Operational Risk

Topic Gateway series No. 51
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 specialists 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 8849 2259
F. +44 (0)20 8849 2468
E. tis@cimaglobal.com
www.cimaglobal.com
**Definition and concept**

What is business/operational risk?

‘Business/operational risk relates to activities carried out within an entity, arising from structure, systems, people, products or processes.’

*CIMA Official Terminology, 2005*

Operational risk has also been defined as:

‘The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.’

*Basel Committee on Banking Supervision, 2004*

Risk management is:

‘A process of understanding and managing the risks that the entity is inevitably subject to in attempting to achieve its corporate objectives. For management purposes, risks are usually divided into categories such as operational, financial, legal compliance, information and personnel. One example of an integrated solution to risk management is enterprise risk management.’

*CIMA Official Terminology, 2005*

**Context**

In the current syllabus, CIMA students will learn and may be examined on this topic in Paper 3, Management Accounting Risk and Control Strategy.

In the CIMA Professional Development Framework, risk (including operational risk) features in Governance, Enterprise Risk Management, and Business Skills, Business Acumen and Manage Risk.

**Related concepts**

Introduction to managing risk; enterprise risk management.
Overview

There is a huge variety of specific operational risks. By their nature, they are often less visible than other risks and are often difficult to pin down precisely. Operational risks range from the very small, for example, the risk of loss due to minor human mistakes, to the very large, such as the risk of bankruptcy due to serious fraud. Operational risk can occur at every level in an organisation.

The type of risks associated with business and operation risk relate to:

- business interruption
- errors or omissions by employees
- product failure
- health and safety
- failure of IT systems
- fraud
- loss of key people
- litigation
- loss of suppliers.

Operational risks are generally within the control of the organisation through risk assessment and risk management practices, including internal control and insurance.
Application

Risk categorisation

Risks can be categorised in a number of ways. A popular way is to use one of four main categories, namely operational risk, financial risk, environmental risk and reputational risk. It is important that risks are categorised in a way that is relevant to the needs of the organisation. Some of the benefits of categorisation include:

- providing a framework that can be used to define who is responsible, to design appropriate internal controls and to assist in simplified risk reporting
- assisting managers to identify how they can use their past experience to categorise risk
- helping organisations to identify related risks in the same category
- giving assistance in recognising which risks are inter-related.

Operational risk identification

Operational risk sources may be internal or external to the business and are usually generated by people, processes and technology.

Identification is one of the most important areas of managing risk. Failure to identify risk will certainly mean that no action is taken to manage that risk.

There are a number of different techniques that can be used to identify risk. A common method used in risk identification is the use of workshops to ‘brainstorm’. This can be used at different levels of the organisation and can identify a large number of risks in a short time. To keep ideas flowing, it is important to keep identification sessions focused on identifying risks and not to move on to evaluate the risks.

Operational risks are largely based on procedures and processes, so this lends itself to the use of audit for risk identification purposes. Risk based audit can be used as a tool to identify risks, as well as a method of reporting to the board on the effectiveness of the organisation’s risk management framework.
Risk based audit can use the following methods to assess risks:

- intuitive or judgemental assessment
- risk assessment matrix
- risk ranking.

Another approach to identifying operational risk is to look for critical dependencies in people, processes, systems and external structures. Once identified, the dependencies can be managed or engineered by adding fail-safes and system redundancies. Other approaches include physical inspection and incident investigation.

Once risks have been identified based on a suitable way of categorising them, it becomes possible to think of tools that may be used to measure and manage them.

**Risk assessment and measuring**

Various methods may be used to assess the severity of each risk once it has been identified. One of the reasons for measuring risk is that it allows the most significant risks to be prioritised.

The result or impact of a risk occurring may be financial loss, damage to reputation, process change or a combination of these. One of the simplest ways to measure risks is to apply an impact and likelihood matrix which provides an overall risk rating.

Adapted from: Emergency Preparedness (Guidance on part 1 of the Civil Contingencies Act 2004)
One of the issues with measuring risk is that there are objective or subjective risks. Many risks are subjective and qualitative, rather than objectively identifiable and measurable. For example, the risks of litigation, economic downturn, loss of key employees, natural disasters and loss of reputation are all subjective judgements. There is an important distinction between objective, measurable risks and subjective, perceived risks. Some of the factors that influence this distinction are:

- how recently the risk has occurred
- how visible the risk is
- how management perceives the risk
- how the organisation establishes formal or informal ways of dealing with the risk.

The analysis can be either quantitative or qualitative, but it should allow for comparison and trend analysis.

One of the issues with risk assessment is that traditional risk assessment techniques often focus on those elements that can be quantified easily. Such techniques fail to address all critical drivers of successful risk management.

**Impact**

When considering the impact of operational risk there are three primary areas that affect the business activity.

**Property exposures** – these relate to the physical assets belonging to or entrusted to the business.

**Personnel exposures** – these relate to the risks faced by all those who work for and with the business, including customers, suppliers and contractors.

**Financial exposures** – these relate to all aspects of the company’s ability to trade, whether profitability or not, and cover internal and external exposures of all types. Financial exposures also include intellectual property, goodwill and patents.
Managing operational risks

Risk evaluation is used to make decisions about the significance of the risks to the organisation and whether each specific risk should be accepted or treated.

When looking at operational risk management, it is important to align it with the organisation’s risk appetite. The risk appetite will be influenced by the size and type of organisation, its capacity for risk and its ability to exploit opportunities and withstand setbacks.

Once the severity of the risk has been established, one or more of the following methods of controlling risk can be applied:

- accepting the risk
- sharing or transferring the risk
- risk reduction
- risk avoidance.

Insurance is a long established control method for transferring risk. This applies to a number of types of operational risk, for example, damage to buildings. However, more recently there has been an increase in the use of insurance combined with other methods such as business continuity management.

One issue with measuring and managing subjective operational risks is that unless the risk occurs, it is not possible to be certain of the impact of the risk. The severity of the risk may be underestimated.

One of the issues with operational risk is the continuously changing business environment. This is stressed in *Internal control: guidance for directors on the Combined Code*, also known as the Turnbull Report (1999), which states:

‘A company’s objectives, its internal organisation and the environment in which it operates, are continually evolving and, as a result, the risks it faces are continually changing. A sound system of internal control therefore depends on a thorough and regular evaluation of the risks to which it is exposed.’

Once a decision has been made about how to manage or control the risk, it is important to have a process in place to monitor actively and to review and report regularly on the risk management framework.
Critical success factors in risk management are:

- clearly identified senior management to support, own and lead on risk management
- existence and adoption of a framework for risk management that is transparent and repeatable
- risk is actively monitored and regularly reviewed
- management of risk is fully embedded in the management process and consistently applied
- clear communication with all staff
- management of risks is closely linked to the achievement of objectives.

**Case studies**

Case: Managing business interruption – Lehman Brothers


One of the key operational risks to any organisation is business interruption. To manage this risk, organisations must have a robust business continuity plan. There is a close link between business continuity management (BCM) and operational risk.

There have been significant developments in the area of BCM. Earlier disaster recovery plans anticipated a failure and subsequent recovery from it, while many business operations now are so time critical that no outage whatsoever can be tolerated. BCM now embraces both the creation of a ‘non-stop’ infrastructure and operational capability, as well as recovery from operational failure.

Five key steps in business continuity management:

1. Assessing and objective setting.
2. Critical process identification.
5. Monitoring, testing and improving.
Other case studies

The Confederation of British Industry (CBI) produces a variety of business guides. Included within these guides are a number of case studies covering the implementation of an operation risk management system. Available from: www.cbi.org.uk [Accessed 18 July 2008]


This article outlines the implementation and embedding of operation risk measures across an organisation.


References


(2000). *Croner’s management of business risk*. Kingston upon Thames: CCH

**Further information**

**Articles**

Full text articles available to CIMA members from Business Source Corporate through My CIMA [www.cimaglobal.com/mycima](http://www.cimaglobal.com/mycima) [Accessed 17 July 2008]

Backhouse, T. *Operational risk management: overcoming the hidden dangers*. Credit Control, 2002, Volume 23, Issue 5, p. 28

Grody, A.D. *Operational risk management to the rescue*. Securities Industry News, 26/05/2008, Volume 20, Issue 21, pp 4-10


Katz, D. *How much of ‘operational’ risk management is hype?* National Underwriter/Property and Casualty Risk and Benefits Management, 05/06/2000, Volume 104, Issue 23, p. 15


Books


CIMA publications


Other publications


Websites

The Business Continuity Institute (BCI)
The BCI promotes business continuity management worldwide.
Available from: www.thebci.org
[Accessed 16 July 2008]

The Journal of Operational Risk
Subscription journal on operational risk.
Available from: www.thejournalofoperationalrisk.com
[Accessed 16 July 2008]

KnowledgeLeader
Subscription website that provides audit programmes, checklists, tools, resources and best practice information to help internal auditors and risk management professionals save time, manage risk, and add value.
30 day free trial available. Available from: http://digbig.com/4xeqb
[Accessed 16 July 2008]