By Richard J. Anderson, CPA, and Mark L. Frigo, CMA, CPA

What Should Directors Ask about Risk Management?

Boards of directors have to pay more attention to risk management than ever before in their corporate oversight duties. Sometimes it helps to ask the right questions.

In this increasingly complex and fast-paced world, significant risk events are happening more often and with greater impact than ever before. According to "The gods strike back" in the February 2010 issue of *The Economist*, "It turns out that in financial markets 'black swans,' or extreme events, occur much more often than the usual probability models suggest." Such events have focused increased attention on risk management in many organizations and in their boardrooms.

Another factor driving a renewed interest in risk management has been the desire by various third parties, such as regulators, institutional investors, and rating agencies, for increased transparency regarding risk processes. For example, the Securities & Exchange Commission (SEC) now requires registrants to describe the board's role in risk oversight. In support of this disclosure, the SEC noted in its release on this requirement that, "We were persuaded by commenters who noted that risk oversight is a key competence of the board and that additional disclosures would improve investor and shareholder understanding of the role of the board in the organization's risk management practices."

For some boards, particularly those of nonfinancial companies, the discharge of their responsibility for risk management oversight is a difficult task. They acknowledge that management is already managing risks, but trying to determine how much additional process capabilities, transparency, and reporting would be helpful may be a daunting task. A 2009 report, "Effective Enterprise Risk Oversight: The Role of the Board of Directors," published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), observes: "The challenge facing boards is how to effectively oversee the organization's enterprise-wide risk management in a way that balances managing risks while adding value to the organization." The key for management is to help the board add strategic value, not just processes and reporting.

To assist boards in meeting this challenge, we've summarized 10 key questions that directors should consider asking (and management teams should be prepared to answer). They are based on our interaction with directors and executives at risk management conferences and our forums in the Strategic Risk Management Lab at DePaul University.

Important Questions

Here are our questions.

1 What are the top risks facing the organization that could significantly impair the organization's ability to achieve its business objectives?

The board should know the key risks that management believes could impair their ability to achieve their business objectives. Also, given the dynamic nature of risk, the board should be receiving periodic updates about these risks. The focus should be on a concise list of the top strategic risks (such as a "top 10" list). We've found that boards receive the most benefit from a concise listing and discussion of the top or strategic risks facing the organization. They should be cautious about initially trying to deal with too large and complex reporting of risks. For example, an organization does face many risks, but a listing or matrix of 30, 40, or 50 risks will over-

whelm a board and not allow a real focus on the key risks. Similarly, while an organization may ultimately want to quantify certain risks, attempting complex quantification of risks at the start of the risk process may again overwhelm the board. Instead, the board should focus on a concise list of the top or key strategic risks that could impair the organization's ability to implement its strategy and achieve its business objectives. It should also ask how management is monitoring these risks and related action plans. To put this another way, the board should start by understanding the organization's key business objectives and risks related to those strategies. This is an area where a strategic risk assessment would be useful.

2 What are the organization's risk management processes and capabilities, and how do we know that they are effective?

The board should understand the overall risk management processes and capabilities of the organization. In addition, because risk management practices are continuing to evolve in general, it should also understand what management will be doing to enhance these processes and capabilities in the organization. For example, is there a strategy and plan to enhance risk management in the organization? The board may also consider asking management how it knows that these processes are operating and are effective across the organization. A final area of inquiry can be to consider the upside of risk, specifically, how management intends to improve risk management to make it a source of competitive advantage and resilience. Again, while acknowledging that management is already managing risks, the board should ensure that there's enough transparency so they can see and understand these processes and how they can be improved.

3 How is risk management integrated into strategy setting, business-unit planning, and decision making?

A key responsibility of the board is strategy setting, and this process should include an understanding and thorough discussion of the related risks. In its *Key Agreed Principles to Strengthen Corporate Governance for Publicly Traded Companies*, the National Association of Corporate Directors (NACD) noted, "Management performance, corporate strategy, and risk management are the prime underpinnings of the corporation's ability to create long-term value." Accordingly, boards should ensure that an organization's risk management processes include strategy setting and its flow down to business-unit planning and decision-making processes. Boards also need to understand the related information flows and how risk processes and metrics are included when the organization is assessing its overall performance.

4 Who in management is responsible for risk management, and is there clarity and accountability for that role and responsibilities?

Directors should ask which executive is responsible for the overall risk management program. As with any other process, accountability is needed for these risk processes to be effective. Though some organizations have created the role of chief risk officer (CRO), that role may or may not be needed. In other organizations, this responsibility may be held by an executive such as the chief financial officer (CFO). CFOs are increasingly being called on to play a more active role in strategic planning (see "What the CFOs Want," *The Wall Street Journal*, June 27, 2011) while managing uncertainty, which places them in an ideal intersection for driving improved risk management. The board should also know if other roles and responsibilities have been defined, such as risk owners for certain significant risks. Finally, along with accountability, the board should also find out if appropriate resources have been allocated to support the risk management processes.

5 Do we understand and agree with management's risk appetite and risk tolerances?

There should be clear dialogue between the board and management about the organization's risk appetite and risk tolerances. Our experience is that the concept of risk appetite is a difficult one for many boards. Yet understanding the amount of risk an organization is willing to accept while striving to achieve its business objectives is a basic issue. In a recent thought paper on risk appetite, "Understanding and Communicating Risk Appetite," which was published in January 2012, COSO noted that, "In con-

ducting appropriate oversight, management and the board must deal with a fundamental question: How much risk is acceptable in pursuing these objectives?" The board should also know how the risk appetite and tolerances are communicated and aligned with business-unit plans, decision making, and operations. If management and the board decide to focus on this area, we would highly recommend they review the new thought paper.

6 What is the organization's risk culture, and how is it reinforced?

The board should ask management to describe the "risk culture" of the organization and how they communicate and reinforce it. Risk culture is a critical underpinning of effective risk management. It's one of two areas of inquiry that Standard & Poor's focuses on in its initial reviews of risk management practices in nonfinancial companies. The board should ask itself how it knows what the risk culture is across the company and what its members should be doing to assist in setting and reinforcing the right risk culture.

Here's a quick self-test question for directors: Can you explain the risk culture of the organization in one minute? Organizations undertaking growth strategies through mergers and acquisitions (M&A) must pay attention to how the integration of the acquired companies will impact risk culture and what needs to be done to ensure the right risk culture is sustainable. Moreover, aggressive growth strategies through M&A often create new risks that are often unforeseen in most due diligence processes.

The board should ask itself how it knows what the risk culture is across the company and what its members should be doing to assist in setting and reinforcing the right risk culture.

7 How does management monitor external events and trends to identify "emerging risks"?

Management should conduct an ongoing process to identify emerging issues and establish appropriate monitoring activities. Management and boards are increasingly aware of the dynamic nature of risks and the need for periodic review and updates of the key risks facing the organization. In particular, recent events such as the credit crisis have focused more attention on the need to monitor developing external events that could ultimately impact the organization. Accordingly, the board should receive periodic updates on management's views of emerging issues and risks. It should also have the opportunity to voice its views on emerging issues. In addition, the board should recognize that some types of emerging risks may not be recognized until they happen, so it may want to probe the organization's crisis management plan and find out how prepared management is to address significant, unexpected risk events.

8 How are compensation and incentive plans aligned with the organization's risk appetite and tolerances?

The board should understand how risk and the organization's risk appetite have been explicitly considered for each major compensation plan. The possible impacts of risks related to compensation policies and plans are another facet of risk where the SEC has expanded its proxy disclosure requirements. There should be clear direction from the board to its compensation committee to ensure that this relationship is considered appropriately when reviewing and approving compensation policies and plans.

In particular, the board should ensure that there's alignment between these plans and the long-term strategies of the organization. For example, are there short-term incentives, such as sales, that don't consider longer-term impacts, such as collectability of the related receivables? The board may also want to consider whether there are or should be consequences (such as clawbacks) included in compensation plans to address situations where subsequent risk events happen or risk tolerances are exceeded. This could include such actions as deferring some incentive compensation until an appropriate time period has passed to ensure a long-term perspective.

9 Is the risk information communicated to the board adequate, timely, and accurate?

The board should make a critical review of the risk information it receives to determine that it's adequate and effective. The information should be clear, concise, and not overly technical or voluminous. While acknowledging that the board must and should rely on management for information, the NACD cautions that, "…directors cannot be overly reliant on management for determining the board's priorities and related agenda, and information needs." The board should also ask itself how it knows that the risk information it's receiving is accurate and complete. The board may want to find out from the audit committee how the completeness and accuracy of risk-related information is addressed by internal auditors or others in the organization. Boards may also want to consider engaging independent advisors to advise and educate the board about these matters.

10 Are we comfortable and confident with risk-related information furnished to external parties, including both financial and nonfinancial reports?

With external parties' increased interest in risk information, the board needs to be comfortable with its external reporting of risks and risk management practices, including both financial and nonfinancial information. The board should also look for consistency of risk information across disclosures—for example, between the proxy statement disclosures and the risk information in the 10-K report. It should also ensure that board committee charters are updated appropriately to reflect activities and responsibilities related to risk and risk management as those processes evolve in the organization.

While it's important to have effective risk management processes, directors should focus on results of these processes and understand the impact and actions resulting from them.

Focus on Results

One final point that directors should keep in mind as they consider the topics outlined in the questions: The objective of an organization's risk management processes is to have actions that will help the organization protect and enhance shareholder value. While it's important to have effective risk management processes, directors should focus on results of these processes and understand the impact and actions resulting from them. It's the results of the risk management processes that are critical, not just the processes themselves.

The questions we presented are intended to be helpful reminders of risk management topics that boards should be considering and management teams should be prepared to answer. Though not meant to be an all-inclusive list of possible areas of inquiry, they give directors a good starting point in considering their oversight of management's risk management activities. The board may also want to consider these questions when planning its agendas so it can identify specific areas for more in-depth discussions, education, or management presentations. Asking the right questions is the first step toward improving risk management and governance. SF

Richard J. (Dick) Anderson, CPA, is a clinical professor in the Center for Strategy, Execution and Valuation and the Strategic Risk Management Lab at DePaul University and a retired partner of Pricewaterhouse Coopers LLP. With PwC, he was a regional leader in the Financial Services Advisory practice, consulting with major financial services organizations on internal auditing practices, risk management, and audit committee activities. You can reach Dick at rander37@depaul.edu.

Mark L. Frigo, Ph.D., CMA, CPA, is director of the Center for Strategy, Execution and Valuation and the Strategic Risk Management Lab in the Kellstadt Graduate School of Business and Ledger & Quill Alumni Foundation Distinguished Professor in the School of Accountancy at DePaul University in Chicago. He is an advisor to executive teams and boards in the area of Strategic Risk Management and strategy execution, and he is an IMA® member. You can reach Mark at mfrigo@depaul.edu.