

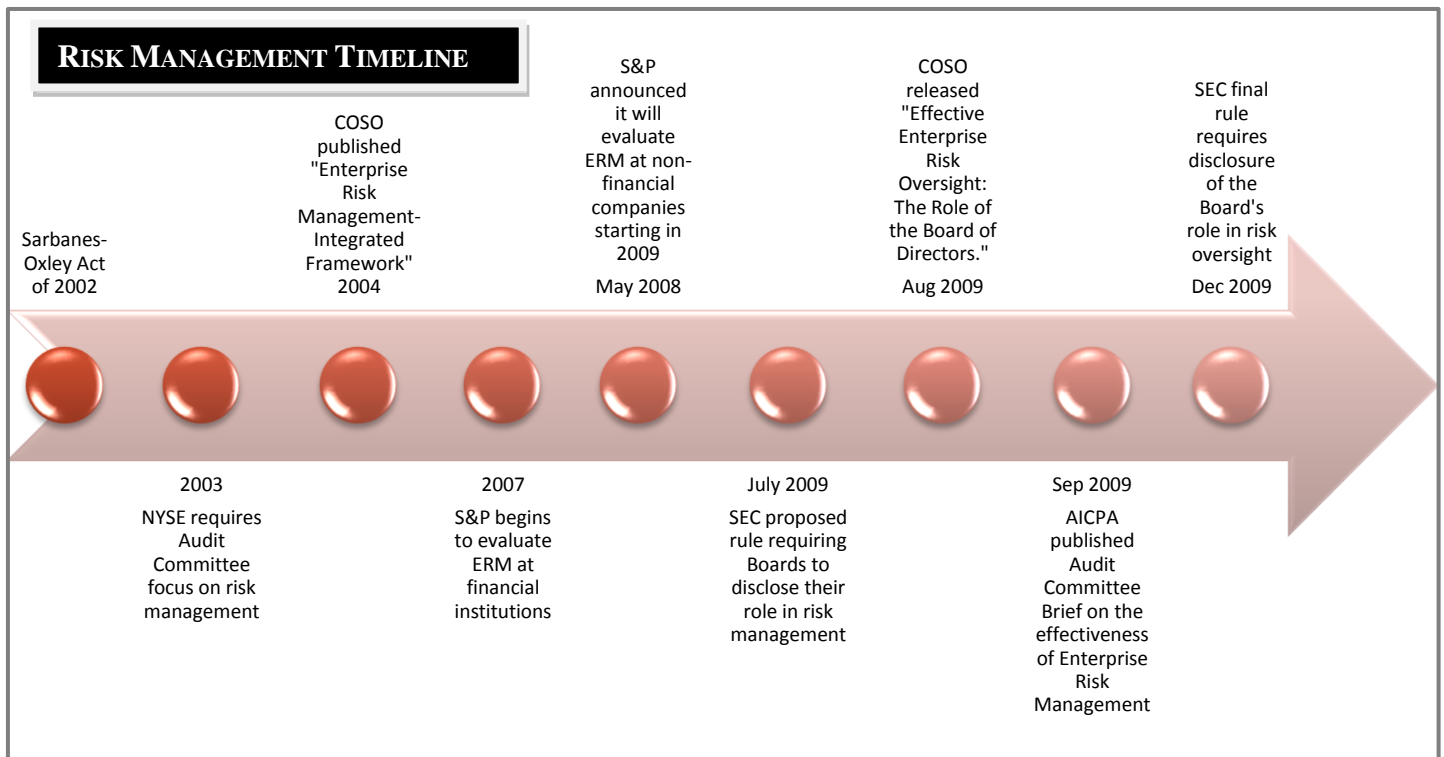


# The risk of Enterprise Risk Management

January 5, 2010  
 By Denise Sanders

The SEC gave final approval to a rule requiring disclosure of certain governance practices, including the Board's role in a company's risk oversight effective February 28, 2010. Other entities recently focusing on the topic of Enterprise Risk Management (ERM) include COSO, the AICPA, and Standard & Poor's credit rating agency. The main targets of concern are the Board and Audit Committee role and ensuring that Board's are addressing risk. The SEC rules provide vague requirements on how a Board or company should be addressing risk and simply require that the Board's role in risk oversight be described. For the Chief Financial Officer or Chief Audit Executive raising awareness to the Board and Audit Committee, the challenges that exist include little SEC or authoritative guidance on what risk management should include, very few benchmarks of companies implementing ERM, and potential litigation or public perception challenges around disclosure.

In this article, I've laid out how we got here, the guidance that exists, and questions that need to be addressed as a company moves toward a plan for addressing the new disclosure rules and implementing ERM.



## ERM BACKGROUND

The practice of risk management has been around a long time but its first real public appearance began after the Enron and WorldCom scandals in the early 2000s, which led to the development of the Sarbanes-Oxley (SOX) Act of 2002. Although entity-wide controls such as risk assessment, monitoring, and communication were part of the overall risk framework, the focus of SOX was on financial reporting risk. This was followed by the New York Stock Exchange governance rules requiring Audit Committees to discuss risk management policies and practices. The concept referred to as "Enterprise Risk Management" was coined by the Committee of Sponsoring Organizations of the Treadway Commission when they published "Enterprise Risk Management – Integrated Framework" in 2004. The COSO ERM framework defined risk broader than financial risk. This document defined ERM as a *"...process, effected by an 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 its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."* The COSO ERM Framework has eight Components and four objectives categories. It is an expansion of the COSO Internal Control-Integrated Framework published in 1992 and amended in 1994. The eight components are:

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring

The four objectives categories are:

- Strategic - high-level goals, aligned with and supporting the organization's mission
- Operations - effective and efficient use of resources
- Reporting - reliability of operational and financial reporting
- Compliance - compliance with applicable laws and regulations

## RECENT FOCUS

ERM has begun to receive more focus lately by Boards and regulators due to recent changes in our environment, including the recent banking financial crisis and recession of 2008/2009. Recent activity includes:

- The SEC proposed in July 2009 and finalized in December 2009 a ruling requiring Boards to disclose their role in the company's risk management process in proxy and information statements, annual reports and registration statements.
- The AICPA Audit Committee Effectiveness Center published an article on effective Enterprise Risk Management in September 2009.
- COSO released a thought paper, Effective Enterprise Risk Oversight: The Role of the Board of Directors in August 2009.
- Standard & Poors (S&P), the credit rating and equity research company announced its plans to include a series of questions about risk management in its company evaluation process. This started with financial companies in 2007. The results of this inquiry is one of the many factors considered in debt rating, which has a corresponding impact on the interest rates lenders charge companies for loans or bonds. On May 7, 2008, S&P also announced that it would begin including an ERM assessment in its ratings for non-financial companies starting in 2009.

## THE CHALLENGES OF ERM DISCLOSURE

The SEC approved rules relating to board leadership structure and the board's role in risk oversight require disclosure about:

- A company's board leadership structure, including whether the company has combined or separated the chief executive officer and chairman position, and why the company believes its structure is the most appropriate for the company at the time of the filing.
- In certain circumstances, whether and why a company has a lead independent director and the specific role of such director.
- The extent of the board's role in the risk oversight of the company.

Questions that companies must now answer for themselves in disclosing this information include:

- What is effective risk oversight? – While articles and whitepapers have been written by the AICPA and COSO, no authoritative/regulatory rules exist on what would be considered effective risk oversight or enterprise risk management practices.
- Does disclosure of the board's role in risk oversight present new bases for potential lawsuits by shareholders when the company has unfavorable results or surprises?
- How favorable or unfavorable is the public perception of delegation of risk oversight by the board to a risk committee or the audit committee?
- To what extent does the lack of a formal enterprise risk management program play in public perception? Many companies have been so focused on Sarbanes-Oxley over the past few years that a broader view of risk has been somewhat obscured. While risks are identified in Item 1A and the management discussion and analysis section of a company's 10-K, and companies inherently address some risks in their operations, many companies do not have formal programs to ensure they address these risks.
- Will companies that disclose a greater level of detail about their risk management practices be better or worse off in the market?
- If your company doesn't have an ERM program, what will you do to implement a program in the coming months? And will you disclose this in absence of an existing program?

### **About Sanders Consulting, LLC**

Sanders Consulting, LLC (SC) is a certified public accounting firm focused on business advisory services to middle-market companies. SC provides services through a high level of experience and expertise with the unique combination of CPA, business and technology skills. The goal of SC is to turn your strategy into results.

SC provides Enterprise Risk Management advisory services, including enterprise risk assessment, program management, organizational design, and ERM software implementation.

For more information on this article or Sanders Consulting, contact:  
Denise Sanders, [dsanders@sandersconsult.com](mailto:dsanders@sandersconsult.com), (713) 447-3623