MAYER | BROWN

ACROSS THE BOARD

Keeping companies and their boards a step ahead

Director College

7. Risk Oversight/Management

MAYER | BROWN

Agenda

- Sources of Duty
- Types of Risk
- Who Should Fulfill the Oversight Responsibility
- Elements of Effective Risk Management Oversight

Sources of Duty

Sources of Duty

- Delaware Fiduciary Law
  - A board's risk oversight responsibility derives primarily from state law fiduciary duties.
    - To be clear, the board cannot and should not be involved in actual day-to-day risk management. Its role is limited to oversight.
  - Generally, directors can only be liable for a failure of board oversight where there is "sustained or systemic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists." *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959, 971 (Del. Ch. 1996).
  - In cases since *Caremark*, the Delaware courts have made clear that there would be no liability under a *Caremark* theory unless the directors intentionally failed entirely to implement any reporting or information system or controls or, having implemented such a system, intentionally refused to monitor the system or act on warnings it provided.

Sources of Duty *(cont'd)*

- New York Stock Exchange Rules
  - NYSE rules impose certain risk oversight obligations on the audit committee of a listed company, while acknowledging that "it is the job of the CEO and senior management to assess and manage the listed company's exposure to risk."
  - NYSE rules require that an audit committee "discuss guidelines and policies to govern the process by which risk assessment and management is undertaken."
  - Discussions should address major financial risk exposures and the steps the company has taken to monitor and control such exposure, including a general review of the company's risk management programs.
  - NYSE rules permit a company to create a separate committee or subcommittee to be charged with the primary risk oversight function as long as the risk oversight processes conducted by that separate committee or subcommittee are reviewed in a general manner by the audit committee, and the audit committee continues to discuss policies with respect to risk assessment and management.

Sources of Duty *(cont'd)*

- Other Sources
  - SEC
    - Proxy statements must disclose any compensation policies or practices that create risks that "are reasonably likely to have a material adverse effect on the company."
    - Proxy statements must disclose the extent of the board's role in risk oversight, including a description of how the board administers its oversight function.
  - "Best Practices"
    - National Association of Corporate Directors—Blue Ribbon Commission on Risk Governance
    - Committee of Sponsoring Organizations of the Treadway Commission
    - Conference Board Corporate Governance Center
  - Institutional Shareholder Services
    - Includes a specific reference to risk oversight as a criteria for choosing to recommend or oppose a director for election.

Sources of Duty *(cont'd)*

- Other Sources
  - Industry specific laws, rules and guidelines
    - Insurance Companies
      - NAIC Corporate Governance Annual Disclosure Model Act requires insurers to describe corporate governance, including "[t]he processes by which the Board of Directors, its committees and senior management ensure an appropriate level of oversight to the critical risk areas impacting the insurer's business activities including risk management processes, the actuarial function, and investment, reinsurance and business strategy decision-making processes."
    - Banks
      - Federal Reserve Board rules adopted under Dodd-Frank require all covered companies, as well as publicly-traded bank holding companies with $10 billion or more in assets, to create a risk committee to oversee risk management practices on an enterprise-wide basis. The committee must have at least one independent director and at least one member with relevant risk management expertise. Each member of the committee must have an understanding of relevant risk management principles and practices.

Types of Risk

Types of Risk

- Financial Reporting Risk and Fraud
- Credit Risk
- Liquidity Risk
- Operational Risk
- Investment Risk
- Privacy and Cyber Security Risk
- Environmental Risk
- Legal/Compliance Risk
- Tax Risk
- Reputational Risk

Who Should Fulfill the Oversight Responsibility

Who Should Fulfill the Oversight Responsibility

- Some commentators believe that risk oversight is equal in importance to oversight of strategy and that the full board should have responsibility
  - Delaware law imposes the duty of oversight on all directors.
- NYSE rules require the audit committee to address major financial risk exposures.
- Some commentators believe the audit committee is already overburdened and that a separate risk committee is appropriate.
- Some commentators would “split the baby” and have the audit committee oversee financial/accounting risks and the full board or another committee other risks.
- ONE SIZE DOES NOT FIT ALL.

Elements of Effective Risk Management Oversight

Elements of Effective Risk Management Oversight

- Identification
  - Identify categories of risk the company faces, including concentrations and interrelationships.
  - Identify potential actors that pose a risk and stakeholders who are subject to risk.
  - Review assumptions and analysis underpinning the determination of the company's principal risks.
  - Ensure procedures are in place to identify new or materially changed risks.
- Measurement
  - Understand the likelihood of occurrence (frequency) and the potential impact (severity) of risks.
  - Review the ways in which risk is measured on an aggregate, company-wide basis.

Elements of Effective Risk Management Oversight *(cont'd)*

- Limits
  - Understand how aggregate and individual risk limits (quantitative and qualitative, as appropriate) are set.
  - Review actions to be taken if risk limits are exceeded.
- Mitigation
  - Review risk mitigation measures.
  - Review response plans.
- Responsibility
  - Set the correct "tone at the top."
  - Allocate responsibilities for risk oversight and management of specific risks to ensure a shared understanding as to accountabilities and roles.
  - Consider cross-disciplinary teams where appropriate.

Elements of Effective Risk Management Oversight *(cont'd)*

- Communication
  - Review procedures for reporting matters to the board.
  - Review quality, type and format of risk-related information provided to the board.
  - Review how risk management strategy is communicated and integrated into the enterprise-wide business strategy.
- Assessment
  - Review the design of the company's risk management functions, as well as the qualifications and backgrounds of senior risk officers.
  - Assess whether management is following risk policies and procedures.
  - Confirm internal audit includes assessment of risk management.
- Compensation
  - Review the company's compensation structure to ensure it is creating proper incentives in light of risks.

Disclaimer

- These materials are provided by Mayer Brown and reflect information as of the date of presentation.
- The contents are intended to provide a general guide to the subject matter only and should not be treated as a substitute for specific advice concerning individual situations.
- You may not copy or modify the materials or use them for any purpose without our express prior written permission.

Americas | Asia | Europe | Middle East

mayerbrown.com