

Rewriting the Textbook On Risk Oversight

By Henry R. Keizer



Henry R. Keizer is global head of audit, KPMG International, and U.S. vice chair-audit, KPMG LLP.

With risk moving to the top of the agenda for directors and senior management—and a distinct increase in the level of commitment to taking a fresh approach to dealing with risk—I believe the textbooks on risk oversight are being rewritten. It may take a long time—perhaps years—before risk oversight models are “perfected.”

In the meantime, we can learn a great deal from the ideas and practices being put to good use now. In our work with audit committees and directors around the country, I’m hearing emerging themes that strike me as being nearly universal in their application. And I believe that, taken as a whole, this powerful combination of insights can help every board get a better handle on risk.

First, be clear about the board’s oversight objectives. Before considering *how* the board should oversee the organization’s risk-management activities, it is helpful to consider the goals and objectives of this oversight effort. What should the board seek to accomplish in its risk oversight role? Clearly, the board needs to satisfy itself that:

- Management has a system in place to manage risk, and the system is appropriate given the company’s business model and strategy.

- The risk appetite inherent in the business model is appropriate.

- The “risk culture” of the organization is based on the principle that management of risk is essential to the successful execution of the company’s strategy.

- The risk-management system operates to inform the board of the major risks facing the company.

Work with management to understand and agree on the types of risk information the board requires.

A number of directors express concern that the quality of the information they receive about risk—and the company’s changing risk profile—sometimes hinders their oversight efforts. As one director said, “I’m not sure that we have a clear picture from management as to what the top five or ten risks to the business are.”

Some boards are setting aside time to work with management to define their information needs. For example, they are asking: What level of risk is inherent in the company’s strategy? What information does the board require about the top risks facing the business? What should be measured and how? What are management’s core risk assumptions? They are also rethinking the format of the information.

Visualization, through graphs and heat maps, can be particularly helpful in testing key risk assumptions and considering the impact of various worst-case scenarios.

Make sure the culture encourages directors to question, challenge, and test management.

Effective oversight requires that directors understand and rigorously test management’s core risk assumptions and assessments; yet some directors say this more dynamic interaction is too adversarial for their boardroom. Business leaders today must understand that we’ve reached an inflection point for corporate governance, and that effective oversight requires the exercise of healthy skepticism. Used appropriately, it’s an important tool for discovering facts, integrating disparate pieces of information, and understanding the company’s risk profile.

Bring the right people into the board’s conversations about risk.

Understanding the implications of the risk information that the board receives—and challenging management’s core risk assumptions when appropriate—requires a rigorous conversation about risk with the people who are knowl-

edgeable about the risks facing the company. Invite the CEO, CFO, chief risk officer (CRO), general counsel, auditors, and business unit leaders responsible for managing the risks—and perhaps the business leaders responsible for IT and human resources as well. And get input from third parties to test and validate management’s core risk assumptions and perceptions.

Focus on the tone at the top, culture, and incentives.

While a robust risk-management process is essential, it’s not enough; directors today are particularly sensitive to the risks that may be posed by the organization’s tone at the top, culture, and incentive structure. These “Capital R” risks, if unattended, may pose the greatest risk of all.

Enlist the chief risk officer to support the board.

We’re seeing more companies naming CROs or the equivalent role to provide senior-level leadership and support for risk management and, in particular, to manage the company’s risk-management processes.

The CRO probably doesn’t “own” specific risks; rather, the role typically is to manage the process and to monitor the upstream reporting processes for risk. The CRO monitors the risks that line and staff managers are dealing with and ensures that relevant information is communicated throughout the organization. Given these responsibilities, the CRO is in a unique position to support the board in its oversight of risk, particularly

in helping to define the types of risk information the board should receive and improving the quality of that information.

Ensure that the risk oversight responsibilities of the full board and its various committees are clear.

How the board delegates responsibility for risk oversight among the full board and its various standing committees is a question

Business leaders today must understand that we’ve reached an inflection point for corporate governance, and that effective oversight requires the exercise of healthy skepticism.

that continues to generate much debate. While I see companies taking various approaches, there appears to be a growing trend for the full board to have oversight responsibility for the company’s “top risks”—those that threaten the company’s strategy, business model, or existence.

The various standing committees tend to have oversight responsibility for the specific risks inherent within their areas of oversight. For example, the audit committee has responsibility to oversee financial reporting risks.

Other boards (of banks, for example) have formed risk committees; and some, it seems, rely on the audit committee to oversee “risk.” Boards are taking different approaches, but I believe a key question for every board is

whether any single committee—such as the audit committee, or even the full board—has the time, resources, and expertise to effectively oversee the full range of risks that the company faces.

Also, consider delegating oversight of the organization’s risk-management system—including management’s processes for identifying, assessing, mitigating, and communicating

about risks—to a standing committee of the board.

The effectiveness of all of these approaches hinges, of course, on directors having a solid understanding of the company and its business and industry. Directors must also stay abreast of the issues and developments affecting the company.

Indeed, the ability—and willingness—of directors to ask that second and third follow-up question about a risk, or about the risk-management process, is a vital sign of how healthy the board’s risk conversations are—and how firm a handle it has on risk oversight. **D**

For information on reprints and editorial permissions, email info@directorship.com or visit www.directorship.com.

Strengthening Risk Oversight

- Be clear about the board’s oversight objectives.
- Work with management to agree on the types of risk information the board requires.
- Ensure that the culture encourages directors to question, challenge, and test management.
- Invite the right people to the board’s conversations about risk.
- Focus on tone at the top, culture, and incentives.
- Enlist the CRO to support the board in its oversight of risk.
- Ensure that risk-oversight responsibilities of the full board and its committees are clear.