Contents

1 Introduction

1.1 PURPOSE OF THIS GUIDE

This guide is intended to help organizations put in place an effective framework for risk management. This will help them take informed decisions about the risks that affect their strategic, programme, project and operational objectives.

The guide provides a route map for risk management, bringing together principles, an approach, a process with a set of interrelated steps and pointers to more detailed sources of advice on risk management techniques and specialisms. It also provides advice on how these principles, approach and process should be embedded, reviewed and applied differently depending on the nature of the objectives at risk.

The M_o_R framework is based on four core concepts as shown in Figure 1.1.

- **M_o_R principles** Principles are essential for the development and maintenance of good risk management practice. They are informed by corporate governance principles and the international standard for risk management, ISO31000: 2009. They are high-level and universally applicable statements that provide guidance to organizations as they design an appropriate approach to risk management as part of their internal controls.
- **M_o_R approach** Principles need to be adapted and adopted to suit each individual organization. An organization's approach to the principles needs to be agreed and defined within a risk management policy, process guide and strategies.
- **M_o_R process** The process is divided into four main steps: identify, assess, plan and

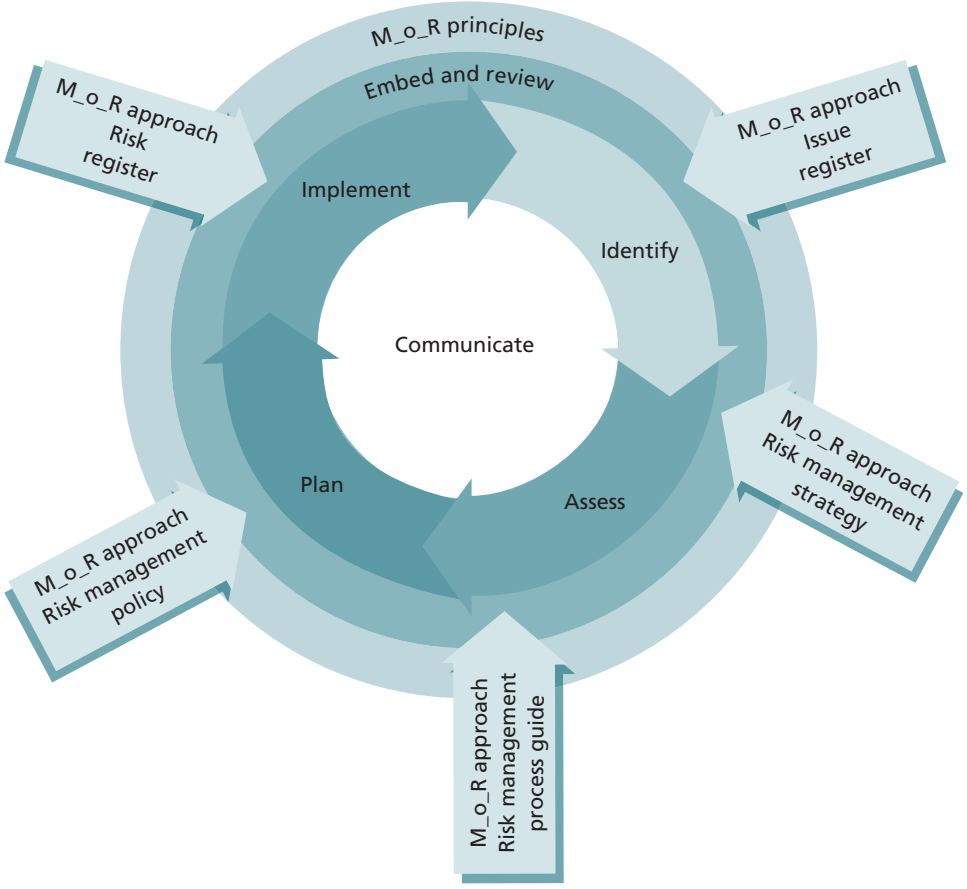

Figure 1.1 M_o_R framework

implement. Each step describes the inputs, outputs, tasks and techniques involved to ensure that the overall process is effective.

- **Embedding and reviewing M_o_R** Having put in place an approach and process that satisfy the principles, an organization should ensure that they are consistently applied across the organization and that their application undergoes continual improvement in order for them to be effective.

1.2 WHAT IS RISK?

Risk is defined as *'an uncertain event or set of events that, should it occur, will have an effect on the achievement of objectives. A risk is measured by the combination of the probability of a perceived threat or opportunity occurring and the magnitude of its impact on objectives.'*

All organizations, including temporary ones such as those concerned with programmes or projects, will encounter uncertain events when trying to achieve their objectives. These uncertain events may arise inside or outside the organization. Each individual uncertain event that would impact one or more objectives is known as a risk. Within this definition, 'threat' is used to describe an uncertain event that would have a negative impact on objectives if it occurred and 'opportunity' is used to describe an uncertain event that would have a positive impact on objectives if it occurred. The combined effect of risks to a set of objectives is known as risk exposure, and is the extent of the risk borne by that part of the organization at that time.

1.3 WHAT IS RISK MANAGEMENT?

Every organization manages its risk in some way, but not always in a way that is visible, repeatable or consistent, to support effective decision-making. The task of risk management is to ensure that an organization makes cost-effective use of a risk management process that includes a series of well-defined steps. The aim is to improve internal control and support better decision-making through a good understanding of individual risks and the overall risk exposure that exists at a particular time.

Accordingly, in this guide, the term **'risk management'** refers to the systematic application of principles, an approach and a process to the tasks of identifying and assessing risks, and then planning and implementing risk responses. This provides a disciplined environment for proactive decision-making.

For risk management to be effective, risks need to be:

- **Identified** This involves considering uncertainties that would affect the achievement of objectives within the context of a particular organizational activity and then describing them to ensure that there is a common understanding.
- **Assessed** This involves estimating the probability, impact and proximity of individual risks so they can be prioritized, and understanding the overall level of risk (risk exposure) associated with the organizational activity.
- **Controlled** This involves planning appropriate responses to risks, assigning owners and actionees and then implementing, monitoring and controlling these responses.

1.4 WHY IS RISK MANAGEMENT IMPORTANT?

Some risk-taking is inevitable if an organization is to achieve its objectives. Those organizations that are more risk aware appreciate that actively managing not only potential problems (threats) but also potential opportunities provides them with a competitive advantage. Taking and managing risk is the very essence of business survival and growth.

Effective risk management is likely to improve performance against objectives by contributing to:

- Fewer sudden shocks and unwelcome surprises
- More efficient use of resources
- Reduced waste
- Reduced fraud
- Better service delivery
- Reduction in management time spent fire-fighting
- Better management of contingent and maintenance activities
- Lower cost of capital
- Improved innovation
- Increased likelihood of change initiatives being achieved
- More focus internally on doing the right things properly
- More focus externally to shape effective strategies.

Many of these benefits are applicable to both the private and public sectors. Whereas the private sector focuses mainly on shareholder returns and the preservation of shareholder value, the public sector's role is to perform cost-effectively, in accordance with government legislation and policies.

1.5 HOW HAS RISK MANAGEMENT DEVELOPED?

Risk has always been an inherent feature in any undertaking therefore risk management is not a new concept for organizations. The nature of risk management, however, has evolved rapidly over recent decades. It was in the 1960s that risk management began to be recognized as one of the essential skills required for management. The earliest application of risk management within organizations tended to focus on insurance management in terms of establishing financial capacity for the negative effects of adverse events. During the 1970s a broader view started to emerge whereby organizations began to develop a better understanding of the nature of the risks being faced and looked at alternatives to insurance. There remained, however, a focus on the negative effects of risk.

Only in recent years have organizations begun to recognize that risk management, in its broadest sense, applies to both negative threats and positive opportunities. In each case a proactive approach is required, which seeks to understand the size of the possible threats and opportunities so that a decision can be made about whether to accept the threat or opportunity or act upon it in some way. Whilst it may be tempting to consider these as separate activities, in practice, opportunities and threats are seldom independent.

The first edition of this guide was published in 2002 in response to UK government guidance on corporate governance and internal control issued in 1999 (Turnbull Guidance). This guidance required company directors to implement a generic framework for risk management across all parts of their organization to establish internal control and to report to shareholders thereon.

Since then the world of risk management has moved forward in both the public and private sectors. Legislation that requires corporate governance and internal control has increased in many parts of the world and this has created an increased focus on formal risk management. In response to organizations devising optimal ways to respond to legislation, and to identify, assess and control risk, other trends have emerged, such as the recent emphasis on enterprise risk management (ERM).

Whilst this guide has been produced in the UK and has primary examples based on UK regulations, it is intended to be of benefit to both domestic and international organizations.

1.6 CORPORATE GOVERNANCE AND INTERNAL CONTROL

A major factor influencing the drive towards more formalized approaches to risk management has been the increased focus given to corporate governance and internal control across the world following the high-profile collapses of a number of major organizations. Corporate governance and internal control regimes exist in all major economies and are designed to protect the assets, earning capacity and reputation of organizations.

The purpose of corporate governance according to the UK Corporate Governance Code (June 2010) is to facilitate effective, entrepreneurial and prudent management that can deliver long-term success to a company.

Corporate governance is described in the most recent UK code as *the system by which organizations are directed and controlled*. Boards of directors are responsible for the governance of their organization. The role of shareholders in governance is to appoint directors and auditors to ensure effective governance is in place. The responsibilities of the board include setting the company's strategic aims, providing the leadership to put them into effect, supervising management and reporting to shareholders on their stewardship. The role of the audit committee is to support the board and accounting officer by reviewing the comprehensiveness and reliability of assurances.

Risk management is one way an organization establishes internal control alongside financial, operational and compliance controls. The UK Corporate Governance Code (2010) defines this principle:

The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board

should maintain sound risk management and internal control systems and review the effectiveness of these at least annually.

Regarding internal control, the current UK Guidance for Directors (2005) states that the board's deliberations should include the consideration of the following factors:

- The nature and extent of the risks facing the company
- The extent and categories of risk which it regards as acceptable for the company to bear
- The likelihood of the risks concerned materialising
- The company's ability to reduce the incidence and impact on the business of the risks that do materialise
- The costs of operating particular controls relative to the benefit thereby obtained in managing the related risks.

Internal audits must cover all internal control systems, not just financial controls.

In the US a more radical approach has been taken resulting in new legislation in the form of the Public Company Accounting Reform and Investor Protection Act of 2002 (also known as Sarbanes-Oxley). The main thrust of the Act is to influence the behaviour and conduct of public companies to ensure that they issue informative and accurate financial statements. Of particular note in the context of risk management are the following provisions:

- The chief executive officer (CEO) and the chief financial officer (CFO) of public companies are held personally accountable for establishing and maintaining internal controls and evaluating their effectiveness. They are also responsible for advising their auditors of all significant deficiencies in the design or operation of the internal controls.
- Public companies are required to include in each annual report an internal control report that states the responsibility of management to establish and maintain an adequate internal control structure and procedures for financial reporting and an assessment of the effectiveness of these.

For those organizations operating in the financial services industry, the Basel Accord (currently Basel II) is also important. The original Basel Accord (Basel I) was agreed in 1988 and contains capital requirement rules stating that credit institutions, such as banks and building societies, must at all times maintain a minimum amount of financial capital in order to cover the risks to which they are exposed. The aim is to ensure the financial 'soundness' of such institutions, to maintain customer confidence in the solvency of the institutions, to ensure the stability of the financial system at large, and to protect depositors against losses. Basel II was issued in 2004 and is a revision of the original framework. Its aim was to make the framework more risk sensitive and representative of the risk management practices of modern banks.

Although the official UK guidance, or other international guidance or legislation, applies strictly only to private companies listed on a stock exchange, the corporate governance principles and generic guidance on internal controls are increasingly judged to be relevant to all organizations in the private and public sectors. This is because they fundamentally outline the way in which the organization can achieve the optimal balance between innovation and control.

The purpose of the M_o_R guide is to provide detailed advice on how to embed effective risk management. Following this advice should achieve the objectives and principles laid down in UK corporate governance and internal control policies for both UK and international organizations across public and private sectors. Whilst organizations will always be controlled by national guidelines, which will vary from country to country, the one constant is the need for organizational risk management that protects and enhances shareholder and wider societal value.

1.7 WHERE AND WHEN SHOULD RISK MANAGEMENT BE APPLIED?

Risk management should be applied continuously with information made available when critical decisions are being made. Decisions about risk will vary depending on whether the risk relates to long-, medium- or short-term organizational objectives (see Figure 1.2).

- **Strategic** decisions are primarily concerned with long-term goals; these set the context for decisions at other levels of the organization. The risks associated with strategic decisions may not become apparent until well into the

future. It is, therefore, essential to review these decisions and associated risks regularly.

- Medium-term goals are usually addressed through **programmes** and **projects** to bring about business change. Decisions relating to medium-term goals are narrower in scope than strategic ones, particularly in terms of timeframe and financial responsibilities.
- At the **operational** level, the emphasis is on short-term goals to ensure ongoing continuity of business services. Decisions about risk at this level, however, must also support the achievement of long- and medium-term goals.

M_o_R describes how risk management applies to long-, medium- and short-term objectives by describing four organizational perspectives. The need to capture and integrate all the risk exposures that are faced by an organization across these four perspectives is discussed in more detail in Chapter 6. Chapter 6 also refers to the use of ERM as a way of capturing all risk exposures and determining the optimal blend of responses to risks through financial provisions or non-financial methods.

Risk management should be the basis for effective management of an organization at all times, including in support of decision-making when planning the introduction of change to any of the organizational perspectives described above.

1.8 RISK SPECIALISMS

In addition to application across the strategic, programme, project and operational perspectives, the guidance within M_o_R applies to the work carried out by risk specialists who focus on particular types of risk in an organization. Such specialisms have developed as organizations have applied particular approaches to managing specific types of risks. In some cases, these have been built into legislation or other government or industry guidance giving them justification as a specialism.

Appendix E provides an introduction to some risk specialisms and directs the reader to more detailed information. The specialisms covered are:

- Business continuity management
- Incident and crisis management
- Health and safety management
- Security risk management
- Financial risk management
- Environmental risk management
- Reputational risk management
- Contract risk management.

Although portfolio, programme and project risk management is a specialism as defined here, it is omitted from this list as programmes and projects are covered as specific M_o_R perspectives.

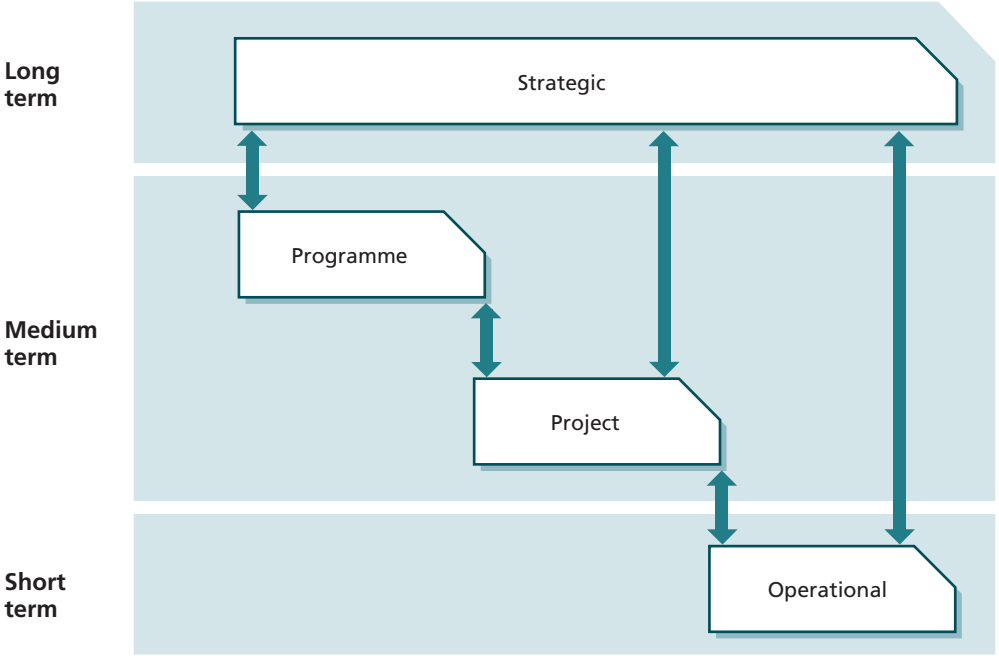

Figure 1.2 Organizational perspectives

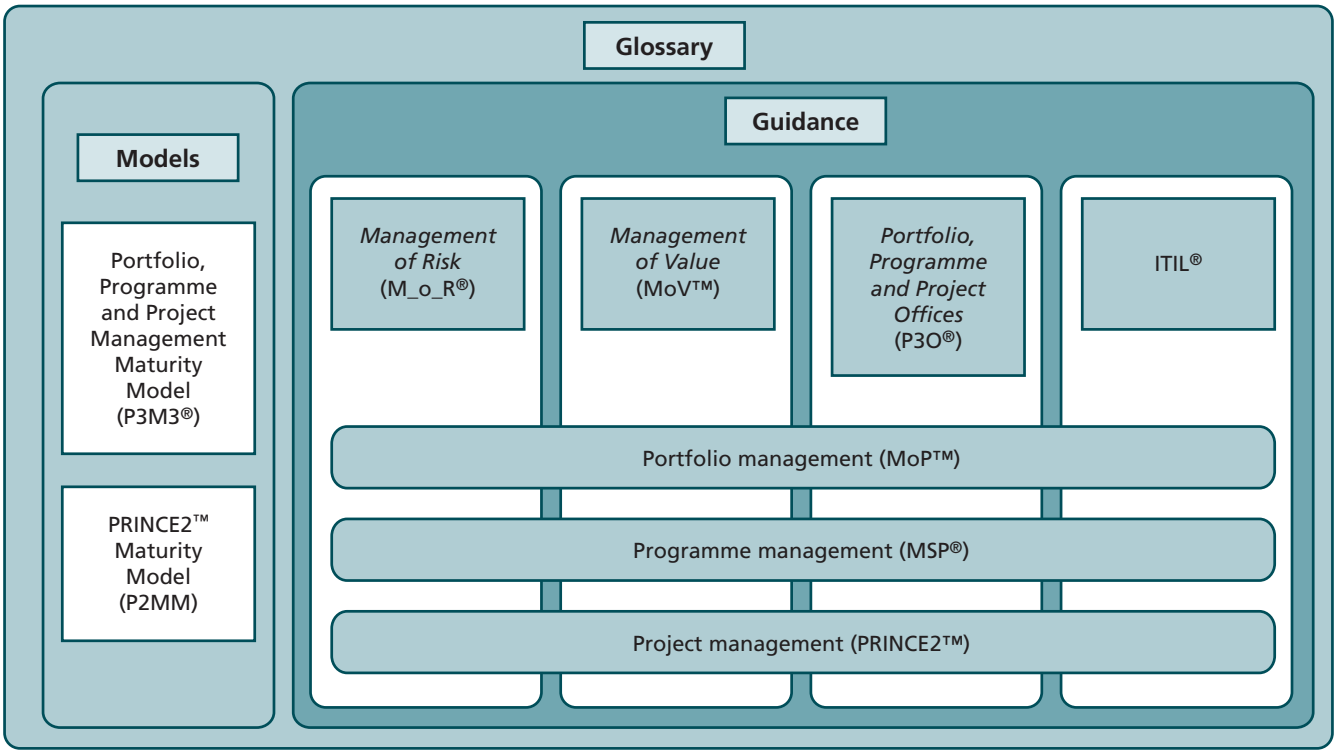

Figure 1.3 M_o_R's relationship with other OGC guides

1.9 OGC BEST-PRACTICE GUIDANCE

Management of Risk is part of a suite of guidance developed by the UK Office of Government Commerce (OGC), which is aimed at helping organizations and individuals manage their projects, programmes and services consistently and effectively. Figure 1.3 outlines the structure of the set, showing how M_o_R fits within the overall scheme.

1.10 HOW TO USE THIS GUIDE

It is recommended that all readers familiarize themselves with the first four chapters of this book, as these provide comprehensive guidance on the most important aspects of risk management. Chapter 5 will be of interest to those with responsibility for reviewing and improving risk management within their organization. Chapter 6 will be of interest to those who manage risks within one or more of the four perspectives covered, have corporate responsibility for risk management or risk management guidance, or have responsibilities for integrating risk management activities across the perspectives (ERM).

Chapter 1 has introduced some key terminology and explained what risk management is; why it is important to organizations; and where and when it should be applied. It has also provided a brief introduction to the subjects of corporate governance and internal control.

Chapter 2 outlines the management of risk principles underlying effective risk management in an organization. They are proven, empowering and universally applicable statements that provide guidance to organizations as they develop and implement their risk management approach.

Chapter 3 presents the management of risk approach and the documents that M_o_R recommends are created and maintained to implement the approach. It is supported by Appendix A, which contains the M_o_R document outlines.

Chapter 4 describes the main steps of the management of risk process. It contains practical pointers for identifying, assessing and controlling risks. It is supported by Appendix B, which contains common techniques used in the risk process.

Chapter 5 describes and provides guidance on how an organization can introduce and embed risk management, and then measure the success and maturity of its risk management. It is supported by Appendix C, which outlines

an approach to performing risk management health checks, and Appendix D, which describes risk management maturity models.

Chapter 6 explains when and how M_o_R principles, concepts and processes should be applied throughout an organization, from the strategic, programme, project and operational perspectives, and when integrating risk management activities across perspectives.

The appendices provide supporting detail as follows:

- **A** Management of risk document outlines
  To be read in conjunction with Chapter 3 on the management of risk approach
- **B** Common techniques
  To be read in conjunction with Chapter 4 on the management of risk process
- **C** Management of risk health check
  To be read in conjunction with Chapter 5 on embedding and reviewing management of risk
- **D** Management of risk maturity model
  To be read in conjunction with Chapter 5 on embedding and reviewing management of risk
- **E** Risk specialisms
  Provides introductory information and links to additional reading about risk specialisms.