairman of Spencer Stuart U.K. and co-leads the Board Services Practice in Europe, the Middle East, Africa and India. Valerie R. Harper is a member of the Asset Management Practice and leads risk management initiatives across financial services. She oversees the firm’s East Coast region in the U.S. and serves as office manager for Stamford.

Additional interviews were conducted by James Colhoun, Carlo Corsi, Will Dawkins, Enzo de Angelis, Ollo den Tex, Duncan Reed, Bertrand Richard and Han van Halder.