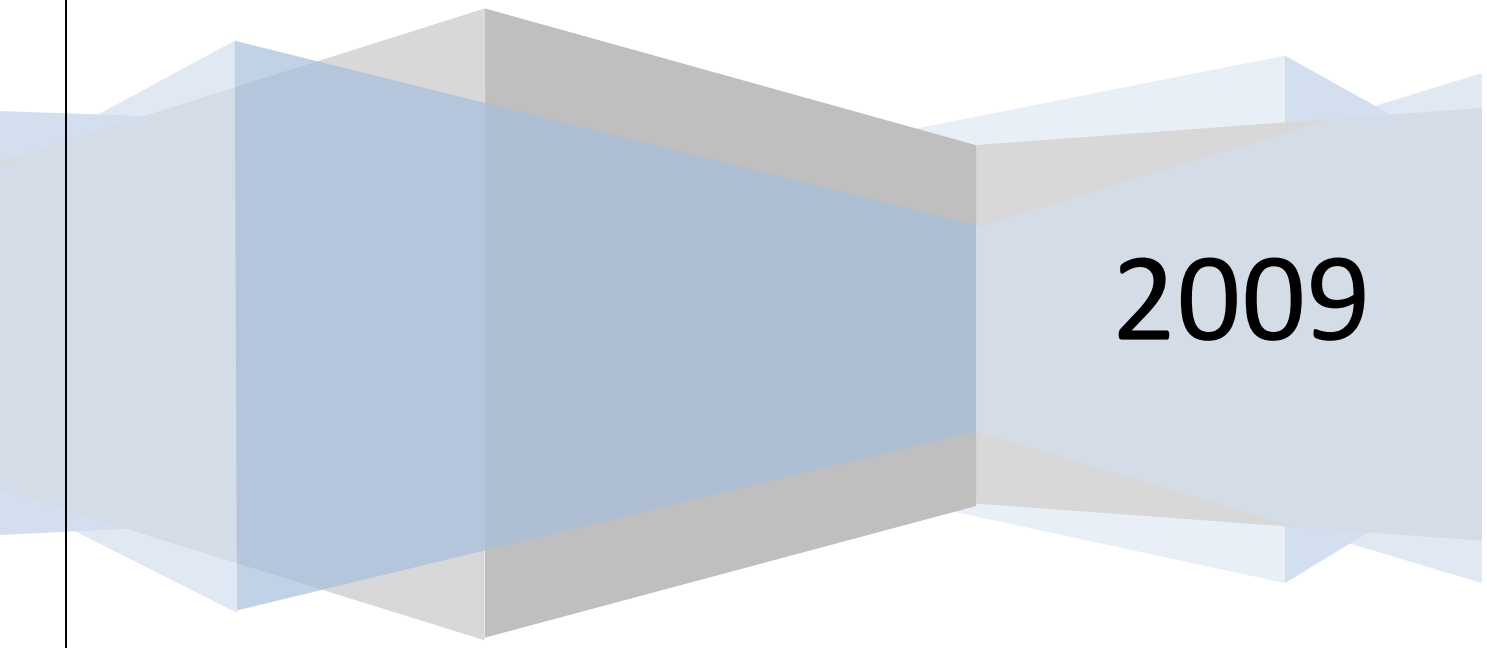
COSO
COMMITTEE OF SPONSORING
ORGANIZATIONS OF THE TREADWAY COMMISSION

Effective Enterprise Risk Oversight

The Role of the Board of Directors



2009

www.coso.org

Effective Enterprise Risk Management Oversight: The Role of the Board of Directors

The role of the board of directors in enterprise-wide risk oversight has become increasingly challenging as expectations for board engagement are at all time highs. Risk is a pervasive part of everyday business and organizational strategy. But, the complexity of business transactions, technology advances, globalization, speed of product cycles, and the overall pace of change have increased the volume and complexities of risks facing organizations over the last decade. With the benefit of hindsight, the global financial crisis and swooning economy of 2008 and the aftermath thereof have shown us that boards have a difficult task in overseeing the management of increasingly complex and interconnected risks that have the potential to devastate organizations overnight. At the same time, boards and other market participants are receiving increased scrutiny regarding their role in the crisis. Boards are being asked – and many are asking themselves – could they have done a better job in overseeing the management of their organization's risk exposures, and could improved board oversight have prevented or minimized the impact of the financial crisis on their organization?

Clearly, one result of the financial crisis is an increased focus on the effectiveness of board risk oversight practices. The New York Stock Exchange's corporate governance rules already require audit committees of listed corporations to discuss risk assessment and risk management policies. Credit rating agencies, such as Standard and Poor's, are now assessing enterprise risk management processes as part of their corporate credit ratings analysis. Signals from some regulatory bodies now suggest that there may be new regulatory requirements or new interpretations of existing requirements placed on boards regarding their risk oversight responsibilities. More importantly, while business leaders know organizations must regularly take risks to enhance stakeholder value, effective organizations recognize strategic advantages in managing risks.

> *".....I want to make sure that shareholders fully understand how compensation structures and practices drive an executive's risk-taking.*
>
> *The Commission will be considering whether greater disclosure is needed about how a company — **and the company's board in particular** — manages risks, both generally and in the context of setting compensation. I do not anticipate that we will seek to mandate any particular form of oversight; not only is this really beyond the Commission's traditional disclosure role, but it would suggest that there is a one-size-fits-all approach to risk management.*
>
> *Instead, I have asked our staff to develop a proposal for Commission consideration that looks to providing investors, and the market, with better insight into how each company and each board addresses these vital tasks."*
>
> *Mary Schapiro, SEC Chairman*
> *April 2009*

The U.S. Treasury Department is considering regulatory reforms that would require compensation committees of public financial institutions to review and disclose strategies for aligning compensation with sound risk-management. While the focus has been on financial institutions, the link between compensation structures and risk-taking has implications for all organizations. Recent comments from U.S. Securities and Exchange Commission Chairman Mary Schapiro, speaking before the Council of Institutional Investors this past spring, indicated potential new regulations may be emerging for greater disclosures about risk oversight practices of public companies. In July 2009, the SEC issued its first set of proposed rules that would expand proxy disclosures about the impact of compensation policies on risk taking and the role of the board in the company's risk management practices. Legislation has also been introduced in Congress that would mandate the creation of board risk committees.

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. Although some organizations have employed sophisticated risk management processes, others have managed risks informally or on an ad hoc basis. In the aftermath of the financial crisis, executives and their boards realize that ad hoc risk management is no longer tolerable and that current processes may be inadequate in today's rapidly evolving business world. Boards, along with other parties, are under increased focus due to the widely-held perception that organizations encountered risks during the crisis for which they were not adequately prepared.

Increasingly, boards and management teams are embracing the concept of enterprise risk management (ERM) to better connect their risk oversight with the creation and protection of stakeholder value. ERM is a process that provides a robust and holistic top-down view of key risks facing an organization. To help boards and management understand the critical elements of an enterprise-wide approach to risk management, COSO issued in 2004 its *Enterprise Risk Management – Integrated Framework*. That framework defines ERM as follows:

> ***Enterprise risk management is a process, effected by the entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of objectives***
>
> ***COSO's Enterprise Risk Management – Integrated Framework (2004)***

In today's environment, the adoption of ERM may be the most effective and attractive way to meet ever increasing demands for effective board risk oversight. If positioned correctly within the organization to support the achievement of organizational objectives, including strategic objectives, effective ERM can be a value-added process that improves long-term organizational performance. Proponents of ERM stress that the goal of effective ERM is not solely to lower risk, but to more effectively manage risks on an enterprise-wide, holistic basis so that stakeholder value is preserved and grows over time. Said differently, ERM can assist management and the board in making better, more risk-informed, strategic decisions.

An entity's board of directors plays a critical role in overseeing an enterprise-wide approach to risk management. Because management is accountable to the board of directors, the board's focus on effective risk oversight is critical to setting the tone and culture towards effective risk management through strategy setting, formulating high level objectives, and approving broad-based resource allocations.

COSO's *Enterprise Risk Management – Integrated Framework* highlights four areas that contribute to board oversight with regard to enterprise risk management:

- ***Understand the entity's risk philosophy and concur with the entity's risk appetite.*** Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of stakeholder value. Because boards represent the views and desires of the organization's key stakeholders, management should have an active discussion with the board to establish a mutual understanding of the organization's overall appetite for risks.

- ***Know the extent to which management has established effective enterprise risk management of the organization***. Boards should inquire of management about existing risk management processes and challenge management to demonstrate the effectiveness of those processes in identifying, assessing, and managing the organization's most significant enterprise-wide risk exposures.

- ***Review the entity's portfolio of risk and consider it against the entity's risk appetite***. Effective board oversight of risks is contingent on the ability of the board to understand and assess an organization's strategies with risk exposures. Board agenda time and information packets that integrate strategy and operational initiatives with enterprise-wide risk exposures strengthen the ability of boards to ensure risk exposures are consistent with overall appetite for risk.

- ***Be apprised of the most significant risks and whether management is responding appropriately.*** Risks are constantly evolving and the need for robust information is of high demand. Regular updating by management to boards of key risk indicators is critical to effective board oversight of key risk exposures for preservation and enhancement of stakeholder value.

Boards of directors often use board committees in carrying out certain of their risk oversight duties. The use and focus of committees vary from one entity to another, although common committees are the audit committee, nominating/governance committees, compensation committees, with each focusing attention on elements of enterprise risk management. While risk oversight, like strategy, is a full board responsibility, some companies may choose to start the process by asking the relevant committees to address risk oversight in their areas while focusing on strategic risk issues in the full board discussion.

While ERM is not a panacea for all the turmoil experienced in the markets in recent years, robust engagement by the board in enterprise risk oversight strengthens an organization's resilience to significant risk exposures. ERM can help provide a path of greater awareness of the risks the organization faces and their inter-related nature, more proactive management of those risks, and more transparent decision making around risk/reward trade-offs, which can contribute toward greater likelihood of the achievement of objectives.

An executive summary of COSO's *Enterprise Risk Management – Integrated Framework* provides an overview of the key principles for effective enterprise risk management and is available for free download at www.coso.org. More detailed guidance, including examples about effective implementation of the key principles, is contained in the full document. COSO's objectives are to improve organizational performance through better integration of strategy, risk, control, and governance. Our Frameworks are based on identified best practices and the development of consistent terminology and approaches that can be used by many organizations in meeting their objectives. We hope that our ERM Framework will help you in that journey to enhancing long-term stakeholder value.

****

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a voluntary private-sector organization comprised of the following organizations dedicated to guiding executive management and governance participants towards the establishment of more effective, efficient, and ethical business operations on a global basis. It sponsors and disseminates frameworks and guidance based on in-depth research, analysis, and best practices.

American Accounting Association
American Institute of Certified Public Accountants
Financial Executives International
Institute of Management Accountants
The Institute of Internal Auditors

1. U.S. Securities and Exchange Commission, *Speech by SEC Chairman: Address to the Council of Institutional Investors*, 2009 (www.sec.gov/news/speech/2009/spch040609.html).
2. Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrated Framework*, September 2004, www.coso.org, New York, NY.