LATHAM & WATKINS LLP

Boardroom Perspectives™

March 26, 2015

Three Practical Steps to Oversee Enterprise Risk Management (ERM)

by Scott Hodgkins, Steven B. Stokdyk, Joel H. Trotter

Introduction

Oversight of enterprise risk management, or ERM, continues to challenge boards and occupy a prominent place on the governance agenda. Effective ERM seeks to balance risk and opportunity while enhancing value-creation opportunities. Proxy advisors may recommend "against" or "withhold" votes against directors of companies that experience a material failure of risk oversight.

A leading ERM framework, developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, directs boards to:

- Concur with management's view of acceptable risk levels, or "risk appetite"
- Understand management's ongoing steps toward effective ERM
- Review the company's risk portfolio against its stated risk appetite
- Know the most significant risks and how management is responding

We recommend three steps for boards to frame their approach to risk oversight, which we discuss further, below:

1. Determine the board's preferred oversight model
2. Develop and review with management the company's approach to risk management
3. Assess board capabilities and effectiveness, reviewing for bias and groupthink

1. Determine the board's preferred oversight model

Typically, boards either retain primary responsibility for risk oversight or delegate initial oversight duties to a committee, such as the audit committee or a risk committee. Where the board retains primary responsibility, individual committees may provide input on specific types of risk, such as compensation risk, audit and financial risk, and regulatory and compliance risk.

In selecting between the active board model and the committee model, the board should consider those directors with the necessary expertise to oversee unique market, liquidity, regulatory, innovation, cybersecurity and other risks that may require special attention. The board should also consider whether adding duties to an existing committee, such as the audit committee, may be too burdensome in light of existing workload.

These issues are unique to each company, and the key is to ensure that the model you choose is effective for your situation.

2. Develop a stated approach to risk management

Some companies may adopt a risk management statement or policy. As with other policy statements, a risk management statement can create a tone-at-the-top benchmark for assessing value-creation opportunities as they arise and provide guideposts for management's operational decisions.

A risk management statement should separately identify:

- Acceptable strategic risks
- Undesirable risks
- Risk tolerances or thresholds in stated categories, such as strategic, financial, operational and compliance

In developing the company's approach, the board should consider:

- Investor expectations of the company's risk appetite
- Competitors' apparent risk appetite
- Stress-tests for risk scenarios, using historical experience and sensitivity analysis
- Long-term strategy versus existing core competencies
- Possible long-term market developments
- Risk concentrations (*e.g.*, customer, supplier, investment, geographic)
- Effects of new business generation on desired risk profile
- Strategic planning and operations compared to articulated risk appetite

Developing a stated approach to risk management requires good working relationships among the board members, the CEO and management, as well as active participation by all involved.

3. Assess board capabilities and effectiveness, reviewing for bias and groupthink

The board must evaluate its own capabilities and effectiveness, paying particular attention to the possible emergence of cognitive bias or groupthink.

In assessing board capabilities and effectiveness, the board should consider:

- Directors' skills and expertise compared to the company's current and future operations
- Possible director education initiatives or new directors with additional skills
- Delegation of risk oversight in highly technical areas, such as cybersecurity
- Retention of independent experts to evaluate specific risk management practices
- Clear allocation of responsibility among the board committees and members
- The balance between board-level risk oversight and management-level day-to-day ERM

Boards must also guard against two types of bias:

- Resistance to new ideas from outsiders, thus overlooking new opportunities or risks
- Confirmation bias, incorrectly filtering information and confirming preconceptions

Maintaining contact with business realities also requires collegiality and open communication among management and directors.

Boards should consider their risk oversight in light of these three steps to assist in framing an effective approach to enterprise-level risk exposures.

Scott Hodgkins
scott.hodgkins@lw.com
+1.213.891.8739

Steven B. Stokdyk
steven.stokdyk@lw.com
+1.213.891.7421

Joel H. Trotter
joel.trotter@lw.com
+1.202.637.2165

You Might Also Be Interested In

2015 Annual Meeting Handbook

Director Tenure: A Solution in Search of a Problem

Boardroom Perspectives: Three Practical Steps to Managing FCPA & Anti-Corruption Risks

Boardroom Perspectives: Three Practical Steps to Stay Ahead of Shareholder Activism