9th International Conference on Recent Innovations in Science, Engineering and Management
Dhruva Institute of Engineering and Technology, Nalgonda, Telangana (RISEM-17)
28th -29th January 2017, www.conferenceworld.in ISBN: 978-93-86171-22-1

OVER VIEW OF ENTERPRISE RISK MANAGEMENT

V.Ramesh Naik[1], Y.Prathyusha[2], Y.Neeraja[3]

[1]*Assistant Professor of Gates Institute of Technology Gooty*

[2,3] *PG Student of Gates Institute of Technology Gooty*

ABSTRACT

The development of an enterprise risk management (ERM) program enables companies to manage corporate risks in a holistic manner as opposed to the silo-based perspective in traditional risk management frameworks. One main question in this regard is what factors drive the implementation of an ERM system in companies and whether ERM programs can actually create value once implemented. ownership are significantly positively related to the implementation of ERM in most empirical studies and, furthermore, that ERM generally has a (significant) positive impact on corporate value and performance.

Enterprise risk management (ERM) refers to a set of processes that enables the effective management of the risks, opportunities, and expected and unexpected events that may affect the enterprise. The successful implementation of ERM is a challenging task in part because it requires collaboration among multiple business units of different sizes, scope, and capability, each facing what it perceives as unique risks. Other difficulties with ERM implementations include lack of adoption of an enterprise-wide governance model, lack of a common risk language (e.g., taxonomy), and uneven levels of maturity within an organization regarding the management of risks. The risk taxonomy provides a foundation for clear and concise communication about risk across the enterprise to enable better risk management. The ERM maturity model, and its associated capability assessment, allows an organization to determine gaps in its current risk management processes and define ways to improve those ERM capabilities. Together, these three frameworks are key enablers for a successful ERM implementation and ongoing operation.

Keywords: Enterprise risk management, Taxonomy, Current risk management, scope, capability

I. INTRODUCTION

Enterprise risk management (**ERM** or **E.R.M.**) in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.

ERM can also be described as a risk-based approach to managing an enterprise, integrating concepts of internal control, the Sarbanes–Oxley Act, and strategic planning. ERM is evolving to address the needs of various stakeholders, who want to understand the broad spectrum of risks facing complex organizations to ensure they

ISBN: 978-93-86171-22-1

are appropriately managed. Regulators and debt rating agencies have increased their scrutiny on the risk management processes of companies

ERM frameworks defined

There are various important ERM frameworks, each of which describes an approach for identifying, analyzing, responding to, and monitoring risks and opportunities, within the internal and external environment facing the enterprise. Management selects a *risk response strategy* for specific risks identified and analyzed, which may include:

1. Avoidance: exiting the activities giving rise to risk
2. Reduction: taking action to reduce the likelihood or impact related to the risk
3. Alternative Actions: deciding and considering other feasible steps to minimize risks.
4. Share or Insure: transferring or sharing a portion of the risk, to finance it
5. Accept: no action is taken, due to a cost/benefit decision

Monitoring is typically performed by management as part of its internal control activities, such as review of analytical reports or management committee meetings with relevant experts, to understand how the risk response strategy is working and whether the objectives are being achieved.

Casualty Actuarial Society framework

In 2003, the Casualty Actuarial Society (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."[1] The CAS conceptualized ERM as proceeding across the two dimensions of *risk type* and *risk management processes.*[1] The risk types and examples include:[2]

Hazard risk

Liability torts, Property damage, Natural catastrophe

Financial risk

Pricing risk, Asset risk, Currency risk, Liquidity risk

Operational risk

Customer satisfaction, Product failure, Integrity, Reputational risk; Internal Poaching; Knowledge drain

Strategic risks

Competition, Social trend, Capital availability

The risk management process involves:

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

ISBN: 978-93-86171-22-1

4. **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.
5. **Assessing/Prioritizing Risks:** This includes the determination of the contribution of each risk to the aggregate risk profile, and appropriate prioritization.
6. **Treating/Exploiting Risks:** This includes the development of strategies for controlling and exploiting the various risks.
7. **Monitoring and Reviewing:** This includes the continual measurement and monitoring of the risk environment and the performance of the risk management strategies.

II. COSO ERM FRAMEWORK

The COSO "Enterprise Risk Management-Integrated Framework" published in 2004 defines 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."[4]

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 - additional components highlighted - are:

- Authority and pledge to the ERM
- RISK Management policy
- Mixer of ERM in the institution
- Risk Assessment
- Risk Response
- communication and reporting
- Information and Communication
- Monitoring

The four objectives categories - additional components highlighted - are:

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

RIMS Risk Maturity Model

The RIMS Risk Maturity Model (RMM) for Enterprise Risk Management, published in 2006, is an umbrella framework of content and methodology that detail the requirements for sustainable and effective enterprise risk management.[5] The RMM model consists of twenty-five competency drivers for seven attributes that create ERM's value and utility in an organization. The 7 attributes are:

- ERM-based approach
- ERM process management

ISBN: 978-93-86171-22-1

- Risk appetite management
- Root cause discipline
- Uncovering risks
- Performance management
- Business resiliency and sustainability

The model was developed by Steven Minsky, CEO of LogicManager, and published by the Risk and Insurance Management Society in collaboration with the RIMS ERM Committee. The Risk Maturity Model is based on the Capability Maturity Model, a methodology founded by the Carnegie Mellon University Software Engineering Institute (SEI) in the 1980s.[6]

Implementing an ERM program

Goals of an ERM program

Organizations by nature manage risks and have a variety of existing departments or functions ("risk functions") that identify and manage particular risks. However, each risk function varies in capability and how it coordinates with other risk functions. A central goal and challenge of ERM is improving this capability and coordination, while integrating the output to provide a unified picture of risk for stakeholders and improving the organization's ability to manage the risks effectively.

Typical risk functions

The primary risk functions in large corporations that may participate in an ERM program typically include:

- Strategic planning - identifies external threats and competitive opportunities, along with strategic initiatives to address them
- Marketing - understands the target customer to ensure product/service alignment with customer requirements
- Compliance & Ethics - monitors compliance with code of conduct and directs fraud investigations
- Accounting / Financial compliance - directs the Sarbanes-Oxley Section 302 and 404 assessment, which identifies financial reporting risks
- Law Department - manages litigation and analyzes emerging legal trends that may impact the organization
- Insurance - ensures the proper insurance coverage for the organization
- Treasury - ensures cash is sufficient to meet business needs, while managing risk related to commodity pricing or foreign exchange
- Operational Quality Assurance - verifies operational output is within tolerances
- Operations management - ensures the business runs day-to-day and that related barriers are surfaced for resolution
- Credit - ensures any credit provided to customers is appropriate to their ability to pay
- Customer service - ensures customer complaints are handled promptly and root causes are reported to operations for resolution
- Internal audit - evaluates the effectiveness of each of the above risk functions and recommends improvements

Common challenges in ERM implementation

ISBN: 978-93-86171-22-1

Various consulting firms offer suggestions for how to implement an ERM program.[7] Common topics and challenges include:

- Identifying executive sponsors for ERM.
- Establishing a common risk language or glossary.
- Describing the entity's risk appetite (i.e., risks it will and will not take)
- Identifying and describing the risks in a "risk inventory".
- Implementing a risk-ranking methodology to prioritize risks within and across functions.
- Establishing a risk committee and or Chief Risk Officer (CRO) to coordinate certain activities of the risk functions.
- Establishing ownership for particular risks and responses.
- Demonstrating the cost-benefit of the risk management effort.
- Developing action plans to ensure the risks are appropriately managed.
- Developing consolidated reporting for various stakeholders.
- Monitoring the results of actions taken to mitigate risk.
- Ensuring efficient risk coverage by internal auditors, consulting teams, and other evaluating entities.
- Developing a technical ERM framework that enables secure participation by 3rd parties and remote employees.

III. INTERNAL AUDIT ROLE

In addition to information technology audit, internal auditors play an important role in evaluating the risk-management processes of an organization and advocating their continued improvement. However, to preserve its organizational independence and objective judgment, Internal Audit professional standards indicate the function should not take any direct responsibility for making risk management decisions for the enterprise or managing the risk-management function.[9]

Internal auditors typically perform an annual risk assessment of the enterprise, to develop a plan of audit engagements for the upcoming year. This plan is updated at various frequencies in practice. This typically involves review of the various risk assessments performed by the enterprise (e.g., strategic plans, competitive benchmarking, and SOX top-down risk assessment), consideration of prior audits, and interviews with a variety of senior management. It is designed for identifying audit projects, not to identify, prioritize, and manage risks directly for the enterprise.

Current issues in ERM

The risk management processes of U.S. corporations are under increasing regulatory and private scrutiny. Risk is an essential part of any business. Properly managed, it drives growth and opportunity. Executives struggle with business pressures that may be partly or completely beyond their immediate control, such as distressed financial markets; mergers, acquisitions and restructurings; disruptive technology change; geopolitical instabilities; and the rising price of energy.

Sarbanes-Oxley Act requirements

ISBN: 978-93-86171-22-1

Section 404 of the Sarbanes-Oxley Act of 2002 required U.S. publicly traded corporations to utilize a control framework in their internal control assessments. Many opted for the COSO Internal Control Framework, which includes a risk assessment element. In addition, new guidance issued by the Securities and Exchange Commission (SEC) and PCAOB in 2007 placed increasing scrutiny on top-down risk assessment and included a specific requirement to perform a fraud risk assessment.[10] Fraud risk assessments typically involve identifying scenarios of potential (or experienced) fraud, related exposure to the organization, related controls, and any action taken as a result.

NYSE corporate governance rules

The New York Stock Exchange requires the Audit Committees of its listed companies to "discuss policies with respect to risk assessment and risk management." The related commentary continues: "While it is the job of the CEO and senior management to assess and manage the company's exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the company's major financial risk exposures and the steps management has taken to monitor and control such exposures. The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken. Many companies, particularly financial companies, manage and assess their risk through mechanisms other than the audit committee. The processes these companies have in place should be reviewed in a general manner by the audit committee, but they need not be replaced by the audit committee."[11]

ERM and corporate debt ratings

Standard & Poor's (S&P), the debt rating agency, plans to include a series of questions about risk management in its company evaluation process. This will rollout to 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, with initial comments in its reports during Q4 2008.

ISO 31000 : the new International Risk Management Standard

ISO 31000 is an International Standard for Risk Management which was published on 13 November 2009. An accompanying standard, ISO 31010 - Risk Assessment Techniques, soon followed publication (December 1, 2009) together with the updated Risk Management vocabulary ISO Guide 73.

Actuarial response

Casualty Actuarial Society

In 2003, the Enterprise Risk Management Committee of the Casualty Actuarial Society (CAS) issued its overview of ERM.[16] This paper laid out the evolution, rationale, definitions, and frameworks for ERM from the casualty actuarial perspective, and also included a vocabulary, conceptual and technical foundations, actual practice and applications, and case studies.[16]

The CAS has specific stated ERM goals, including being "a leading supplier internationally of educational materials relating to Enterprise Risk Management (ERM) in the property casualty insurance arena,"[17] and has sponsored research, development, and training of casualty actuaries in that regard.[18] The CAS has refrained

ISBN: 978-93-86171-22-1

from issuing its own credential; instead, in 2007, the CAS Board decided that the CAS should participate in the initiative to develop a global ERM designation, and make a final decision at some later date.

Society of Actuaries

In 2007, the Society of Actuaries developed the Chartered Enterprise Risk Analyst (CERA) credential in response to the growing field of enterprise risk management.[20] This is the first new professional credential to be introduced by the SOA since 1949.[21] A CERA studies to focus on how various risks, including operational, investment, strategic, and reputational combine to affect organizations. CERAs work in environments beyond insurance, reinsurance and the consulting markets, including broader financial services, energy, transportation, media, technology, manufacturing and healthcare.

It takes approximately three to four years to complete the CERA curriculum which combines basic actuarial science, ERM principles and a course on professionalism. To earn the CERA credential, candidates must take five exams, fulfill an educational experience requirement, complete one online course, and attend one in-person course on professionalism.

CERA Global

Initially all CERAs were members of the Society of Actuaries[] but in 2009 the CERA designation became a global specialized professional credential, awarded and regulated by multiple actuarial bodies.[23]

Institute and Faculty of Actuaries

The Institute and Faculty of Actuaries (the merged body formed in 2010 from the Institute of Actuaries and the Faculty of Actuaries) is the professional body representing actuaries in the United Kingdom. In March 2008, Enterprise Risk Management was adopted as one of the six actuarial practice areas, reflecting the increased involvement of actuaries in the ERM field.

A regular newsletter communicates the ongoing work that the profession performs in respect of ERM.

Some of the key areas that the profession works on are summarised below (together with some of the recent outcomes in each area):

- Education, CPD, Career Support and Development

From April 2010 actuaries were able to study ERM as one of the Specialist Technical Stage exams (ST9 course information), which (with other exam passes) gives candidates the Chartered Enterprise Risk Actuary (CERA) qualification. In July 2010 the first nine actuaries to obtain the CERA qualification were announced. The CERA qualification is offered by 13[24] participating actuarial associations, with further information available at a global or UK level.

Various events (e.g. networking evenings and webinars) are available to actuaries and other interested parties. The main event is the Risk and Investment Conference, which is often held during the summer months (e.g. 2011 Risk & Investment Conference). There is also some regularly reviewed material available from the profession which may be of use in developing knowledge of ERM.

- Research & Thought Leadership

A committee has been established to consider research and thought leadership in the ERM field (including what the “elevator speech” on ERM issues might be, definition of the scope of ERM and demonstration of the value of ERM).

ISBN: 978-93-86171-22-1

Some areas in which work has been completed include:

- ERM - A guide to Implementation
- A survey on actuaries in risk management
- A suggested common risk classification system for the actuarial profession

Research topics will be categorised and subject to a number of tests before proceeding with the research.

- enterprise-wide test (not just topic-specific / silo-based)
- risk management test (management = taking actions, not just modelling)
- director test (important enough for the Board, not just line managers)

- Communications & Marketing

Actuaries continue to look to demonstrate and promote the value of actuaries and the CERA qualification in the field of ERM - including through publication of articles in the Actuary

The Actuarial Profession also liaises with other professions where appropriate- e.g. the Institution of Civil Engineers on considering ERM in the context of Risk Analysis and Management for Projects (RAMP).

Companies Increasingly Focusing on ERM

It is clear that companies recognize ERM as a critical management issue. This is demonstrated through the prominence assigned to ERM within organizations and the resources devoted to building ERM capabilities. In a 2008 survey by Towers Perrin,[25] at most life insurance companies, responsibility for ERM resides within the C-suite. Most often, the chief risk officer (CRO) or the chief financial officer (CFO) is in charge of ERM, and these individuals typically report directly to the chief executive officer. From their vantage point, the CRO and CFO are able to look across the organization and develop a perspective on the risk profile of the firm and how that profile matches its risk appetite. They act as drivers to improve skills, tools and processes for evaluating risks and to weigh various actions to manage those exposures. Companies are also actively enhancing their ERM tools and capabilities. Three quarters of responding companies said they have tools for specifically monitoring and managing enterprise-wide risk. These tools are used primarily for identifying and measuring risk and for management decision making. Respondents also reported that they have made good progress in building their ERM capabilities in certain areas.

In this study, more than 80% of respondents reported that they currently have adequate or better controls in place for most major risks. In addition, about 60% currently have a coordinated process for risk governance and include risk management in decision making to optimize risk adjusted returns.

In another survey conducted in May and June 2008, against the backdrop of the developing financial crisis, six major findings came to light regarding risk and capital management among insurers worldwide:

- Embedding ERM is proving to be a significant challenge
- Company size matters
- European insurers are better positioned
- ERM is influencing important strategic decisions
- Economic capital standards are gaining ground
- Operational risk remains a weak spot

ISBN: 978-93-86171-22-1

V. CONCLUSION

ERM forms part of the glue that holds corporate governance together. It also contributes to an organisation's long-term profitability and sustainable growth. Effective risk management initiatives need to be both proactive and embedded within the culture of an organisation

1. *Enterprise Risk Management Committee (May 2003). "Overview of Enterprise Risk Management" (PDF).*
2. Ackerman, Shawna. 2001. The Enterprise in Enterprise Risk Management. Casualty Actuarial Society Enterprise Risk Management Seminar.
3. ARI Risk Management Consultants. 2001. Enterprise Risk Management: The Intersection of Risk and Strategy. http://www.riskadviser.net/Cases/case.htm Banham, Russ. 1999. Understanding the Skepticism about Enterprise Risk Management.
4. CFO Magazine. April 1, 1999. Bernstein, Peter L. 1996. Against the Gods: The Remarkable Story of Risk. John Wiley and Sons, Inc. New York.
5. *Enterprise Risk Management Committee (May 2003). "Overview of Enterprise Risk Management" (PDF).*
6. *Enterprise Risk Management Committee (May 2003). "Overview of Enterprise Risk Management" (PDF).*
7. *"Enterprise Risk Management — Integrated Framework: Executive Summary"(PDF). Committee of Sponsoring Organizations of the Treadway Commission.*
8. www.google.com
9. www.wikipedia.com

.