ENTERPRISE RISK MANAGEMENT (ERM) – FAILURE IS NOT AN OPTION

Robert B. Matthews, Sam Houston State University
Ronald J. Daigle, Sam Houston State University
Paul Vanek, Sam Houston State University

ABSTRACT

The Enterprise Risk Management (ERM) framework provides a useful framework for planning, conducting, and evaluating risk management evolutions in a wide range of enterprises. This paper addresses an overview of ERM, including background, conceptual framework, implementation guidance, and thoughts for future consideration.

INTRODUCTION

> *"You want a valve that doesn't leak and you try everything possible to develop one. But the real world provides you with a leaky valve. You have to determine how much leaking you can tolerate."*
>
> *Obituary of Arthur Randolph, January 3, 1996*

In September 1992 (amended 1994) the Committee of Sponsoring Organizations (COSO) of the Treadway Commission published *Internal Control – Integrated Framework (COSO-IC)*, the result of a project begun in 1987 to develop integrated guidance on internal control. This publication presented a common definition of internal control and a framework for evaluating and improving internal control systems. COSO-IC defined internal control as "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:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations (COSO, 1992)."

In addition to the above three internal control objectives, COSO-IC identified five components of internal control (COSO, 1992):

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

The COSO-IC framework gained widespread acceptance. It became the predominant standard used by U.S. companies use to evaluate their compliance with the Foreign Corrupt Practices Act of 1977 (FCPA). According to a poll by CFO Magazine released in 2006 (Shaw, 2006), 82% of respondents claimed they used COSO-IC for their internal control framework. Other frameworks identified by respondents included COBIT (Control Objectives for Information and Related Technology) 33%, AS2 (Auditing Standard No. 2, PCAOB) 28%, and SAS 55/78 (AICPA) 13%.

Following the turn of the millennium, several high-profile business scandals and failures (Enron, Tyco, Adelphia, Peregrine, and WorldCom) led to enactment of the Sarbanes-Oxley Act of 2002 (SOX), which extends the long-standing requirement for public companies to maintain systems of internal control and requires management to certify and the independent auditor to attest to the effectiveness of those systems. COSO-IC became the broadly accepted standard for satisfying those reporting requirements.

In response to accompanying calls for enhanced corporate governance and risk management, in 2004 COSO published *Enterprise Risk Management - Integrated Framework (COSO-ERM),* which defines enterprise risk management (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 (COSO, 2004, p. 2)." COSO-ERM expanded the earlier definition of internal control to provide a more robust and extensive focus on the broader subject of ERM. COSO-ERM expanded the objectives identified in COSO-IC, to include Strategic in addition to COSO-IC's Operations, Reporting, and Compliance (COSO, 2004, p. 3).

COSO-ERM also modified the internal control components identified in COSO-IC, and increased the number from five to eight, as follows (COSO, 2004, pp. 3-4):

- Changed Control Environment to Internal Environment
- Added Objective Setting, Event Identification, and Risk Response
- Retained Risk Assessment, Control Activities, Information and Communication, and Monitoring

While COSO-IC focused on component units within the enterprise, COSO-ERM focuses on the enterprise level and intermediate division or subsidiary levels as well as the individual component units.

The changes in emphasis resulting from these differences between COSO-IC and COSO-ERM are summarized as follows:

COSO-IC	COSO-ERM
Rules-based, bottom-up approach, at least initially.	Top-down, holistic, principles-based approach.
Focus on controls over transactions.	Focuses on risks associated with events.
When used for SOX compliance purposes, does not specifically address operational, strategic or compliance risks not related to financial reporting.	Specifically addresses operational, strategic, and compliance risks as well as financial reporting risks.

Like the earlier COSO-IC framework, the COSO ERM framework is also gaining increasing acceptance as a standard for risk management in various enterprises.

A somewhat different approach was taken by the Casualty Actuarial Society (CAS) in 2003. CAS defined ERM as the "discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organization's short- and long-term value to its stakeholders (ERM Committee, 2003, p. 8)." CAS conceptualized ERM as proceeding across the two dimensions of risk type and risk management processes (ERM Committee, 2003, p. 8). The risk types and examples include (ERM Committee, 2003, pp. 9-10):

- Hazard risk (tort liability, property damage, natural catastrophe)
- Financial risk (pricing risk, asset risk, currency risk, liquidity risk)
- Operational risk (customer satisfaction, product failure, integrity, reputational risk)
- Strategic risks (competition, social trends, capital availability)

The CAS risk management process involves (ERM Committee, 2003, pp. 11-13):

- Establishing Context: This includes an understanding of the current conditions in which the organization operates on an internal, external and risk management context.
- Identifying Risks: This includes the documentation of the material threats to the organization's achievement of its objectives and the representation of areas to the organization may exploit for competitive advantage.
- Analyzing/Quantifying Risks: This includes the calibration and, if possible, creation of probability distributions of outcomes for each material risk.

- Integrating Risks: This includes the aggregation of all risk distributions, reflecting correlations and portfolio effects, and the formulation of the results in terms of impact on the organization's key performance metrics.
- Assessing/Prioritizing Risks: This includes the determination of the contribution of each risk to the aggregate risk profile, and appropriate prioritization.
- Treating/Exploiting Risks: This includes the development of strategies for controlling and exploiting the various risks.
- Monitoring and Reviewing: This includes the continual measurement and monitoring of the risk environment and the performance of the risk management strategies.

Other risk frameworks in use throughout the world include (Schanfield & Helming, 2008):

- AIRMIC – Association of Insurance and Risk Managers
- ALARM – The National Forum for Risk Management in the Public Sector (UK)
- AS/NZ 4360:2004 (Australia/New Zealand)
- British Standard 31100
- CoCo – Criteria of Control (Canada)
- Combined Code on Corporate Governance (UK)
- FERMA – Federation of European Risk Management Associations
- Internal Control (Hong Kong)
- IRM – Institute of Risk Management
- ISO 31000 (International Organization for Standardization)
- King Report on Corporate Governance (King 1)
- King Report on Corporate Governance in South Africa (King 2)
- Risk and Insurance Management Society (RIMS) Risk Maturity Model

Risk management expert Felix Kloman defines risks as, "a measure of the probable likelihood, consequences (favorable and unfavorable), and timing of a future event or situation that would affect the company (Kloman, Felix, quoted in Schanfield & Helming, 2008)." Such a definition focuses upon both the downside risk and the upside opportunity.

BACKGROUND

A review of how things have changed since the 1970s provides some perspective as to the significance of risk management:

1970s	End of Vietnam War Yom Kippur War and first Arab oil embargo, 1973 Dow-Jones Industrial Average (DJIA) high of 1011, 1976 Foreign Corrupt Practices Acts (FCPA), 1977 Fall of the Shah of Iran, US Embassy hostage situation, Iranian oil embargo, 1979 Oil increased from $5/bbl to $15/bbl over the decade
1980s	The "Reagan Years" IBM PC, 1981 DJIA low of 776, 1982 Oil $20/bbl, mid-80s DJIA high of 2722, 1987 Stock market crash, 1987 COSO begins research into fraudulent financial reporting, 1987 Fall of Berlin Wall, 1989
1990s	Desert Storm, 1991 COSO-IC released, 1992 Development of the Internet Fall of Barings Bank, 1997 Oil $10/bbl, 1997 COSO concludes research, 1997 Fall of Long Term Capital Management, 1998 First DJIA close over 10000, 1999 Y2K efforts, 1999-2000
2000	DJIA high of 11723 Dot-Com bubble burst
2001	Terrorist attack of 9/11 Fall of Enron Basel II Accords introduced
2002-03	Fall of Arthur Andersen, WorldCom, and Adelphia Sarbanes-Oxley Act of 2002 DJIA low of 7286, 2002 Continued political unrest Global "War on Terrorism" CAS-ERM issued, 2003 Oil $30/bbl
2004	Auditing Standard 2 (AS2) released by PCAOB First year for SOX 404 compliance for large public companies COSO-ERM released Oil $50/bbl
2005-06	AS2 required for external auditors Oil $79/bbl, 2006

2007	Audit Standard 5 (AS5) supersedes AS2 DJIA high of 14164 Oil $99/bbl
2008	Global recession Failure of US financial institutions and TARP response Oil $120/bbl
2009	DJIA low of 7062 Economic stimulus plan Increase in pirate activity in Indian Ocean Christmas Day aircraft bomb attempt over Detroit, Michigan Oil $50-$70/bbl
2010	Blowout of Mississippi Canyon 252 oil well operated by BP Times Square truck bomb attempt

Flowing through those events are the following general trends that must be kept in mind in comparing the need for a more rigorous ERM today than previously:

YESTERDAY	TODAY
Simpler times	Requirements, systems, and tools are more complex
Frequent breakdowns occurred within companies, but repairs could be made without computer scientists, engineers, attorneys, environmental experts, accountants, and financial analysts. Failure in one area of the business seldom directly impacted another area	Breakdowns can lead to a significant "domino effect" with far-reaching consequences
Hazards which ultimately resulted in losses were easier to contain.	Media's role has changed from observer to a catalyst of negative public opinion

In November 2007, Standard & Poor's (S&P) announced a Request for Comment: Enterprise Risk Management Analysis for Credit Ratings of Non-financial Companies (Dreyer & Ingram, 2007). When the comment period closed in March 2008, over 90 responses had been received. The comments generally supported S&P's proposal to introduce ERM analysis for non-financial companies. In May 2008 S&P announced that they would want to include ERM in its evaluation of non-financial companies. During the third and fourth quarters of 2008, S&P worked to develop benchmark and evaluation criteria. In 2009, S&P began to include ERM in its evaluation of credit ratings. S&P focused on the risk management culture and strategic risk management. S&P views ERM as a gauge of the quality of management at the helm.

Also in November 2007, S&P reported on its ERM evaluation process for insurers (Santori, Bevan, & Myers, 2007). This reflected the results of a pilot program conducted by S&P that included 78 insurance companies. The composition of the pilot companies was 37% property and

casualty, 21% life, 13% reinsurance, 12% health, 12% multiline, and 1% mortgage insurers. The S&P ratings breakdown was 13% AA and AAA, 45% A, and 42% BBB and lower. S&P found the quality of risk management to be as follows (Santori, Bevan, & Myers, 2007):

8%	Excellent	Master of controls, preparations for unknown future risks, and strategic applications
24%	Strong	Basic risk controls in place for all major risks, plus processes to prepare for unknown future risks and to make strategic choices among risks based on risk/reward framework
62%	Adequate	Basic risk controls in place for all major risks
6%	Weak	Lacking basic controls for important risk(s)

S&P also found that in assessing the ERM impact on ratings (Santori, Bevan, & Myers, 2007):

5%	ERM evaluations strengthened the ratings
25%	ERM evaluations affirmed or supported ratings
65%	ERM evaluations were neutral to ratings
5%	ERM evaluations were negative to ratings

Comparison of these two sets of results suggests a possible correlation between findings and ratings, as follows:

Findings		Impact	
Excellent	8%	5%	Strengthen
Strong	24%	25%	Affirm/support
Adequate	62%	65%	Neutral
Weak	6%	5%	Negative

The crisis in the global banking industry provides an obvious recent example of the consequences of failure to assess enterprise risks effectively. This sector once claimed leadership in risk management. That reputation has been lost in a flurry of bad loan portfolios, failed banks, nationalization/bailouts of some banks, and shotgun mergers of others. Several prominent organizations have weighed in with analyses of what went wrong (Baker, 2008).

The Financial Stability Forum (FSF) issued a report on 2 April 2009, "FSF Principles for Sound Compensation Practices," which stated in part (FSF, 2009):

- "Compensation practices at large financial institutions are one factor among many that contributed to the financial crisis that began in 2007. High short-term profits led to generous bonus payments to employees without regard to the longer-term risks they imposed on their firms. These perverse incentives amplified the excessive risk-taking that severely threatened the global financial system and left firms with fewer resources to absorb losses as risks materialized. The lack of attention to risk also contributed to the large, income cases extreme, absolute level of compensation in the industry."
- "To date, most governing bodies (henceforth, 'board of directors') of financial firms have viewed compensation systems as being largely unrelated to risk management and risk governance. This must change."
- "As a practical matter, most financial institutions have viewed compensation systems as being unrelated to risk management and risk governance."

Shortly after the FSF report, the Institute of International Finance (IIF) issued a report stating that the crisis "raised questions about the ability of certain bank boards to oversee senior managements and to understand and monitor the business (Baker, 2008)."

The Economist Intelligence Unit (EIU) surveyed banks worldwide and reported that only 18% had an ERM strategy in place that was "well-formulated and rolled out across the business (Baker, 2008)."

The Association of Chartered Certified Accountants (ACCA) reported that (ACCA 2008):

- The principal source of the global credit crunch is a failure of corporate governance at banks, which encouraged excessive short-term thinking and blindness to risk.
- Risk management and remuneration/incentive systems must be linked. Executive bonus payments should be deferred until there is incontrovertible evidence that profits have been realized, cash received, and accounting transactions cannot be reversed.

Bruce Caplain has identified three factors that are imperative in an enterprise's ERM effort (Caplain, 2008):

- Management's commitment, including the Board
- The enterprise's governance structure of oversight functions that focus on risk and on identifying and mitigating issues
- The design of the enterprise's ERM effort—is it just another program, or is the risk mind-set fully embedded?

As suggested by the foregoing, the value of ERM may be at its greatest during times of economic decline or crisis. Several factors operate:

- The changing risk environment (KPMG 2008)
  - Arguably there have never been more risks to a business than there are in the current marketplace.
  - Even leaving aside today's prevailing concerns around the credit crunch, consider the following:
    - Technology entering new markets
    - Changing consumer habits
    - New products
    - Dealing with emerging economies.
  - These are all aspects of business which carry far greater risks than they used to, thanks to the effects of globalization and a more demanding end-user.

- Increased scrutiny from legal and regulatory agencies (Wheeler & Yoo 2009)
  - SEC
  - Department of Justice
  - Stock exchanges
  - Securities fraud trial lawyers
  - Sections 302 and 404 of the Sarbanes-Oxley Act
  - Foreign Corrupt Practices Act of 1977
  - Industry-specific regulations (privacy, anti-money-laundering, risk-based capital requirements)

- Increased criticism from shareholders and other stakeholders (Wheeler & Yoo 2009)
  - Outsourcing/third party resources
  - Credit rating agencies
  - Institutional investors
  - Personal liability for Board members

CONCEPTUAL FRAMEWORK

The COSO-IC, COSO-ERM, and CAS-ERM structures share many common elements. The CAS-ERM risks can be related to the COSO-IC and COSO-ERM objectives, as follows:

COSO-IC OBJECTIVES	COSO-ERM OBJECTIVES	CAS-ERM RISKS
	Strategic	Strategic risk
Operations	Operations	Operational risk
Financial Reporting	Financial Reporting	Financial risk
Compliance	Compliance	Hazard risk

Similarly, the CAS-ERM process can be related to the COSO-IC and COSO-ERM components, as follows:

COSO-IC COMPONENTS	COSO-ERM COMPONENTS	CAS-ERM PROCESSES
Control Environment	Internal Environment	Establishing Context
	Objective Setting	
	Event Identification	Identifying Risks
Risk Assessment	Risk Assessment	Analyzing/ Quantifying Risks
	Risk Response	Integrating Risks
		Assessing/ Prioritizing Risks
Control Activities	Control Activities	Treating/ Exploiting Risks
Information and Communication	Information and Communication	
Monitoring	Monitoring	Monitoring and Reviewing

This suggests a conceptual framework as follows:

- Establishing environment/context
  - Establish management's philosophy regarding risk, recognizing that unexpected as well as expected events may occur
  - Establish the entity's risk tolerance and risk culture
  - Consider how all aspects of the entity's activities may impact the risk culture

- Setting objectives
  - Consider risk strategy in setting management objectives
  - Determine at a high level how much risk management and the board of directors are willing to accept
  - Align risk tolerance with risk appetite

- Identifying events/risks
  - Identify both internal and external occurrences that can affect strategy and achievement of objectives
  - Differentiate risks (possible negative effects) and opportunities (possible positive effects)
  - Note that a particular event may have both risk and opportunity components

- Assessing/analyzing/quantifying risks
  - Utilize both quantitative and qualitative approaches
  - Understand the extent to which events may impact objectives
  - Assess risks for both likelihood and impact

- Responding/integrating/prioritizing risks
  - Once a risk has been identified and analyzed, there are several alternatives for treating the risk:
    - Accept the risk.
      - Management "self-insures" by doing nothing
      - Accepts implications
    - Avoid the risk
      - Management eliminates the activity
    - Transfer, share, outsource the risk
      - Financial risks – Use of derivatives, hedging or insurance
      - Operational risks – Use of third parties to perform
        - Payroll processing
        - Manufacturing
        - Other back office
    - Mitigate the risk – Fix the problems
  - Evaluate the options in relation to
    - The entity's risk appetite
    - Costs vs. benefits of various responses
    - Effects of alternatives on impact and likelihood of risks
  - Select and execute the most appropriate response

- Controlling/treating risks and exploiting opportunities
  - Implement policies and procedures to ensure that management's risk tolerance and other management directives are carried out
  - Occur throughout the organization, at all levels, and in all functions
  - Include both information technology controls and application controls

- Recording, reporting, and communicating information
  - Identify, capture, and communicate relevant information in a form and on a timetable to assist stakeholders in carrying out their duties and responsibilities and evaluating opportunities
  - Communicate down, across, and up the organization

- Monitoring and reviewing
  - Conduct continuous ongoing management reviews and separate examinations to ensure the proper functioning of other ERM components
  - Adjust scope of monitoring and reviewing activities to reflect ongoing risk assessment

The elements of the process may be viewed in matrix form, as follows:

	Strategic	Operations	Financial Reporting	Compliance
Establishing environment/context	√	√	√	√
Setting objectives	√	√	√	√
Identifying events/risks	√	√	√	√
Assessing/analyzing/quantifying risks	√	√	√	√
Responding/integrating/prioritizing risks	√	√	√	√
Controlling/treating risks and exploiting opportunities	√	√	√	√
Recording, reporting, and communicating information	√	√	√	√
Monitoring and reviewing	√	√	√	√

IMPLEMENTATION GUIDANCE

The conceptual approach to implementing ERM includes the following stages:

- Planning
  - Understand the entity's environment, business model, and risk management process
  - Understand and document the entity's tone at the top and risk appetite
    - Determine risk philosophy
    - Survey risk culture
    - Consider entity's organizational integrity and ethical values

- Establish the ERM organization within the enterprise
  - Decide roles and responsibilities
  - Designate Chief Risk Officer with sufficient power to facilitate accomplishment of objectives

- Risk Assessment
  - Conduct enterprise risk assessment
    - Interviews
    - Facilitated sessions
    - Documentation
  - Train appropriate personnel for ongoing risk management activities
  - Assess risks
    - Identify
    - Measure
    - Prioritize
  - Manage risks
    - Control
    - Share or transfer
    - Diversify
    - Avoid

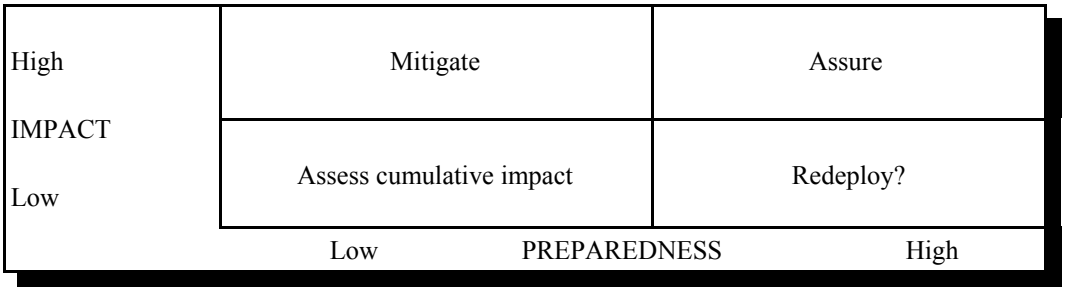
- Risk Response/Mitigation
  - Implement corrective plans/activities
  - Monitor risks
    - Process level
    - Activity level
    - Entity level
  - Monitor ongoing program development and implementation

The appropriate approach to various risk reaction and control activities depends upon the impact of the related risks and the entity's evaluation of the extent to which each of those activities prepares the entity to deal with the risk.

- If a risk has high potential impact, and the enterprise is not well prepared to handle it, immediate mitigation/remediation is required.
- If a risk has high potential impact, but the enterprise is well prepared to handle it, steps must be taken to assure that preparedness is maintained.

- If a risk has low potential impact, and the enterprise is not well prepared to handle it, immediate mitigation/remediation may not be necessary, unless a number of such risks may have a significant cumulative effect.
- If a risk has low potential impact, and the enterprise is well prepared to handle it, there is a reasonable question whether certain of the enterprise's assets and capabilities might better be redeployed to deal with more pressing risks.

This can be shown graphically as follows:



A third dimension, the likelihood that the risk will materialize, should also be considered. This may be considered in conjunction with the potential impact, so that the approach is weighted more heavily toward likely impact rather than maximum potential impact.

Common faults in implementing ERM have been found to be:

- Lack of visible, active support from Board and/or C-level management
- Implementing without a framework or plan
- Organization not ready – too much too soon
- Lack of integration with business goals and objectives
- Implementing as a project or part-time endeavor
- Failure to address the need for change management
- Failure to drive ERM to its full potential

By contrast, ERM success factors have included:

- Strong, visible support from C-level management
- Alignment of ERM to the key strategic and financial objectives and business processes
- Dedicated team of cross-functional staff to integrate ERM into significant business practices / processes
- Recognition that ERM is a continuous process and takes time to evolve

- Adequate training and supporting tools
- Leveraging well-accepted processes within the organization and introducing ERM as a value-add rather than a new stand-alone program

The changes that are required include (Wheeler & Yoo 2009):

- Clear and consistent support from Executive Management and the Board
- Long-term commitment to ERM, linked to strategic planning
- Building ERM into business processes efficiently and without undue administrative burden
- Well defined roles and responsibilities for risk, leading to improved accountability
- Risk considerations built into incentives and performance management

THOUGHTS FOR CONSIDERATION

Enterprises should consider the following thoughts with respect to their ERM effort:

- What is the number one risk facing your company today? (Wheeler & Yoo, 2009)
  - Reputational
  - Operational (technology, human capital, physical security)
  - Regulatory/legal
  - Market
  - Credit
  - Disaster (natural, terrorism)

- What is your enterprise's philosophy towards risk? (Wheeler & Yoo 2009)
  - Risk assessment
    - Annual point-in-time snapshot
    - Internal audit driven
    - Focus on current issues
  - ERM
    - Real-time, ongoing assessment
    - Continuous risk monitoring
    - Ownership of risk by process owners, embedded in the business

- How has risk management evolved in your organization? (Wheeler & Yoo 2009)
  - Developing
  - Implementing

- Improving
- Integrating

- What is the number one change barrier to overcome in your organization? (Wheeler & Yoo 2009)
  - People
    - Lack of time/skills/resources
    - Difficulty obtaining buy-in from employees
    - Lack of management support
  - Processes
    - Regulatory complexity
    - Difficulty defining risk appetite
    - Unclear lines of responsibility
  - Information
    - Lack of available data
    - Threats from unknown/unforeseeable risks
    - Difficulty in identifying emerging risks

- How can you and your group foster an ERM culture within your organization?

S&P has proposed the following questions for management meetings (S&P, 2009):

- What are the company's top risks, how big are they, and how often are they likely to occur? How often is the list of top risks updated?
- What is management doing about top risks?
- What size quarterly operating or cash loss has management and the board agreed is tolerable?
- Describe the staff responsible for risk management programs and their place in the organization chart. How do you measure success of risk management activities?
- How would a loss from a key risk impact incentive compensation of top management on planning/budgeting?
- Tell us about discussions about risk management that have taken place at the board level or among top management when making strategic decisions.
- Give an example of how your company has responded to a recent "surprise" in your industry and describe whether the surprise affected your company differently from others.

The following questions must be answered if ERM is to be made "real" for an enterprise (Baker 2008):

- What do we want to accomplish?
- What could stop us from accomplishing it?
- What should we do to make sure that those things either (1) don't happen, or (2) can be managed if they do happen?

CONCLUSION

As the complexity of modern life, and the speed with which things happens, increases continuously, the need for an effective ERM is steadily and continuously increasing. In implementing ERM, the most important consideration may be to remember what ERM is and can do, and perhaps more importantly, what it is not and cannot do.

Consistent with this discussion, ERM is about:

- Identifying and assessing key risks
- Designing and implementing processes by which those risks can be managed
- Maintaining residual risks at a level acceptable to the organization
- Linking risks back to the organizational objectives

Just as importantly, ERM is not:

- A silver bullet against bad judgment
- A once a year event
- A stand-alone, one-off initiative
- A guarantee that goals and objectives will be achieved

REFERENCES

Association of Chartered Certified Accountants (ACCA) (2008). Climbing out of the credit crunch. Retrieved May 11, 2010, from http://www.accaglobal.com/pdfs/credit_crunch.pdf

Baker, N. (2008). Real-world ERM. *Internal Auditor, 65*(6), 32-37.

Caplain, Bruce (2008). "Risk Management: Why it Failed, How to Fix It," *Internal Auditor*. Retrieved May 11, 2010 from http://www.theiia.org/intAuditor/free-feature/2008/risk-management-why-it-failed-how-to-fix-it-ii/.

Committee of Sponsoring Organizations (COSO) of the Treadway Commission (1992). *Internal control – integrated framework*. New York, NY: American Institute of Certified Public Accountants.

Committee of Sponsoring Organizations (COSO) of the Treadway Commission (2004). Enterprise risk management – integrated framework: Executive summary. Retrieved May 11, 2010, from www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf

Dreyer, S.J. & D. Ingram (2007). *Request for comment: Enterprise risk management analysis for credit ratings of nonfinancial companies*, New York, NY: Standard & Poor's (November 15).

Enterprise Risk Management Committee (2003). *Overview of enterprise risk management*. Arlington, VA: Casualty Actuarial Society (May).

Financial Stability Forum (FSF) (2009). FSF principles for sound compensation practices. (2 April). Retrieved May 11, 2010, from http://www.financialstabilityboard.org/publications/r_0904b.pdf

KPMG (2008). Value creation in a changing environment. Retrieved May 11, 2010 from http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Pages/Value-creation-in-a-changing-risk-environment.aspx

Santori, L., K. Bevan & C. Myers (2007). *Summary of standard & poor's enterprise risk management evaluation process for insurers*. New York, NY: Standard & Poor's (November 15).

Schanfield, A. & D. Helming (2008). 12 ERM implementation challenges. *Internal Auditor, 65*(6), 41-44.

Shaw, H. (2006). The trouble with COSO: Critics say the Treadway Commission's controls framework is outdated, onerous, and overly complicated. But is there an alternative? *CFO Magazine* (March 15), retrieved on May 11, 2010, from http://www.cfo.com/printable/article.cfm/5598405

Simmons, M.R. (1997). COSO based auditing. *Internal Auditor, 54*(6) 68-72.

Standard & Poor's (2008). Enterprise risk management – rating agency view. Seminar presentation.

Standard & Poor's (2009). Discussion questions for management meetings. Seminar presentation.

Wheeler, J.A., & K.K. Yoo (2009). Enterprise risk management: what's new and what's next. Institute of Internal Auditors webinar (19 February).