# TOP TAKEAWAYS

## Board's Oversight of Enterprise Risk Management

These are the top takeaways from the roundtable on the **Board's Oversight of Enterprise Risk Management**, which was moderated by Curt Creely on November 17, 2011, during the NDI Executive Exchange, a segment of Foley's National Directors Institute. Featured participants in the roundtable were Laurie J. Champion of Aon Global Risk Consulting and John Gimpert of Deloite & Touche LLP. These takeaways reflect the input of the audience members in addition to the individuals just mentioned.

1. **The board's oversight of risk is not a new responsibility.** It was widely agreed that the principle that a company's board of directors has oversight of enterprise risk management is not new. However, it was noted that with the advent of enhanced regulations and required disclosures for public companies, the board's role in such function has received enhanced scrutiny, which has caused boards to evaluate their risk oversight function and to refresh their risk oversight practices. It was also noted that there have been several well regarded reports that have been published on the topic of board oversight of risk – the Committee of Sponsoring Organizations of the Treadway Commission; and the National Association of Corporate Directors – Blue Ribbon Commission on Risk Governance.

2. **Boards responsible for risk oversight, not risk management.** It was noted that the proper role of directors in risk management is one of oversight and not management. Although the analysis and management of risk have become increasingly complex, it was agreed that directors do not need to be risk experts. However, they do need to become reasonably familiar with risk management concepts and principles, especially as they relate to the company and the industry in which the company operates. Although directors must exercise oversight of risk management processes, it was agreed that risk management is the responsibility of management and directors should not be expected to involve themselves in the day-to-day implementation of risk management.

3. **More public disclosure on risk management.** It was noted that, with the advent of the Securities and Exchange Commission rules requiring enhanced disclosure regarding risk management, there has been increased disclosure in proxy statements in the past year surrounding risk management. Although financial firms generally have more sophisticated risk management processes, and their disclosure generally reflects that, the increased disclosure was noted across all sectors. It was also noted that future proxy statement disclosure is likely to center around the connection between a company's strategy and risk appetite.

4. **Possible link between share performance and strong risk management.** It was noted that a recent study has shown there is potentially a correlation between having strong risk management processes and share price. Although the study was one of the first of its kind, it suggests that implementing certain enterprise risk management best practices may ultimately improve a company's performance and share value.

5. **Risk should be viewed broadly.** It was widely agreed that boards should assume a broad definition of risk and use categorizations when considering them. There are many types of risk that can damage a company, and risks categories range from financial risks, human resource risks, reputation risks, operational risk, regulatory risk, among others. Using these categorizes, as well as geographic and time based categories, can assist a board in the consideration of such risks as well as help identify so-called "gray swan" or "black swan" type events in order to plan for them. In attempting to counter the common issue of prioritizing risks from events that occurred most recently, it was suggested that directors should think in terms of multiple-year risk horizons.

6. **Strategy and enterprise risk management.** Frequently the processes related to the development of strategic planning and management of risk get addressed in separate "silos" within an organizational structure However, it was noted that strategic development and risk management should be closely intertwined as a company's risk appetite, which is primarily a risk management consideration, will inform aspects of a company's strategic plan. Additionally, as the risk landscape for a company changes, a company should consider how such changed circumstances impact its strategic plan. It was noted that companies need to consider ways to ensure they are compensated for the risk assumed as well as maximize their profits, both of which require analysis of the strategic plan in the context of risk management.

7. **Where a director starts.** For a director or chairman charged with risk oversight, a good starting point would be to review and analyze the risk assessment prepared by management. It was noted that directors should have a good understanding of such assessment, be willing to challenge management's conclusions, and confirm that information included in such an assessment is generally reliable. As part of this process, time should be spent understanding the company's current risk exposure and how that exposure might change over time, as well as consider the relationship between the company's risk exposure and its strategic goals.

8. **A risk management process.** In order to effectively oversee risk management, a board needs to develop a process by which it can obtain information on the status of business risks to inform its decisions. The process should include management regularly compiling and reporting comprehensive information regarding the company's risk exposure. A necessary aspect to the reporting process is ensuring that the information provided is reliable and timely. In addition to reports, a board should occasionally obtain information first hand, whether by speaking with managers directly or visiting company plants periodically in order to surface risks that were not initially identified as well as better understand the risks facing the company. As part of the information gathering process, directors should test how the information gathered interacts and integrates into the company's strategic plans.

9. **The next step – establishing a risk-conscious culture.** A company's culture will in large part guide employee actions from the top down so it is important for companies to actively develop a risk-conscious culture. Examples were provided where a disconnect existed between management's view and the employees' view of risk management and the negative impacts that resulted. As such, It was emphasized that developing a risk-conscious culture is more than having senior management provide speeches on the subject, but requires a strong commitment from top management in word and deed that is reinforced by policies that have consequences, whether by compensation or otherwise. It was also noted that a risk-conscious culture does not mean that a company becomes risk adverse but rather that a company appropriately calculates the risk versus reward of its decisions.

10. **Seeking outside advisors to assist, not supplant.** It was submitted that companies can benefit from seeking outside advisors to assist in creating a good risk assessment process. However, it was noted that directors and management should not expect to delegate their responsibilities to the outside advisors or assume the outside advisors will supplement the role of the board in the process. It was submitted that advisors can be helpful in reviewing a company's process to ensure information received is reliable, but the process of identifying and ensuring proper management of risks remains the board's responsibility.

**For more information**
For more information on the roundtable on Independent Chair / Lead Director / Governance Committee Chair, please feel free to contact the moderator directly:

Curt Creely
Foley & Lardner LLP
ccreely@foley.com