Risk Management Oversight: Is *Your* Board at Risk?

By Richard Leblanc

Increasingly, boards are becoming concerned with the concept of risk, particularly directors' understanding of risk; emerging and non-quantifiable—but potentially significant—risks; and how risk oversight is handled by the board and its committees.

Models of risk have emerged, as have technology and the sophistication of enterprise risk management, risk advisors, and assurance processes. Increasingly, companies are addressing non-financial reporting risks (including operational and reputational), internal controls over such risks, and the capacity of audit committees and boards to oversee them. Outside of financial institutions, we may see the development of certain risks being lodged within other committees, separate risk committees, and overall strategic risk being overseen by the board.

Board Self-Assessment

The proliferation of structural-oriented, non-robust questionnaires means that "soft-ball" risk management questions are asked by, and of, boards. In asking and answering such questions, the opportunity to have discussions surrounding risk best practices may be lost. The board may have a false sense of reality.

"We missed it." This phenomenon may be traceable to a board not asking the right questions at the right time. Why is this so? At the heart is a risk that was not known, or partially known, by the board or a committee. This omission can cost shareholders.

In my investigation of best practices in risk management oversight by boards, the consensus by directors is that it is a complex area. I canvassed the literature, academics and practitioners, conducted interviews with directors and auditors, and drew upon empirical data, including observation of boards in action. The following twelve robust items can gauge where a board may be on a continuum of risk best practices. Ask yourself where you would rate a board on which you serve.

Reprinted from Directors Monthly with permission of the publisher.

1133 21st Street, NW
Suite 700
Washington, D.C. 20036
202-775-0509
www.nacdonline.org

Director Summary: Risk management can be complex and potential risks cannot always be foreseen. The author enumerates twelve best practices for directors to measure the risk management practices of their boards. By incorporating some or all of these best practices, boards can fortify their companies with secure oversight standards.

Risk Management Oversight: Best Practices

1. *There exists a clear understanding of the scope of risk oversight by the board and board committees.*

The risk profile established by the board is concerned with material business risks, as identified by the company's risk management system. Oversight is allocated by the board to its committees, and appropriately documented.

2. *There exists an effective process to identify material business risks.*

There are regular updates of material risks overseen by the relevant committee(s), using systematic methods, tools, techniques, and judgments supported by functional risk registers and backed by appropriate action plans.

3. *Committees have a clear understanding of the board's risk appetite (i.e., the acceptable amount and type of risk) for relevant material categories of risk.*

Each material risk subject to a committee's review is clearly defined and communicated. Strategic parameters for management guide risk mitigation actions and risk tolerance ranges. These practices allow a committee to compare the consistency between current risk management performance and the defined risk appetite set by the board.

4. *The company adopts a culture.*

This includes exhibiting appropriate behaviors consistent with the agreed appetite for risks overseen by each committee.

5. *Effective discussions (including meaningful, robust dialogue) occur in committee meetings regarding risk management performance.*

The relevant committee receives regular, detailed, comprehensive, analytical information on risk impact including: updates on new, ongoing, mitigated, and monitored risk ratings; risk and control "ownership" information; and risk registers to regularly track impact and likelihood of risk for risks subject to committee review.

6. The audit committee has a clear understanding of how each relevant material risk may impact the company's financial position (i.e., changes to the financial condition or business performance).

Each member of the audit committee is able to apply his or her informed understanding of key risks to the company's strategy, the market, competitors, and the economy, and to critically review: business plans; budgets; major projects; accounting treatments; management bias, and capital structure. This review may include the use of risk-responsive, multi-scenario financial models, which could include links to business continuity plans under crisis conditions, produced by management at the request of the committee.

7. There exists effective oversight of fraud risk by the audit committee.

The oversight of fraud risk by the audit committee is accomplished by:

- establishing tone-at-the-top, which embodies integrity, accuracy, completeness, and relevance;
- to the extent feasible, satisfying itself as to the integrity of the CEO and CFO and that both instill a culture of integrity throughout the company;
- overseeing the identification, implementation, assessment, and monitoring of appropriate controls and the potential for override;
- recognizing, and acting upon, improper pressures, opportunities, and potential for material misstatement of financial reports.

8. Communication with, and confidence in, senior executives responsible for risk management.

A dedicated mandate exists within the company to provide overall risk management direction, coordination, integration, and implementation.

For example, a chief risk officer, or the equivalent, would perform the following two critical functions: integrate business unit risk data as applicable; and provide reporting on the company's risk profile, regulatory compliance, and contingency planning to the audit committee and/or the board

9. Appropriate key risk indicators (or red flags, early warning indicators, etc.) are used to monitor material changes that may impact the company's risk profile.

Impacts could be changes in, or concerns regarding, management, operations, systems, and economic and industry conditions.

10. The audit committee clearly understands how the company's material risks impact the committee's functions.

Each member understands the impact of material risks on: audit scope, the systems of internal control and compliance, and the financial reporting process.

11. The board, audit committee, and management are committed to a robust, effective system of risk management and reporting.

Effective risk management systems are: enterprise-wide, robust and dynamic; integrated into operations; real-time, continual; culturally embedded; and evaluated, monitored, and mitigated material business risks to the company.

Effective risk reporting is accurate, regular, detailed, comprehensive, and contains analytical information.

12. The company's risk management system enhances the board's strategic capability.

The risk management system brings efficiency, rigor, and quality data to: risk-return trade-off opportunities; capital allocation decisions; performance metrics; and other risk-adjusted responses.

Conclusion: Risk Management is a Complex Area

As the *Report of the NACD Blue Ribbon Commission on Board Evaluation: Improving Director Effectiveness* states, "To be effective, boards need the right people, the right issues, the right information, the right process, and the right follow-through." This is especially true for risk management oversight by boards.

The consensus in risk management is that this is a complex area that requires careful thought by directors, and that not all risks can be predicted or controlled. However, to the extent that directors and boards are uneasy about the quality of risk information, reporting, and systems, these twelve best practices may stimulate directors' thinking and comfort level in questioning management. Risk management should not be an exercise in bureaucracy, but a practical way to mitigate risk and identify opportunity: to enhance the strategic and oversight capability of the board. ■

Richard Leblanc, PhD, is an assistant professor of corporate governance at York University, and regularly speaks to, and advises, boards. He may be reached at rleblanc@yorku.ca.