AICPA® AUDIT COMMITTEE BRIEF
From the Audit Committee Effectiveness Center

January 2010

Adding Value, Not Bureaucracy: Linking Governance, Enterprise Risk Management and Internal Controls

Organizations are beginning to recover from the financial crisis of 2008, and many are instituting or improving practices that may help prevent another crisis (or lessen the impact, should another crisis occur). Risk management is the area most frequently targeted for improvement; many organizations are being asked by their boards, regulators or other stakeholders to reevaluate the way they are managing risk. Credit rating agencies such as Standard and Poor's have for more than a year assessed enterprise risk management (ERM) during analysis of corporate credit ratings. In addition, the SEC in December 2009 approved rules that will expand corporate proxy disclosure regarding risk management, compensation and corporate governance matters. This heightened focus on risk management practices and ERM's potential implementations has some corporate executives wondering if they will in the future face an even heavier compliance burden – or if building on existing processes will more effectively manage risk while creating value for the organization.

A primary driver of ERM-related concerns is confusion about what ERM means and how it applies to corporate governance and internal controls. If you start with an understanding of corporate governance as a broad system of structuring, operating and controlling an organization so it can achieve long-term goals to the satisfaction of shareholders and key stakeholders, then it is easy to see how a process of managing enterprise-wide risks is central to effective corporate governance. A key component of corporate governance is the board's responsibility to hold itself and management accountable to shareholders. (Usually, we think of the board and management as being held accountable for performance, but the recent financial crisis has shown we also must hold management accountable for the risks it takes in its quest to hit performance targets.) An effective ERM process helps management and the board to objectively consider their organization's overall appetite for risk, and ensures the organization's strategic objectives are consistent with that appetite. For example, a firm with a low appetite for risk should be setting more modest strategic objectives than a firm with a higher appetite for risk-taking.

Due to the planning, organizing and controlling that are central to risk management, ERM is focused more at the strategic level. However, ERM recognizes that businesses face risks all the time; therefore, establishing risk appetite and risk tolerance facilitates the decision-making process and clarifies responsibilities and accountabilities consistent with effective corporate governance. Internal controls, on the other hand, are more focused on the day-to-day-process level – they are a subset of ERM, which is a subset of corporate governance (as illustrated in the chart below):

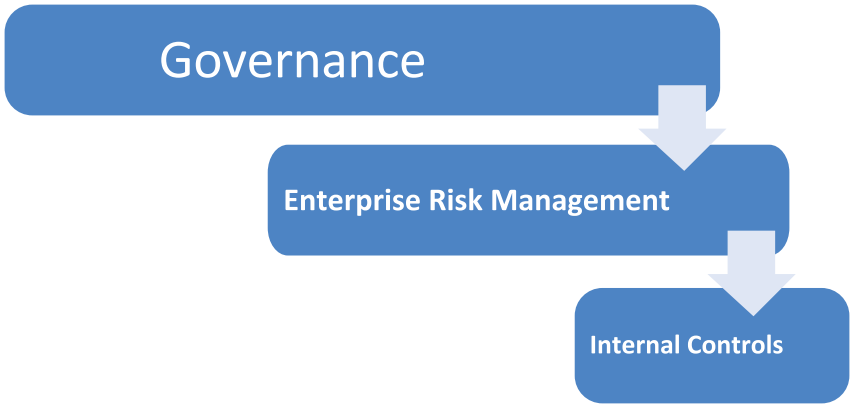
The AICPA and NC State's ERM Initiative are jointly hosting a 1½ -day workshop, Board and Senior Management Roles in Risk Oversight: Taking a Strategic View of the Enterprise, in New York, NY, October 14-15, 2010. **http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/PRDOVR~PC-AUDITCONF/PC-AUDITCONF.jsp**

AUDIT COMMITTEE BRIEF

From the **Audit Committee Effectiveness Center**

"Good corporate governance is a system in which those who manage a company — that is, officers and directors — are effectively held accountable for their decisions and performance. But accountability is impossible without transparency. By adopting these rules, we will improve the disclosure around risk, compensation, and corporate governance, thereby increasing accountability and directly benefiting investors."

– Mary L. Schapiro, SEC Chairman



Most organizations already have an effective system of internal controls that focuses on operations, reporting and compliance. ERM moves beyond internal controls in its connection to strategy-setting. The following chart compares the COSO definition of internal controls with the COSO definition of ERM, and highlights where ERM builds on and moves beyond internal controls:

Internal Controls	ERM
Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: • Operations – effectiveness and efficiency of operations. • Reporting – reliability of financial reporting. • Compliance – compliance with applicable laws and regulations	Enterprise risk management is 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 in four categories: • Strategic – high-level goals, aligned with and supporting its mission • Operations – effective, efficient use of resources • Reporting – reliability of reporting • Compliance – compliance with applicable laws and regulations

While internal control and ERM both have the purpose of providing greater assurance regarding the achievement of objectives, ERM is broadly applied: it takes an entity-level portfolio view of risks that will be considered in strategy-setting, as well as the organization's risk appetite.

It is also helpful to compare the components of internal control to the components of ERM, again as defined by COSO:

For more information:

From the SEC

SEC Approves Enhanced Disclosure About Risk, Compensation and Corporate Governance (Dec. 16, 2009) *sec.gov/news/press/2009/2009-268.htm*

Audit Committee Toolkits:

Public Companies
cpa2biz.com/AST/Main/CPA2BIZ_Primary/FinancialManagement/Management/AuditCommittee/PRDOVR~PC-991001/PC-991001.jsp

Private Companies
cpa2biz.com/AST/Main/CPA2BIZ_Primary/FinancialManagement/Management/AuditCommittee/PRDOVR~PC-991007/PC-991007.jsp

Not-for-Profit Organizations
cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/AuditPreprationandPlanning/PRDOVR~PC-991004/PC-991004.jsp

Government Organizations
cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/AuditPreprationandPlanning/PRDOVR~PC-991005/PC-991005.jsp

Internal Control	ERM
Control Environment	Internal Environment
	Objective-setting
Risk Assessment (and identification)	Risk Identification
	Risk Assessment
	Risk Response
Control Activities	Control Activities
Information and Communication	Information and Communication
Monitoring	Monitoring

Two additional key components of ERM are: the role ERM plays in setting objectives by accounting for the organization's existing risks and appetite for risk, and the choice of response to risks – again based on the organization's risk appetite. Internal controls are one means of responding to risks, but there are numerous others as well, such as insurance programs, disaster recovery plans, financial hedges, diversification efforts, etc.

How can a firm implement ERM so it will add value to shareholders' satisfaction? An important first step is developing a list of the top risks facing an organization – and then, prioritizing those risks based upon the expected severity of impact and likelihood of occurrence. Organizations should leverage risk-assessment work that has already been done by their independent and internal auditors. That top-level risk list can be used in strategy-setting, to help the organization consider how new strategic initiatives could add or reduce existing risks. It should also be used in communications with the board, to assist the board with its oversight role. Having a shared understanding of the most significant risks should also help the organization focus on the best way to monitor those risks going forward – and to formulate a response plan *before* a risk event occurs. As the organization realizes value from these simple first steps, it can begin to extend ERM further into the organization and, ultimately, develop greater sophistication in its risk management processes by embedding ERM in the decision-making process and culture of the company.

Author Bio

Bonnie Hancock is the executive director of the NC State University Enterprise Risk Management (ERM) Initiative and a lecturer in accounting at NC State's College of Management. She also is a director of AgFirst Farm Credit Bank and a consultant to boards and senior management teams on matters involving ERM and strategic planning. Her background includes executive positions at Progress Energy and Exploris Museum: she served as president of Exploris; at Progress Energy, she was president of Progress Fuels (a Progress Energy subsidiary with more than $1 billion in assets), senior vice president of finance and information technology, vice president of strategy, and vice president of accounting and controller. She offers insight on boards and executive management and practical perspectives on managing risk across increasingly complex global enterprises.