1

COMPELLING REASONS FOR ENTERPRISE RISK MANAGEMENT

Now that you have seen that implementing risk management processes can be easily achieved through the seven steps outlined in the introduction, let's examine the current regulatory climate and how it allows public companies to easily leverage their existing COSO framework into a successful ERM programme.

Though President Bush signed the Sarbanes-Oxley Act into law in 2002 into law in response to numerous financial and accounting frauds such as those at Enron and WorldCom, there is no explicit regulatory requirement to implement a comprehensive system of risk management. The Sarbanes-Oxley Act required large publicly traded companies (above a certain market capitalisation) to adopt an internal control framework, conduct risk assessments and tests of controls for reliable financial reporting, and disclose the results of the risk assessments of internal control over financial reporting in their public filings with the Securities and Exchange Commission (SEC). Yet, the scope of this legislation is narrow in that it focuses on risks associated with financial reporting and not on the much broader topic of enterprise risk.

In response to this legislation, most public companies adopted the COSO Internal Control—Integrated Framework[1] and spent millions upon millions of dollars to implement and report on their respective systems of internal control to the SEC. Unfortunately, many companies treated Sarbanes-Oxley as a compliance requirement instead of an opportunity to strengthen risk management over this facet of their enterprise risk portfolio.

Since that time, other public, private, non-profit, and governmental organisations have embarked on implementing more robust systems of internal control over financial reporting, either as a direct response to boards of directors and those charged with oversight or in anticipation of further regulation.

Hence, when business leaders hear *COSO* or *enterprise risk management* or *ERM*, they tend to think, 'Is this just an expensive compliance exercise?' and 'Why does my company need this?' We think these are very fair questions that deserve thoughtful responses.

Risk management and control maturity are often driven by regulatory compliance. However, being reactive to regulation provides the wrong motive to manage risk and leads to overcontrol; because people don't 'buy into' the effort, it's not sustainable. Long-term success is predicated on behavioural change. Time spent helping people clearly see the risk to achieving objectives leads to better-designed controls, management buy-in, and sustainable processes. When risk management makes sense, one of the de facto by-products is regulatory compliance.[2]

We don't suggest a company attempt to establish any system of risk management simply for the sake of compliance. If compliance becomes the motivator, you will fail to get long-term buy-in from employees and the effort will not be sustainable. Rather, if more time were spent focusing on identifying risks to objectives and assessing their likelihood and potential impact against the organisation's known risk management strategies, you would tend to get buy-in because the reason for implementing robust risk management make sense. Said differently, risk management is directed at risk, not at compliance.

The impact of the recent recession, which began in 2008, highlights the downstream consequences that materially affected and crippled several companies in multiple industries, such as investment banking, deposit banking, mortgage lending, construction, automobiles, insurance, and so on. No doubt we will see increased legislation forcing companies to implement systems of risk management and internal control that are more robust.

That said, on December 16, 2009, the SEC amended its proxy disclosure requirements.[3]

The amendments require registrants to make new or revised disclosures about

- compensation policies and practices that present material risks to the company;
- stock and option awards of executives and directors;
- director and nominee qualifications and legal proceedings;
- board leadership structure;
- the board's role in risk oversight; and
- potential conflicts of interest of compensation consultants that advise companies and their boards of directors.

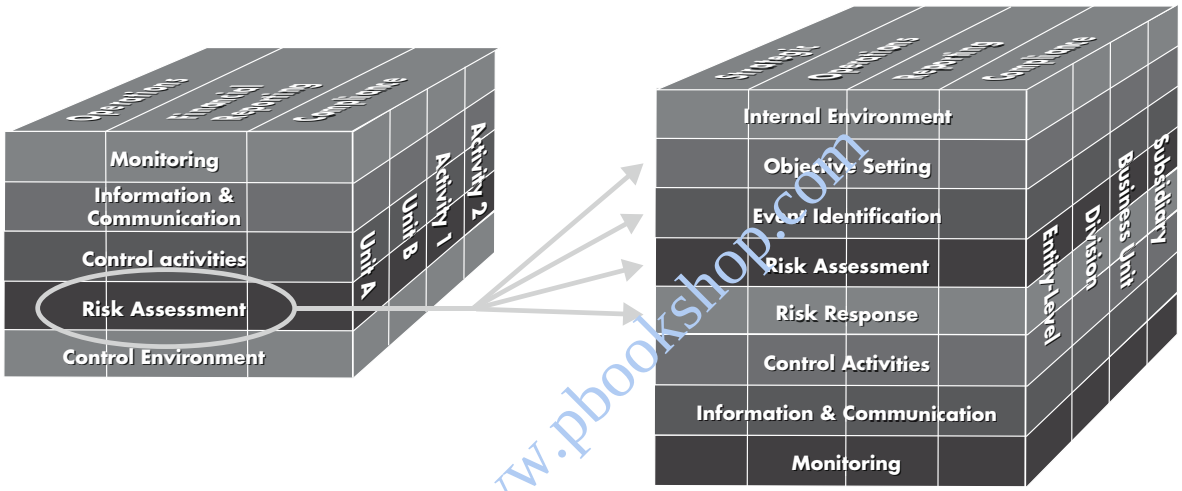
There have been numerous white papers and speeches from regulators, academics, and leaders in industry espousing greater risk management and risk oversight, several of which we reference in the appendixes. We believe it is only a matter of time before regulators, outside directors, and those charged with governance mandate that broader sections of industry implement ERM.

With that in mind, this publication demonstrates that you can implement a robust ERM system using the COSO ERM framework along with relatively straightforward risk concepts and simple desktop tools without spending millions of dollars.

Throughout this publication we expand on concepts contained in the COSO *Enterprise Risk Management—Integrated Framework* along with lots of practical application to assist you in developing your company's risk management system. An executive summary of COSO's *Enterprise Risk Management—Integrated Framework* that provides an overview of the key principles for effective ERM is available for free download at www.coso.org.

THE EVOLUTION OF THE COSO[4] INTERNAL CONTROL: INTEGRATED FRAMEWORK TO THE COSO ERM FRAMEWORK[5]

Most public companies should be able to leverage their existing COSO Internal Control—Integrated Framework to use the COSO ERM framework pictured below and introduced previously in exhibit 1-1. The ERM framework essentially adds a 'Strategic' objective category and breaks out the COSO component 'Risk Assessment' into four separate components: (1) objective setting, (2) event identification, (3) risk assessment, and (4) risk response as depicted in the following figure.



Endnotes

1 The Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed the widely accepted COSO *Internal Control—Integrated Framework*.

2 Quoted in the white paper *Is Enterprise Risk Management at a Crossroads?* Jointly Commissioned by the AICPA and CIMA, August 2010; Scott M. McKay CPA, CFE, CIA, CCSA, Director Corporate Audit, Cree, Inc.

3 SEC Release No. 33-9089 *Proxy Disclosure Enhancements*, Final Rule.

4 COSO *Internal Control—Integrated Framework*, September 1992, www.coso.org, New York, NY.

5 COSO *Enterprise Risk Management—Integrated Framework*, September 2004, www.coso.org, New York, NY.