Board Perspectives: Risk Oversight

Ten Principles for Risk Oversight Revisited

Issue 75

Following the global financial crisis, risk oversight became an imperative for boards of public companies, particularly in the United States. Boards of listed companies across all industries have since formulated their respective approaches to risk oversight and organized themselves accordingly. Below, we revisit 10 timeless principles for boards to use to evaluate their risk oversight process as it stands today.

While risk oversight has always been an important part of the board's agenda, the disruptive financial crisis taught everyone a lesson about just how important it is. The risk oversight playbook has evolved over recent years, during which many boards took a hard look at their membership, how they operate, and whether their operations and the information to which they have access are conducive to effective risk oversight.

In addition, regulators have taken an active interest in board risk oversight. For example, the U.S. Securities and Exchange Commission requires that proxy disclosures shine a spotlight on the board's role in overseeing the company's risk management process, the directors' qualifications to understand the entity's risks, and the board's compensation committee's evaluation of the entity's various compensation arrangements to ensure that they are not encouraging the undertaking of excessive, unacceptable risks.

Ten Principles of Effective Risk Oversight

1. Understand the company's key drivers of success.
2. Assess the risks in the company's strategy.
3. Define the role of the full board and its standing committees with regard to risk oversight.
4. Consider whether the company's risk management system – including people and processes – is appropriate and has sufficient resources.
5. Work with management to understand and agree on the types (and format) of risk information the board requires.
6. Encourage a dynamic and constructive risk dialogue between management and the board, including a willingness to challenge assumptions.
7. Closely monitor the potential risks to the company's culture and its incentive structure.
8. Monitor critical alignments of strategy, risk, controls, compliance, incentives and people.
9. Consider emerging and interrelated risks: What's around the next corner?
10. Periodically assess the board's risk oversight processes: Do they enable the board to achieve its risk oversight objectives?

Source: Chapter 4, *Report of the NACD Blue Ribbon Commission – Risk Governance: Balancing Risk and Reward*, National Association of Corporate Directors, October 2009, pages 14-19.

Just over six years ago, the National Association of Corporate Directors (NACD) published its *Report of the NACD Blue Ribbon Commission – Risk Governance: Balancing Risk and Reward*. This report recommends 10 principles to assist boards in strengthening their oversight of the company's risk management. According to the report, "the Commission believes that [the 10] principles provide a foundation that boards can use to build a more comprehensive risk oversight system tailored to the specific needs of their respective companies."

We agree. These 10 principles still stand today. Offered as guidance to directors, they not only provide a context for understanding the risk oversight process, but also present an outstanding framework for a board to use when evaluating its current risk oversight process. The principles are discussed below:

1. **Understand the company's key drivers of success**.

   Understanding the business and industry, what drives value creation, how the business model works, and the critical issues affecting the company lays a vital foundation to an effective risk oversight process. Accordingly, directors must remain abreast of these matters; processes must be in place to help them in this regard.

2. **Assess the risks in the company's strategy.**

   This principle and the one before it are interrelated. Both are especially important because they focus on understanding the corporate strategy and the risks inherent in the strategy. This understanding provides the context for identifying the risks that truly matter – the critical enterprise risks that threaten the execution of the company's strategy and business model – versus the everyday, ongoing risks of managing the business.

   It is vital that directors understand the risks inherent in the business model, including the key assumptions underlying the continued viability of the business model, and agree with executive management on the company's risk appetite in the pursuit of enterprise value creation.

3. **Define the role of the full board and its standing committees with regard to risk oversight.**

   This principle is important for directors to keep in focus as they collaborate in clarifying risk oversight responsibilities for the full board and the various standing committees. The NACD Blue Ribbon Commission (BRC) asserts that, "as a general rule, the full board should have primary responsibility for risk oversight, with the board's standing committees supporting the risks inherent in their respective areas of oversight." We agree.

   Our experience is that the vast majority of directors agree with this general rule, as it mirrors the full board's responsibility for strategy. It also recognizes that there are always outliers due to unique circumstances. Finally, the NACD BRC points to the importance of distinguishing management's responsibilities from the board's.

4. **Consider whether the company's risk management system – including people and processes – is appropriate and has sufficient resources.**

   This principle is important because, too often, risk is an afterthought to strategy, and risk management is an appendage to performance management (i.e., risk management is often what the NACD BRC describes as a "side activity"). This principle addresses such issues as positioning the chief risk officer or an equivalent executive for success. It looks beyond mere risk identification to consider the adequacy of other dimensions of managing risk, including sourcing, measuring, mitigating and monitoring risk through appropriate policies, processes, people, reporting, methodologies, and systems and data.

5. **Work with management to understand and agree on the types (and format) of risk information the board requires.**

   This principle remains a common issue for many boards. We often hear directors complaining of being overwhelmed with reports or too many agenda topics while being underwhelmed with

insightful information for decision-making. The emphasis on more leads to a cry for less and a sharper focus on actionable information (e.g., "Tell me what I need to know, and recommend what I need to do."). Whether or not there is reliance on quantitative models, reporting should provide different perspectives on a given risk.

To focus the risk oversight dialogue, the NACD BRC introduces five categories of risks facing each board:

- Governance risks
- Critical enterprise risks (as discussed above)
- Board-approval risks
- Business management risks (i.e., the normal ongoing risks)
- Emerging risks and nontraditional risks (e.g., climate change, slowdown in foreign markets, disruptive technological innovation)

These categories are useful, as the critical enterprise risks and emerging risks should capture most of the board's attention, whereas the business management risks should be addressed through periodic status reporting and escalation of significant issues.

6. **Encourage a dynamic and constructive risk dialogue between management and the board, including a willingness to challenge assumptions.**

   This principle addresses the need for constructive engagement between boards and management on risk matters. The principle's reference to challenging assumptions is especially important in light of the financial crisis, after which many have questioned whether boards really understood the key variables driving an institution's success and exposing it to failure, as well as the sensitivity of those variables to changes in the market. When an organization is making a lot of money, directors need to understand the risks undertaken to achieve success, rather than simply applauding as management breaks out the champagne.

7. **Closely monitor the potential risks to the company's culture and its incentive structure.**

   As with the sixth principle, this principle points to another lesson of the financial crisis: the potential impact of a company's culture and incentive compensation structure on behaviors, decisions and attitudes toward taking and managing risk.

   Culture and incentives form the glue that binds all elements of the risk management infrastructure together, because they reflect the shared values, goals, practices and reinforcement mechanisms that embed risk into an organization's decision-making processes and risk management into its operating processes. In effect, they represent a look into the soul of an organization to ascertain whether risk-reward trade-offs really matter to its leaders.

   One of the significant lessons of the financial crisis is the danger of "heads I win, tails you lose" compensation structures for executives whose actions – or inaction – can expose the organization to significant risks well beyond the level of risk the board might consider acceptable.

8. **Monitor critical alignments of strategy, risk, controls, compliance, incentives and people.**

   This principle speaks to the importance of aligning critical elements to get everyone and everything – people, processes and the organization – on the same page. Without alignment, there is likely to be a disconnect between a company's strategy and its execution, and disconnects can be costly as well as risky. Nevertheless, alignment is hard for management to achieve – and even more challenging for directors to oversee.

9. **Consider emerging and interrelated risks: What's around the next corner?**

   Emerging risks deal with issues that are not on management's radar currently. They require an anticipatory and forward-looking focus. The worst kind of uncertainty is being unaware of what we

don't know; while senior managers have knowledge from internal and external sources, do they really understand what they don't know?

The fundamental question raised by this principle is an inquiry as to whether management looks out far enough, is monitoring what matters in the external environment and devotes sufficient time to "connecting the dots." Sooner or later, something fundamental in the organization's business will change. And when disruptive change occurs, a company's risk profile is likely to be altered in significant ways. Therefore, directors need to know that management devotes sufficient time to thinking about the unthinkable and response readiness preparation, as both are key to a world-class reaction.

10. **Periodically assess the board's risk oversight processes: Do they enable the board to achieve its risk oversight objectives?**

    The last principle advocates applying the best practice of periodic board self-evaluations to the risk oversight process.

In closing, directors should use these 10 timeless principles to assess their board's risk oversight process to ascertain whether the process needs a refresh or redirection.

Questions for Boards

Following are some suggested questions that boards of directors may consider, based on the risks inherent in the entity's operations:

- Has the board articulated its risk oversight objectives? Are those objectives incorporated into the board's charter?
- Has the board evaluated the effectiveness of its processes in achieving its risk oversight objectives? If so, has the board considered the NACD BRC's 10 principles of effective risk oversight in evaluating its risk oversight processes?
- Is the board proactively taking steps to address any gaps that impede its risk oversight effectiveness?

How Protiviti Can Help

Protiviti assists boards and executive management with assessing the board risk oversight process, the risks inherent in the enterprise's strategy and business plans, and the capabilities for managing those risks. We help organizations identify and prioritize the risks that can impair their reputation and brand image and lead to failure to execute the corporate strategy successfully.

About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 *Fortune* 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is partnering with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on www.nacdonline.org/Magazine/author.cfm?ItemNumber=9721. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* are consolidated into a printed booklet that is co-branded with NACD. Protiviti will also post these articles at **Protiviti.com.**

protiviti®
Risk & Business Consulting.
Internal Audit.