CIMA

Enterprise Risk Management

Topic Gateway Series No. 49

Prepared by Jasmin Harvey and Technical Information Service

July 2008

About Topic Gateways

Topic Gateways are intended as a refresher or introduction to topics of interest to CIMA members. They include a basic definition, a brief overview and a fuller explanation of practical application. Finally they signpost some further resources for detailed understanding and research.

Topic Gateways are available electronically to CIMA members only in the CPD Centre on the CIMA website, along with a number of electronic resources.

About the Technical Information Service

CIMA supports its members and students with its Technical Information Service (TIS) for their work and CPD needs.

Our information and accounting specialists work closely together to identify or create authoritative resources to help members resolve their work related information needs. Additionally, our accounting specialists can help CIMA members and students with the interpretation of guidance on financial reporting, financial management and performance management, as defined in the *CIMA Official Terminology* 2005 edition.

CIMA members and students should sign into My CIMA to access these services and resources.

The Chartered Institute
of Management Accountants
26 Chapter Street
London SW1P 4NP
United Kingdom

T. +44 (0)20 7663 5441
F. +44 (0)20 7663 5442
E. tis@cimaglobal.com
www.cimaglobal.com

Definition and concept

Enterprise Risk Management (ERM) can be defined as the:

' … 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.'

Enterprise Risk Management – Integrated Framework, the Committee of Sponsoring Organisations, COSO, 2004

The CIMA Official Terminology uses the COSO (Committee of Sponsoring Organisations) definition. However, there is no universally agreed definition and the COSO definition is just one of a number of definitions developed for Enterprise Risk Management. For example, see the Australian/New Zealand Risk Management Standard 4360.

Some research indicates that ERM is still a 'rather elusive and under-specified concept'. Although ERM has been discussed at length by professionals in the field, 'little progress seems to have been made in achieving this elusive nirvana'.

Managing Business Risk, 5th ed., page 30

Differing terminology, methodology and measures means that ERM in practice will differ across industries and organisations. What is important for ERM to be effective is that an organisation's interpretation and use of ERM terminology, methodology and measures is consistent within that organisation.

Context

In the current syllabus, ERM is core to the syllabus for P3 Management Accounting Risk and Control Strategy of the professional qualification. Students must understand enterprise risk management and will be examined on it.

In the CIMA Professional Development Framework, ERM is found under Governance – ERM.

Related concepts

Risk management; enterprise wide risk management; internal control.

Overview

In the last decade, risk management has transformed from the traditional silo approach practised by individual departments and functions to a holistic, co-ordinated and integrated process which manages risk throughout the organisation. This integrated approach has become known as ERM. 'Enterprise wide' means the removal of traditional functional, divisional, departmental or cultural barriers.

Enterprise Risk Management, KMPG, page 2

A number of drivers have contributed to increased emphasis on risk awareness and the need for a co-ordinated, enterprise wide approach. Drivers include globalisation, the increased complexity of doing business, regulatory compliance/corporate governance developments, and greater accountability for the board and senior management to increase shareholder value.

These drivers mean that an organisation and its board must have a thorough understanding of the key risks affecting the organisation and what is being done to manage them. ERM offers a framework to provide this understanding and also to integrate risk management in decision making activity throughout the organisation.

Underlying principles of ERM

The key underlying principles of ERM include:

- consideration in the context of business strategy
- it is everyone's responsibility, with the tone set from the top
- a focused strategy, led by the board
- active management of risk
- creation of a risk aware culture
- a comprehensive and holistic approach to risk management
- consideration of a broad range of risks (strategic, financial, operational and compliance)
- implementation through a risk management framework or system.

Application

Development of a risk strategy

The purpose of developing a risk strategy is to articulate clearly how risk should be approached in an organisation. A risk strategy is important to embed risk within the organisation's culture. Such a strategy must be consistent with and reviewed alongside the organisation's business strategy. Key elements to include are:

- a statement of the value proposition specific to the organisation
- the agreed risk appetite of the organisation (see below for a definition of risk appetite)
- agreed objectives for risk management based on the organisation's objectives and business strategy
- a statement of the organisation's cultural approach to risk
- details of who owns risk management at various levels within the organisation
- reference to the risk management framework or system
- details of performance evaluation for monitoring the effectiveness of the risk management framework.

Adapted from *Enterprise Governance Executive Report,* CIMA

ERM frameworks

ERM is a term used by COSO which published the *COSO Enterprise Risk Management – Integrated Framework* in 2004. This has become a well known framework on how to implement ERM.

COSO was not the first to publish practical guidance on an enterprise wide approach to risk management. The first edition of the joint Australian/New Zealand Standard for Risk Management was published in 1995. A further edition, published in 1999, provides guidance on how to establish and implement an enterprise wide risk management process.

In 2001, KMPG published a report titled *Enterprise Risk Management: an emerging model for building shareholder value.* This report puts forward an ERM framework where risk strategy is built around and supports the organisation's business strategy and objectives. It is important to understand that there is no one methodology that should be followed by an organisation.

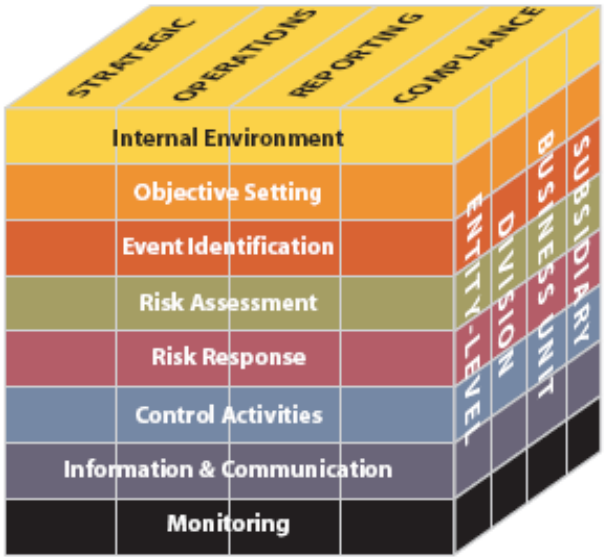
Two examples are given below for illustration.

1. KPMG

The KPMG framework maintains that ERM and its strategy should be intrinsically linked to an organisation's business strategy. Risk portfolio development, risk optimisation, and measuring and monitoring take place in the context of strategies based on an ERM structure. This ensures that risk management is embedded in the organisation's structure.

Source: *Enterprise Risk Management: an emerging model for building shareholder value,* A KPMG White Paper, KPMG, November 2001.

2. COSO – ERM Framework



Source: COSO (2004) *Enterprise Risk Management – Integrated Framework*

The COSO ERM Framework is presented here in more detail to introduce some key risk terms. It comprises a three dimensional matrix in the form of a cube which reflects the relationships between four objectives, seven components and four different organisational levels.

The four objectives are:

- strategic (high level goals, aligned with and supporting the organisation's mission)
- operations (efficient and effective use of resources)
- reporting (reliability of reporting)
- compliance (compliance with laws and regulations).

These categories may be the responsibility of different executives across the entity and address different needs. Responsibility for different objectives and related risks needs to be clearly articulated and communicated. The necessary resources must be defined for each organisational level, including each business unit. Integrating risk management into strategy, performance management, training and development, and budgetary processes helps to assign responsibilities.

The COSO Framework identifies eight components which must function effectively for risk management to be successful. The eight interrelated components are:

1. Internal environment

This is the tone of the organisation, including the risk management philosophy and risk appetite. Risk management philosophy is the general attitude or approach an organisation takes in dealing with risks. Risk appetite is level of risk that a company can undertake and successfully manage over an extended time period.

2. Objective setting

Objectives should be aligned with the organisation's mission and need to be consistent with the organisation's defined risk appetite. The capacity for undertaking risk (risk appetite) will vary by company and depend on the organisation's unique circumstances.

3. Event identification

These are internal and external events (both positive and negative) which impact upon the achievement of an entity's objectives and must be identified.

4. Risk assessment

Risks are analysed to consider their likelihood and impact as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis. COSO defines inherent risk as the risk to an organisation in the absence of any actions management might take to alter either the risk's probability or impact. These risks may result from an organisation's industry, strategy or environment. Residual risk is the risk that remains after management has responded to the risk. Management must decide whether residual risk is within the entity's risk appetite.

5. Risk response

Management selects risk response(s) to avoid, accept, reduce or share risk. The intention is to develop a set of actions to align risks with the entity's risk tolerances and risk appetite. Risk tolerance is the acceptable variation relative to the achievement of an objective. This variation is often measured using the same units as its related objective. In setting risk tolerance, management considers the relative importance of the related objective, and aligns risk tolerances with risk appetite. An entity operating with its risk tolerance is operating within its risk appetite.

6. Control activities

Policies and procedures help ensure the risk responses are effectively carried out. Examples of control activities include segregation of duties, physical controls, IT controls, analysis of results versus targets and reviews by senior management/specialists.

7. Information and communication

The relevant information is identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Sources of information will be internal and external with the historic, current and projected information used.

8. Monitoring

The entire ERM process is monitored and modifications made as necessary. A combination of ongoing and specific interval monitoring activities is required. Activities can include: reviewing operating reports for inaccuracies; identifying weaknesses in control activities by internal and external auditors; and senior management assessments of risk responses against targets. Specific interval monitoring can occur at critical times, for example, reporting periods, or after unexpected events or outcomes.

ERM is not strictly a serial process where one component affects only the next. It is a multidirectional process in which almost any component can and does influence another. The type of company, including size, industry and structure, will determine how the components function in practice.

What is important for companies to understand is that ERM is an ongoing process which must be refined and adapted to meet changes in business strategy. Maintaining the momentum is usually the most challenging part for organisations.

The four organisational levels are:

- entity level
- division
- business unit
- subsidiary.

Managing risk across all organisational levels emphasises the importance of managing risks across the enterprise as a whole.

Source: *Enterprise Risk Management – Integrated Framework*. COSO (2004)

As previously noted, there is no one framework or methodology that an organisation must use.

Implementing ERM in practice

Implementing ERM in practice constitutes a major change management programme for organisations and will take time. The following provides an overview of the main activities of implementing ERM in practice:

1. The risk appetite and philosophy of the organisation is set from the commitment and behaviour of the top of the organisation.
2. The establishment of a risk strategy is critical to the implementation process.
3. Developing the ERM structure is important in determining how ERM is to be integrated into the organisation. Usually this does not involve replacing existing structures but enhances them by embedding and aligning risk management.
4. In practice, an individual ('risk champion') or small team is appointed with the primary responsibility for implementing ERM. Who this is will depend on the size and nature of the organisation. This role is one of facilitation. The individual will need to involve and engage the rest of the organisation in the risk management process.
5. Holding risk workshops with senior management is an effective way of identifying and prioritising key risks.
6. In order to identify, assess and respond to risk, tools and techniques are used. For details on these tools and techniques, please refer to the Introduction to Managing Risk and Financial Risk Management topic gateways.
7. Embedding risk into the culture of the organisation involves many activities. These include: communicating risk and progress; developing training programmes to incorporate risk into induction and other training; embedding risk into business processes; and aligning risk management tools and techniques with organisational culture.

8. Measuring, monitoring and reporting risk management effectiveness. Key Performance Indicators (KPIs) and critical success factors need to be identified and performance measured. The appropriate corrective action must be taken. A periodic process for reporting should be established.

Roles and responsibilities

The key roles and responsibilities for ERM are summarised below:

Chief Executive Officer (CEO) - This is the ultimate risk manager for any organisation. The CEO must assess the organisation's enterprise risk management capabilities and lead any related major initiatives or changes.

Board of directors - The board has ultimate responsibility for the oversight of risk management, including reviewing risk management processes and providing direction on matters related to risk and internal control.

Audit committee - This is the committee responsible for examining the effectiveness of the internal control function. It has an important role to play in examining the exposure of the organisation to a variety of risks.

Chief risk officer or risk manager - This position leads the process of establishing and maintaining effective risk management activities across the organisation.

Senior management - They have responsibility for assessing key risks, for reviewing risk management capabilities and for initiating any necessary changes.

Internal audit - This has responsibility for internal control and for providing independent assurance concerning the risk management process. Internal audit forms an opinion about the soundness of internal controls to manage the agreed level of risk.

Managers and business units - They manage day to day risks within their allocated areas of responsibility within agreed risk tolerances. Manager should also promote the organisation's risk management philosophy and compliance with risk appetite to staff.

Some organisations will have a dedicated risk management function (usually dependant upon size and industry). The function could consist of a single risk champion, risk manager or a large department. The role of the risk management function involves:

- setting risk management strategy and related policies
- raising awareness of risk management throughout the organisation
- building a risk aware culture with appropriate training and education
- designing and reviewing risk management processes
- co-ordination of risk management activities
- developing risk response processes
- reporting on risk externally and internally.

Source: adapted from *Risk Management Standard* (ALARM, AIRMIC, IRM)

Benefits of effective ERM

The benefits of effective ERM include:

- protecting and building shareholder value through enhanced decision making by integrating risks and building investor confidence
- focusing management attention on the most significant risks
- a common language which is understood throughout the organisation
- improved capital efficiencies and resource allocation
- reduced cost of capital through managing risk.

Limitations of ERM

ERM is a process or methodology for enterprise wide risk management. In common with most methodologies, it is not an exact science.

Factors such as human error, imprecise calculations, incomplete information and breakdown of internal controls preclude a board and management from having complete confidence in the effectiveness of ERM

Enterprise Risk Management – Integrated Framework, COSO, 2004

The success of an ERM framework is dependent on a number of key factors:

- CEO and senior management commitment
- assignment of risk management responsibilities within the organisation
- allocation of appropriate resources for training
- the development of enhanced risk awareness by all stakeholders.

An ERM framework will not be effective if any of these factors fail.

Source: *Risk Management Standard* (ALARM, AIRMIC, IRM)

For some organisations, a comprehensive ERM framework may be too complex or unsuitable. However, a modified approach is still encouraged to identify, measure and manage a broad range of risks in a cohesive manner across the organisation.

Key developments in enterprise risk management

More recently, ERM has focused on:

1. Alignment of the entire ERM process (not just risk appetite) with business strategy and embedding ERM into the culture of the entity.
2. A greater emphasis on strategic risk rather than compliance with risk mitigation requirements, such as Sarbanes-Oxley in the US or the UK Combined Code.
3. Enhanced external risk reporting due to corporate governance regulations and developments in narrative reporting such as the US Management's Discussion and Analysis (MD&A) and the enhanced Business Review in the UK. These require disclosure of the principal risks and uncertainties facing the organisation and its core business. The demand for reporting risk externally is also growing as investors, financial analysts and other external stakeholders become aware of the critical role of risk management.
4. Enhanced internal risk reporting, as inadequate risk reporting can lead to a failure to fully integrate identified risks into strategic and operational decisions.
5. Taking more intelligent risks to exploit opportunities. Progressive companies are using ERM as a tool to gain competitive advantage through being able to take on more risk for greater company returns. They need to manage risks in a way that will maximise the upside while providing protection against the downside.

6. ERM technology, which has evolved at a rapid pace. For medium to large organisations, investment in innovative ERM technology can help to ensure that ERM processes are working effectively.

Case studies

The ICFAI Centre for Management Research has a large number of company case studies on ERM.
www.icmr.icfai.org/casestudies/sit_cat.asp?cat=Enterprise%20Risk%20Management

PricewaterhouseCoopers (PwC), Managing Risk has a number of case studies and white papers relating to risk management.
www.pwc.com/Extweb/pwcpublications.nsf/docid/5000BED2DA815F4485256F9000305828

References

Collier, P.M. and Agyei-Ampomah, S. (2006). *Management accounting: risk and control strategy.* Oxford: Elsevier. (CIMA Official Study System)

Connell, B. *Strategic risk: critical to organisations.* Plenary presentation at the Management Accounting Research Group (MARG) Conference, April 2006

Mikes, A. (2005). *Enterprise Risk Management in action.* Discussion Paper 35, ESRC Centre for Analysis of Risk and Regulation. London: LSE. Available from: www.lse.ac.uk
[Accessed 5 June 2008]

CIMA Official Terminology. (2005). Chartered Institute of Management Accountants (CIMA). London: CIMA Publishing

COSO. (2004). *Enterprise Risk Management: integrated framework.* Executive Summary. Available from: http://digbig.com/4xamj
[Accessed 5 June 2008]

Enterprise governance: getting the balance right. (PDF 733KB). CIMA Executive Report, February 2004. London: CIMA/IFAC. Available from:
www.cimaglobal.com/executivereports
[Accessed 5 June 2008]

Enterprise Risk Management: an emerging model for building shareholder value. A KPMG White Paper, KPMG, November 2001. Available from:
http://digbig.com/4xamk
[Accessed 5 June 2008]

(2002). *A risk management standard.* Association of Insurance and Risk Managers (AIRMIC), National Forum for Risk Management in the Public Sector (ALARM) and Institute of Risk Management (IRM) Available from: http://digbig.com/4xamh
[Accessed 5 June 2008]

Further information

CIMA publications

Bekefi, T. and Epstein, M.J. (2006). *Integrating social and political risks into business decisions.* Management Accounting Guideline, Canada: The Society of Management Accountants of Canada (CMA-Canada)

Collier, P. M. et al. (2006). *Risk and management accounting: best practice guidelines for enterprise-wide internal control procedures.* CIMA Research Executive Summaries Series, Volume 2, Number 11. Available from: **www.cimaglobal.com/researchexecsummaries**
[Accessed 5 June 2008]

Epstein, M.J. and Rejc, A. (2006). *The reporting of organisational risks for internal and external decision makers.* Management Accounting Guideline. Canada: The Society of Management Accountants of Canada (CMA)

Spedding, L. and Rose, S. (2008). *Business risk management handbook: a sustainable approach*. Oxford: CIMA Elsevier

CIMA/AICPA and CMA Canada. (2005). *Identifying, measuring and managing organisational risk for improved performance.* Management Accounting Guideline, Canada: The Society of Management Accountants of Canada (CMA-Canada)

CIMA Official Terminology, (2005). Chartered Institute of Management Accountants (CIMA). London: CIMA Publishing

Enterprise Governance. (PDF 31KB). CIMA Discussion Paper. (2004). London: CIMA/IFAC. Available from: **www.cimaglobal.com/discussionpapers**
[Accessed 5 June 2008]

Enterprise Governance: getting the balance right. (PDF 150KB). CIMA Research Executive Summary. August 2004. London: CIMA/IFAC. Available from: **www.cimaglobal.com/executivereports**
[Accessed 5 June 2008]

Fraud and Risk Management Working Group. (2002). *Risk management: a guide to good practice.* London: CIMA

Other articles and publications

Beasley, M. et al. *Working hand-in-hand: balanced scorecards and enterprise risk management.* Strategic Finance, Volume 87, Issue 9, March 2006, pp 49-55
Available from: www.imanet.org
[Accessed 5 June 2008]

Reuvid J. (ed.) (2008). *Managing business risk*. 5th ed. London: Kogan Page
Contains some useful material on ERM.

Enterprise Risk Management: an emerging model for building shareholder value. A KPMG White Paper, KPMG, November 2001. Available from: http://digbig.com/4xamk [Accessed 5 June 2008]

Websites

There are a number of organisations which offer ERM solutions from large consulting firms to boutique risk management practices. Thorough due diligence should be undertaken before pursuing one of these.

HM Treasury's Risk Portal section of the Treasury website

Provides a number of publications on risk management including the *Orange Book: Management of Risk.*
Available from: http://digbig.com/4xamm
[Accessed 5 June 2008]

The Committee of Sponsoring Organizations (COSO)

The website offers a number of articles and publications on risk, including the COSO's ERM framework.
Available from: http://www.coso.org
[Accessed 5 June 2008]

The Institute of Risk Management

This is the professional education body for risk management. Established as a not-for-profit organisation, the Institute is governed by practicing risk professionals and has strong links to leading universities and business schools across the world.
Available from: http://www.theirm.org

The Institute of Risk Management website also provides a link to the Risk Management Standard. Available from: http://digbig.com/4xamn [Accessed 5 June 2008]

Australian Standard AS 4360 risk management portal on the Australian Standards website. This brings together the Standard, its companion products, news and information.
Available from: http://www.riskmanagement.com.au
[Accessed 5 June 2008]

CIMA reading lists

Available to CIMA members only via **www.cimaglobal.com/mycima**
[Accessed 5 June 2008]

Enterprise risk management

CIMA topic gateways

Available to CIMA members only via **www.cimaglobal.com/mycima**
[Accessed 5 June 2008]

Introduction to managing risk

Financial risk management

First published in 2008 by:

The Chartered Institute
of Management Accountants
26 Chapter Street
London
SW1P 4NP
United Kingdom

Printed in Great Britain