Enterprise risk management

Enterprise risk management (**ERM**) 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 (threats and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring process. 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, data protection 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 are appropriately managed. Regulators and debt rating agencies have increased their scrutiny on the risk management processes of companies.

According to Thomas Stanton of Johns Hopkins University, the point of enterprise risk management is not to create more bureaucracy, but to facilitate discussion on what the really big risks are.[1]

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."[2] The CAS conceptualized ERM as proceeding across the two dimensions of *risk type* and *risk management processes*.[2] The risk types and examples include:[3]

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:[4]

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.
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.

COSO ERM framework

The COSO "Enterprise Risk Management-Integrated Framework" published in 2004 (New edition COSO ERM 2017 is not Mentioned and the 2004 version is outdated) 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."[5]

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 - 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

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.

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.[6] 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
- 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.[7]

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
- Corporate Security - identifies, evaluates, and mitigates risks posed by physical and information security threats

Common challenges in ERM implementation

Various consulting firms offer suggestions for how to implement an ERM program.[8] Common topics and challenges include:[9]

- 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.

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.[10]

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 404 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 corporations worldwide 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

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.[11] 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."[12]

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.[13] 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.[14] 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,[15] with initial comments in its reports during Q4 2008.[16]

IFC Performance Standards

International Finance Corporation Performance Standards[17] focus on the management of Health, Safety, Environmental and Social risks and impacts. The third edition was published on January 1, 2012 after a two-year negotiation process with the private sector, governments and

civil society organizations. They have been adopted by the Equator Principles (http://www.equator-principles.com/) Banks, a consortium of over 118 commercial banks in 37 countries.

Data Privacy

Data privacy rules, such as the European Union's General Data Protection Regulation, increasingly foresee significant penalties for failure to maintain adequate protection of individuals' personal data such as names, e-mail addresses and personal financial information, or alert affected individuals when data privacy is breached. The EU regulation requires any organization--including organizations located outside the EU--to appoint a Data Protection Officer reporting to the highest management level[18] if they handle the personal data of anyone living in the EU.

Actuarial response

Casualty Actuarial Society

In 2003, the Enterprise Risk Management Committee of the Casualty Actuarial Society (CAS) issued its overview of ERM.[19] 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.[19]

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,"[20] and has sponsored research, development, and training of casualty actuaries in that regard.[21] The CAS has refrained 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.[22]

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.[23] This is the first new professional credential to be introduced by the SOA since 1949.[24] 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.[24]

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.[24]

CERA Global

Initially all CERAs were members of the Society of Actuaries[25] but in 2009 the CERA designation became a global specialized professional credential, awarded and regulated by multiple actuarial bodies.[26]

See also

- Actuarial science
- Airmic
- Basel III
- Benefit risk
- Committee of Sponsoring Organizations of the Treadway Commission
- Cost risk
- Credit risk
- Financial risk management § Corporate finance
- Information Quality Management
- ISO 31000
- Market risk and strategic planning
- Operational risk management
- Optimism bias
- Risk adjusted return on capital
- Risk appetite

- Risk management tools
- RiskLab
- ISA 400 Risk Assessments and Internal Control
- SOX 404 top-down risk assessment
- Total Security Management
- Web Presence Management
- Certifications:
  - Certified Risk Professional (Institute of Risk Management)
  - Chartered Enterprise Risk Actuary (Institute and Faculty of Actuaries)
  - Chartered Enterprise Risk Analyst (Society of Actuaries)

References

1. *Thomas Stanton (Feb 18, 2017). "Enterprise Risk Management" (https://www.youtube.com/watch?v=voGyHN-tWMg) . YouTube. TEDxJHUDC. "The whole point of enterprise risk management is not to create another layer of bureaucracy, but rather to have your chief risk officer facilitate the conversations and then the discussions about priorities – what are the really big risks we've got to grapple with."*
2. *Enterprise Risk Management Committee (May 2003). "Overview of Enterprise Risk Management" (https://www.casact.org/research/erm/overview.pdf) (PDF). Casualty Actuarial Society: 8. Retrieved 2008-09-15.*
3. *Enterprise Risk Management Committee (May 2003). "Overview of Enterprise Risk Management" (https://www.casact.org/research/erm/overview.pdf) (PDF). Casualty Actuarial Society: 9–10. Retrieved 2008-09-15.*
4. *Enterprise Risk Management Committee (May 2003). "Overview of Enterprise Risk Management" (https://www.casact.org/research/erm/overview.pdf) (PDF). Casualty Actuarial Society: 11–13. Retrieved 2008-09-15.*
5. *"Enterprise Risk Management — Integrated Framework: Executive Summary" (http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf) (PDF). Committee of Sponsoring Organizations of the Treadway Commission. September 2004. Retrieved 2008-09-16.*
6. *"RIMS - Risk Maturity Model (RMM)" (http://www.rims.org/resources/erm/pages/RiskMaturityModel.aspx) .*

7. *"Archived copy" (https://web.archive.org/web/20181225110843/https://www.rims.org/resources/ERM/Pages/RiskMaturityModelFAQ.aspx)* . Archived from *the original (http://www.rims.org/resources/ERM/Pages/RiskMaturityModelFAQ.aspx)* on 2018-12-25. Retrieved 2013-10-24.
8. *ERM Implementation Advice (http://www.protiviti.it/downloads/PRO/pro-gb/ProtivitiBulletin6.pdf)*
9. *ERM Frequently Asked Questions (http://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/WhitePapersArticlesGuidetoEnterpriseRiskManagementFrequentlyAskedQuestions!OpenDocument)*
10. *Role of Internal Auditing in ERM (http://www.theiia.org/download.cfm?file=283)* *Archived (https://web.archive.org/web/20130905225145/http://www.theiia.org/download.cfm?file=283)* 2013-09-05 at the *Wayback Machine*
11. *PCAOB Auditing Standard No 5 (http://www.pcaob.org/Rules/Docket_021/2007-05-24_Release_No_2007-005.pdf)* *Archived (https://web.archive.org/web/20070627001642/http://www.pcaob.org/Rules/Docket_021/2007-05-24_Release_No_2007-005.pdf)* 2007-06-27 at the *Wayback Machine*
12. *"NYSE Listing Standards Part 7d" (https://web.archive.org/web/20140611083439/http://www.nyse.com/pdfs/finalcorpgovrules.pdf)* (PDF). Archived from *the original (https://www.nyse.com/pdfs/finalcorpgovrules.pdf)* (PDF) on 2014-06-11. Retrieved 2017-08-27.
13. *S&P Ratings - Treasury & Risk Article (http://www.treasuryandrisk.com/article-print.php?article=714)* *Archived (https://web.archive.org/web/20070928191041/http://www.treasuryandrisk.com/article-print.php?article=714)* 2007-09-28 at the *Wayback Machine*
14. *S&P ERM for Financial Institutions (http://www.mgt.ncsu.edu/pdfs/erm/sp_erm_busdevbk.pdf)*
15. *S&P ERM FAQs (http://www.towersperrin.com/tp/getwebcachedoc?webc=HRS/USA/2008/200806/ERM_NonFinanFAQ.pdf)*
16. *S&P ERM Announcement (http://www.towersperrin.com/tp/getwebcachedoc?webc=HRS/USA/2008/200805/ERM4Corp.pdf)*
17. *"Performance Standard 1" (http://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/sustainability-at-ifc/policies-standards/performance-standards/ps1)* .
18. *"FERMA ECIIA Cyber Risk Governance Report | Ferma" (https://www.ferma.eu/ferma-eciia-cyber-risk-governance-report-0)* . www.ferma.eu. Retrieved 2018-10-01.
19. Enterprise Risk Management Committee (May 2003). *"Overview of Enterprise Risk Management" (https://www.casact.org/area/erm/overview.pdf)* (PDF). *Casualty Actuarial Society*. Retrieved 2008-09-15.
20. *"ERM SAM Goals" (https://www.casact.org/about/ERM_SAMs.pdf)* (PDF). CAS Centennial Goal and SAM Goals. *Casualty Actuarial Society*. March 2008. Retrieved 2008-09-15.
21. *"Enterprise Risk Management Web Site" (https://www.casact.org/research/erm/)* . *Casualty Actuarial Society*. 2008. Retrieved 2008-09-15.

22. *"Executive Summary: CAS Board of Directors Meeting" (https://web.archive.org/web/20100627193942/http://www.casact.org/about/governance/bod/061707ES.pdf)* *(PDF). Casualty Actuarial Society. June 17, 2007. Archived from the original (https://www.casact.org/about/governance/bod/061707ES.pdf) (PDF) on June 27, 2010. Retrieved 2008-09-15.*

23. *"Credential Overview" (http://www.ceranalyst.org/overview.asp)* *. Society of Actuaries. 2008. Retrieved 2008-09-15.*

24. *"CERA Fast Facts" (http://www.ceranalyst.org/cera-facts-overview.asp)* *. Society of Actuaries. 2008. Retrieved 2008-09-15.*

25. *"Benefits" (http://www.ceranalyst.org/benefits.asp)* *. Society of Actuaries. 2008. Retrieved 2008-09-15.*

26. *"The CERA Treaty" (https://web.archive.org/web/20150112142729/http://www.ceraglobal.org/about/treaty)* *. CERA Global. 2009. Archived from the original (http://www.ceraglobal.org/about/treaty) on 2015-01-12. Retrieved 2015-01-12.*

External links

- Thomas Stanton (Feb 18, 2017). "Enterprise Risk Management" (https://www.youtube.com/watch?v=voGyHN-tWMg) . *YouTube*. TEDxJHUDC.
- Airmic / Alarm / IRM (2010) "A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000" (https://web.archive.org/web/20100705072108/http://www.theirm.org/documents/SARM_FINAL.pdf)
- Hopkin, Paul "Fundamentals of Risk Management 2nd Edition" Kogan-Page (2012) ISBN 978-0-7494-6539-1