irm

Fundamentals of Risk Management

Understanding, evaluating and implementing effective risk management

Paul Hopkin

KoganPage

Preface

Benefits of enterprise risk management

A string of large and highly public organizational and Governmental failures over the past 10 years (Woolworths, Golden Wonder, Northern Rock, Citigroup, Enron and even the entire banking system of Iceland) has focused the attention of investors, customers and regulators on the way in which directors, managers and boards are managing risk. This has led to a greater appreciation of the wider scope of risks facing organizations, which in turn has led to risk management becoming a core management discipline.

Risk is everywhere and derives directly from unpredictability. The process of identifying, assessing and managing risks brings any business full circle back to its strategic objectives: for it will be clear that not everything can be controlled. The local consequences of events on a global scale, such as terrorism, pandemics and credit crunches, are likely to be unpredictable. However, they can also include the creation of new and valuable opportunities. Many of today's household names were born out of times of adversity.

Risk management provides a framework for organizations to deal with and to react to uncertainty. Whilst it acknowledges that nothing in life is certain, the modern practice of risk management is a systematic and comprehensive approach, drawing on transferable tools and techniques. These basic principles are sector-independent and should improve business resilience, increase predictability and contribute to improved returns. This is particularly important given the pace of change of life today.

Risk management involves a healthy dose of both common sense and strategic awareness, coupled with an intimate knowledge of the business, an enquiring mind and most critically superb communication and influencing skills.

The Institute of Risk Management's International Certificate in risk management is an introductory qualification which reflects the changing and global nature of risk management. Recognizing both the enterprise-wide (or 'ERM') importance of comprehensive risk management

and the growing use of international standards (such as ISO 31000), this qualification equips future professional risk managers with the fundamental knowledge and tools to make invaluable contributions to long-term organizational growth and prosperity.

This textbook, as well as being the core reading for the IRM International Certificate, is a valuable resource for all organizations and indeed anyone with an interest in risk management.

Sophie Williams is Deputy Chief Executive of the Institute of Risk Management, risk management's leading worldwide professional education, training and knowledge body. Further information about the International Certificate or the Institute is available from the IRM website www.theirm.org.

Sophie Williams

Acknowledgements

The author is grateful to a large number of people who have helped with the development of the ideas that are included in this book. In particular, the following individuals provided considerable input into the final version:

- Richard Archer;
- Bill Aujla;
- Steve Fowler;
- Alex Hindson;
- Edward Sankey;
- Paul Taylor;
- Carolyn Williams;
- Sophie Williams.

Paul Hopkin

THIS PAGE IS INTENTIONALLY LEFT BLANK

Introduction

Risk management in context

This book is intended for all who want a comprehensive introduction to the theory and application of risk management. It sets out an integrated introduction to the management of risk in public and private organizations. Studying this book will provide insight into the world of risk management and may also help readers decide whether risk management is a suitable career option for them.

Many readers will wish to use this book in order to gain a better understanding of risk and risk management and thereby fulfil the primary responsibilities of their jobs with an enhanced understanding of risk. This book is designed to deliver the syllabus of the International Certificate in Risk Management qualification of the Institute of Risk Management. However, it also acts as an introduction to the discipline of risk management for those interested in the subject but not (yet) undertaking a course of study.

An introduction to risk and risk management is provided in the first Part of this book and the key features of risk management are set out in the next two Parts. Parts 4, 5 and 6 concentrate on the application of risk management tools and techniques, as well as considering the outputs from the risk management process and the benefits that arise.

We all face risks in our everyday lives. Risks arise from personal activities and range from those associated with travel through to the ones associated with personal financial decisions. There are considerable risks present in the domestic component of our lives and these include fire risks in our homes and financial risks associated with home ownership. Indeed, there are also a whole range of risks associated with domestic and relationship issues, but these are outside the scope of this book.

This book is primarily concerned with business and commercial risks and the roles that we fulfil during our job or occupation. However, the task of evaluating risks and deciding

how to respond to them is a daily activity not only at work, but also at home and during leisure activities.

Nature of risk

Recent events in the world have brought risk into higher profile. Terrorism, extreme weather events and the global financial crisis represent the extreme risks that are facing society and commerce. These extreme risks exist in addition to the daily, somewhat more mundane risks mentioned above.

Evaluating the range of risk responses available and deciding the most appropriate response in each case is at the heart of risk management. Responding to risks should produce benefits for us as individuals, as well as for the organizations where we work and/or are employed.

Within our personal and domestic lives, many of the responses to risk are automatic. Our ways of avoiding fire and road traffic accidents are based on well-established and automatic responses. Fire and accident are the types of risks that can only have negative outcomes and they are often referred to as hazard risks.

Certain other risks have established or required responses that are imposed on us as individuals and/or on organizations as mandatory requirements. For example, in our personal lives, buying insurance for a car is usually a legal requirement, whereas buying insurance for a house is often not, but is good risk management and very sensible.

Keeping your car in good mechanical order will reduce the chances of a breakdown. However, even vehicles that are fully serviced and maintained do occasionally break down. Maintaining your car in good mechanical order will reduce the chances of breakdown, but will not eliminate them completely. These types of risks that have a large degree of uncertainty associated with them are often referred to as control risks.

As well as hazard and control risks, there are risks that we take because we desire (and probably expect) a positive return. For example, you will invest money in anticipation that you will make a profit from the investment. Likewise, placing a bet or gambling on the outcome of a sporting event is undertaken in anticipation of receiving positive payback.

People participate out of choice in motor sports and other potentially dangerous leisure activities. In these circumstances, the return may not be financial, but can be measured in terms of pride, self-esteem or peer group respect. Undertaking activities involving risks of this type, where a positive return is expected, can be referred to as taking opportunity risks.

Risk management

Organizations face a very wide range of risks that can impact the outcome of their operations. The desired overall aim may be stated as a mission or a set of corporate objectives. The events that can impact an organization may inhibit what it is seeking to achieve (hazard risks), enhance that aim (opportunity risks), or create uncertainty about the outcomes (control risks).

Risk management needs to offer an integrated approach to the evaluation, control and monitoring of these three types of risk. This book examines the key components of risk management and how it can be applied. Examples are provided that demonstrate the benefits of risk management to organizations in both the public and private sectors. Risk management also has an important part to play in the success of not-for-profit organizations such as charities and (for example) clubs and other membership bodies.

The risk management process is well established, although it is presented in a number of different ways and often uses differing terminologies. The different terminologies that are used by different risk management practitioners and in different business sectors are explored in this book. In addition to a description of the established risk management standards, a simplified description of risk management that sets out the key stages in the risk management process is also presented to help with understanding.

The risk management process cannot take place in isolation. It needs to be supported by a framework within the organization. Once again, the risk management framework is presented and described in different ways in the range of standards, guides and other publications that are available. In all cases, the key components of a successful risk management framework are the communications and reporting structure (architecture), the overall risk management strategy that is set by the organization (strategy) and the set of guidelines and procedures (protocols) that have been established. The importance of the risk architecture, strategy and protocols (RASP) is discussed in detail in this book.

The combination of risk management processes, together with a description of the framework in place for supporting the process, constitutes a risk management standard. There are several risk management standards in existence, including the IRM Standard and the recently published British Standard BS 31100. There is also the American COSO ERM framework. The latest addition to the available risk management standards is the international standard, ISO 31000, published in 2009. The well established and respected Australian Standard AS 4360 (2004) was withdrawn in 2009 in favour of ISO 31000. AS 4360 was first published in 1995 and ISO 31000 includes many of the features and offers a similar approach to that previously described in AS 4360.

Further information on existing standards and other published guides is set out in Chapter 1.6. Additionally, references are included in each Part of this book to provide further material to enable the reader to gain a comprehensive introduction to the subject of risk management.

Risk management terminology

Most risk management publications refer to the benefits of having a common language of risk within the organization. Many organizations manage to achieve this common language and common understanding of risk management processes and protocols at least internally. However, it is usually the case that within a business sector, and sometimes even within individual organizations, the development of a common language of risk can be very challenging.

Reference and supporting materials have a great range of terminologies in use. The different approaches to risk management, the different risk management standards that exist and the wide range of guidance material that is available often use different terms for the same feature or concept. This is regrettable and can be very confusing, but it is inescapable.

Attempts are being made to develop a standardized language of risk, and ISO Guide 73 has been developed as the common terminology that should be used in all ISO standards. The terminology set out in ISO Guide 73 will be used throughout this book as the default set of definitions, wherever possible. However, the use of a standard terminology is not always possible and alternative definitions may be required.

To assist with the difficult area of terminology, Appendix A sets out the basic terms and definitions that are used in risk management. It also provides cross reference between the different terms in use to describe the same concept. Where appropriate and necessary a table setting out a range of definitions for the same concept is included within the relevant chapter of the book and these tables are cross-referenced in Appendix A.

Benefits of risk management

There are a range of benefits arising from successful implementation of risk management. These benefits are summarized in this book as compliance, assurance, decisions and efficiency/effectiveness/efficacy (CADE3). Compliance refers to risk management activities designed to ensure that an organization complies with legal and regulatory obligations.

The board of an organization will require assurance that significant risks have been identified and appropriate controls put in place. In order to ensure that correct business decisions are taken, the organization should undertake risk management activities that provide additional structured information to assist with business decision making.

Finally, a key benefit from risk management is to enhance the efficiency of operations within the organization. Risk management should provide more than assistance with the efficiency of operations. It should also help ensure that business processes (including process enhancements by way of projects and other change initiatives) are effective and that the selected strategy is efficacious, in that it is capable of delivering exactly what is required.

Risk management inputs are required in relation to strategic decision making, but also in relation to the effective delivery of projects and programmes of work, as well as in relation to the routine operations of the organization. The benefits of risk management can also be identified in relation to these three timescales of activities within the organization. The outputs from risk management activities can benefit organizations in three timescales and ensure that the organization achieves:

- efficacious strategy;
- effective processes and projects;
- efficient operations.

In order to achieve a successful risk management contribution, the intended benefits of any risk management initiative have to be identified. If those benefits have not been identified, then there will be no means of evaluating whether the risk management initiative has been successful.

Therefore, good risk management must have a clear set of desired outcomes/benefits. Appropriate attention should be paid to each stage of the risk management process, as well as to details of the design, implementation and monitoring of the framework that supports these risk management activities.

Features of risk management

Failure to adequately manage the risks faced by an organization can be caused by inadequate risk recognition, insufficient analysis of significant risks and failure to identify suitable risk response activities. Also, failure to set a risk management strategy and to communicate that strategy and the associated responsibilities may result in inadequate management of risks. It is also possible that the risk management procedures or protocols may be flawed, such that these protocols may actually be incapable of delivering the required outcomes.

The consequences of failure to adequately manage risk can be disastrous and result in inefficient operations, projects that are not completed on time and strategies that are not delivered, or were incorrect in the first place. The hallmarks of successful risk management are considered in this book. In order to be successful, the risk management initiative should be proportionate, aligned, comprehensive, embedded and dynamic (PACED).

Proportionate means that the effort put into risk management should be appropriate to the level of risk that the organization faces. Risk management activities should be aligned with other activities within the organization. Activities will also need to be comprehensive, so that any risk management initiative covers all the aspects of the organization and all the risks that it faces. The means of embedding risk management activities within the organization are discussed in this

book. Finally, risk management activities should be dynamic and responsive to the changing business environment faced by the organization.

Book structure

The book is presented in six Parts, together with two appendices. Part 1 provides the introduction to risk management and introduces all of the basic concepts. These concepts are explored in more detail in later Parts. Part 2 explores the importance of risk management strategy and considers the vital importance of the risk management policy, as well as exploring the successful implementation of that policy.

Part 3 considers the importance of risk assessment as a fundamental requirement of successful risk management. Risk classification and risk analysis tools and techniques are considered in detail in this Part. Part 4 considers the impact of risk on organizations, and this extends to the evaluation of corporate governance requirements. Also, the analysis of stakeholder expectations and the relationship between risk management and a simple business model is considered.

Part 5 sets out the options for risk response in detail. Analysis of the various risk control techniques is presented, together with examples of options for the control of selected hazard risks. This Part also considers the importance of insurance and risk transfer. Finally, Part 6 considers risk assurance and risk reporting. The role of the internal audit function, together with the importance of corporate social responsibility and the options for reporting on risk management are all considered.

Appendix A provides a glossary of terms and cross-references the different terminologies used by different risk management practitioners. Appendix B provides a step-by-step implementation guide to enterprise risk management (ERM), as described in Chapter 25. It includes reference to all of the acronyms used in the book and sets out the key concepts relevant to each step of the successful implementation of a risk management initiative.

Risk management in practice

In order to bring the subject of risk management to life, short illustrative examples are used throughout the text. These examples focus on a small number of organizations in order to give some context to the ideas described. Risk management activities cannot be undertaken out of context, and so these organizations provide context to the ideas and concepts that are described.

The most often used examples to illustrate a point are a haulage company, a sports club, a theatre, a publisher and the large stock-exchange-listed company that, for the sake of illustration, owns

the sports club and the haulage company. Examples are also used of how risk management principles can be applied to the personal risks faced in private life.

In addition to these general examples, real life situations and examples are also used, where a case study is helpful. Each Part of the book concludes with a brief extract from the report and accounts of a selected company to illustrate the main risk management topics covered in the Part. Although many of these examples are from the UK, the principles are equally applicable to other parts of the world.

Future for risk management

As the global financial crisis has enfolded, there is an increasing tendency for news reports to indicate that risk is bad and risk management has failed. In reality, neither of these two statements is correct. Organizations have to address the risks that they face because many of them have to undertake high-risk activities, either because these activities cannot be avoided, or because the activities are undertaken in order to produce a positive outcome for the organization and its stakeholders.

The global financial crisis does not demonstrate the failure of risk management, but rather the failure of the management of organizations to successfully address the risks that they faced. Achieving benefits from risk management requires carefully planned implementation of the risk management process in the organization, as well as the design and successful embedding of a suitable and sufficient risk management framework.

By setting out an integrated approach to risk management, this book provides a description of the fundamental components of successful management of business/corporate risks. It describes a wealth of risk management tools and techniques and provides information on successful delivery of an integrated and enterprise-wide approach to risk management.

Global financial crisis

The extract below offers a summary of the actions that would help to avoid a repeat of the global financial crisis. Many organizations lack a common risk management framework across the enterprise. This has many elements, each of which is required to help avoid similar disasters in the future:

- First, there should be common processes, terminology and practices for managing risks of all kinds.
- Second, it is essential that risk tolerances be fully understood, communicated and monitored across the enterprise.

- Third, risk management practices should be incorporated into all key business processes and decisions.
- And, fourth, management should make risk-related decisions using dedicated high quality risk information.

Part 1

Introduction to risk management

Learning outcomes for Part 1

- provide a range of definitions of risk and risk management and describe the usefulness of the various definitions;
- list the characteristics of a risk that need to be identified in order to provide a full risk description;
- describe options for classifying risks according to the nature, source and timescale of impact;
- outline the options for the attachment of risks to various attributes of an organization and describe advantages of each approach;
- use a risk matrix to represent the likely impact of a risk materializing in terms of likelihood and magnitude;
- outline the principles (PACED) and aims of risk management and its importance to operations, projects and strategy;
- describe the nature of hazard, control and opportunity risks and how organizations should respond to each type;

- outline the development of the discipline of risk management, including the various specialist areas and approaches;
- describe the key benefits of risk management in terms of compliance, assurance, decisions and efficiency/effectiveness/efficacy (CADE3);
- describe the key stages in the risk management process and the main components of a risk management framework;
- briefly describe the key features of the best-established risk management standards and frameworks.

Part 1 Further reading

British Standard BS 31100 (2008) Risk management – Code of practice, www.standardsuk.com.
COSO Enterprise Risk Management – Integrated Framework (2004) Executive Summary, www.coso.org.
Financial Reporting Council Internal Control Revised Guidance for Directors on the Combined Code (2005), www.frc.org.uk.
Institute of Risk Management A Risk Management Standard (2002), www.theirm.org.
International Standard ISO 31000 (2009) Risk management – Principles and guidelines, www.iso.org.
ISO Guide 73 (2009) Risk management – Vocabulary – Guidelines for use in standards, www.iso.org.

Approaches to defining risk

Definitions of risk

The *Oxford English Dictionary* definition of risk is as follows: 'a chance or possibility of danger, loss, injury or other adverse consequences' and the definition of at risk is 'exposed to danger'. In this context, risk is used to signify negative consequences. However, taking a risk can also result in a positive outcome. A third possibility is that risk is related to uncertainty of outcome.

Take the example of owning a motorcar. For most people, owning a motorcar is an opportunity to become more mobile and gain the related benefits. However, there are uncertainties in owning a motorcar that are related to maintenance and repair costs. Finally, motor cars can be involved in accidents, so there are obvious negative outcomes that can occur.

Definitions of risk can be found from many sources and some key definitions are set out in Table 1.1. An alternative definition is also provided to illustrate the broad nature of risks that can affect organizations. The Institute of Risk Management (IRM) defines risk as the combination of the probability of an event and its consequence. Consequences can range from positive to negative. This is a widely applicable and practical definition that can be easily applied.

The international guide to risk-related definitions is ISO Guide 73 and it defines risk as 'effect of uncertainty on objectives'. This definition appears to assume a certain level of knowledge about risk management and it is not easy to apply to everyday life. The meaning and application of this definition will become clearer as the reader progresses through this book.

Guide 73 also notes that an effect may be positive, negative, or a deviation from the expected. These three types of events can be related to risks as opportunity, hazard or uncertainty, and this relates to the example of motorcar ownership outlined above. The guide notes that risk is often described by an event, a change in circumstances, a consequence, or a combination of these and how they may affect the achievement of objectives.

Table 1.1 Definitions of risk

Organization	Definition of risk
ISO Guide 73 ISO 31000	Effect of uncertainty on objectives. Note that an effect may be positive, negative, or a deviation from the expected. Also, risk is often described by an event, a change in circumstances or a consequence.
Institute of Risk Management (IRM)	Risk is the combination of the probability of an event and its consequence. Consequences can range from positive to negative.
"Orange Book" from HM Treasury	Uncertainty of outcome, within a range of exposure, arising from a combination of the impact and the probability of potential events.
Institute of Internal Auditors	The uncertainty of an event occurring that could have an impact on the achievement of the objectives. Risk is measured in terms of consequences and likelihood.
Alternative Definition by the author	Event with the ability to impact (inhibit, enhance or cause doubt about) the mission, strategy, projects, routine operations, objectives, core processes, key dependencies and / or the delivery of stakeholder expectations.

The Institute of Internal Auditors (IIA) defines risk as the uncertainty of an event occurring that could have an impact on the achievement of objectives. The IIA adds that risk is measured in terms of consequences and likelihood. Different disciplines define the term risk in very different ways. The definition used by health and safety professionals is that risk is a combination of likelihood and magnitude, but this may not be sufficient for more general risk management purposes.

Risk in an organizational context is usually defined as anything that can impact the fulfilment of corporate objectives. However, corporate objectives are usually not fully stated by most organizations. Where the objectives have been established, they tend to be stated as internal, annual, change objectives. This is particularly true of the personal objectives set for members of staff in the organization, where objectives usually refer to change or developments, rather than the continuing or routine operations of the organization.

It is generally accepted that risk is best defined by concentrating on risks as events, as in the definition of risk provided in ISO 31000 and the definition provided by the Institute of Internal Auditors, as set out in Table 1.1. In order for a risk to materialize, an event must occur. Greater clarity is likely to be brought to the risk management process if the focus is on events. For example, consider what could disrupt a theatre performance.

The events that could cause disruption include a power cut, absence of a key actor, substantial transport failure or road closures that delay the arrival of the audience, as well as the illness of a significant number of staff. Having identified the events that could disrupt the performance, the management of the theatre needs to decide what to do to reduce the chances of one of these events causing the cancellation of a performance. This analysis by the management of the theatre is an example of risk management in practice.

Types of risks

Risk may have positive or negative outcomes or may simply result in uncertainty. Therefore, risks may be considered to be related to an opportunity or a loss or the presence of uncertainty for an organization. Every risk has its own characteristics that require particular management or analysis. In this book, as in the Guide 73 definition, risks are divided into three categories:

- hazard (or pure) risks;
- control (or uncertainty) risks;
- opportunity (or speculative) risks.

It is important to note that there is no 'right' or 'wrong' subdivision of risks. Readers will encounter other subdivisions in other texts and these may be equally appropriate. It is, perhaps, more common to find risks described as two types, pure or speculative. Indeed, there are many debates about risk management terminology. Whatever the theoretical discussions, the most important issue is that an organization adopts the risk classification system that is most suitable for its own circumstances.

There are certain risk events that can only result in negative outcomes. These risks are hazard risks or pure risks, and these may be thought of as operational or insurable risks. In general, organizations will have a tolerance of hazard risks and these need to be managed within the levels of tolerance of the organization. A good example of a hazard risk faced by many organizations is that of theft.

There are certain risks that give rise to uncertainty about the outcome of a situation. These can be described as control risks and are frequently associated with project management. In general, organizations will have an aversion to control risks. Uncertainties can be associated with the benefits that the project produces, as well as uncertainty about the delivery of the project on time, within budget and to specification. The management of control risks will often be undertaken in order to ensure that the outcome from the business activities falls within the desired range.

At the same time, organizations deliberately take risks, especially marketplace or commercial risks, in order to achieve a positive return. These can be considered as opportunity or speculative risks, and an organization will have a specific appetite for investment in such risks.

The application of risk management tools and techniques to the management of hazard risks is the best and longest-established branch of risk management, and much of this text will concentrate on hazard risks. There is a hierarchy of controls that apply to hazard risks and this will be discussed in a later chapter. Hazard risks are associated with a source of potential harm or a situation with the potential to undermine objectives in a negative way. Hazard risks are the most common risks associated with organizational risk management, including occupational health and safety programmes.

Control risks are associated with unknown and unexpected events. They are sometimes referred to as uncertainty risks and they can be extremely difficult to quantify. Control risks are often associated with project management. In these circumstances, it is known that the events will occur, but the precise consequences of those events are difficult to predict and control. Therefore, the approach is based on minimizing the potential consequences of these events.

There are two main aspects associated with opportunity risks. There are risks/dangers associated with taking an opportunity, but there are also risks associated with not taking the opportunity. Opportunity risks may not be visible or physically apparent, and they are often financial in nature. Although opportunity risks are taken with the intention of having a positive outcome, this is not guaranteed. Opportunity risks for small businesses include moving a business to a new location, acquiring new property, expanding a business and diversifying into new products.

Risk description

In order to fully understand a risk, a detailed description is necessary so that a common understanding of the risk can be identified and ownership/responsibilities may be clearly understood. Table 1.2 provides information on the range of information that must be recorded to fully understand a risk. The list of information set out in Table 1.2 is most applicable to hazard risks and the list will need to be modified to provide a full description of control or opportunity risks.

So that the correct range of information can be collected about each risk, the distinction between hazard, control and opportunity risks needs to be clearly understood. The example below is intended to distinguish between these three types of risk, so that the information required in order to describe each type of risk can be identified.

Table 1.2 Risk description

- Name or title of risk
- Statement of risk, including scope of risk and details of possible events and dependencies
- Nature of risk, including details of the risk classification and timescale of potential impact
- Stakeholders in the risk, both internal and external
- Risk attitude, appetite, tolerance or limits for the risk
- Likelihood and magnitude of event and consequences should the risk materialize at current/residual level
- Control standard required or target level of risk
- Incident and loss experience
- Existing control mechanisms and activities
- Responsibility for developing risk strategy and policy
- Potential for risk improvement and level of confidence in existing controls
- Risk improvement recommendations and deadlines for implementation
- Responsibility for implementing improvements
- Responsibility for auditing risk compliance

Computer viruses

In order to understand the distinction between hazard, control and opportunity risks, the example of the use of computers is useful. Virus infection is an operational or hazard risk and there will be no benefit to an organization suffering a virus attack on its software programs. When an organization installs or upgrades a software package, control risks will be associated with the upgrade project.

The selection of new software is also an opportunity risk, where the intention is to achieve better results by installing the new software, but it is possible that the new software will fail to deliver all of the functionality that was intended and the opportunity benefits will not be delivered. In fact, the failure of the functionality of the new software system may substantially undermine the operations of the organization.

Inherent level of risk

It is important to understand the uncontrolled level of all risks that have been identified. This is the level of the risk before any actions have been taken to change the likelihood or magnitude of the risk. Although there are advantages in identifying the inherent level of risk, there are practical difficulties in identifying this with certain types of risks.

Identifying the inherent level of the risk enables the importance of the control measures in place to be identified. The Institute of Internal Auditors (IIA) has the view that the assessment of all risks should commence with the identification of the inherent level of the risk. The guidance from the IIA states that 'in the risk assessment, we look at the inherent risks before considering any controls.' The new International Risk Management Standard, ISO 31000, recommends that risks are assessed at both inherent and current levels.

Often, a risk matrix will be used to show the inherent level of the risk in terms of likelihood and magnitude. The reduced or current level of the risk can then be identified, after the control or controls have been put in place. The effort that is required to reduce the risk from its inherent level to its current level can be clearly indicted on the risk matrix.

Terminology varies and the inherent level of risk is sometimes referred to as the absolute risk or gross risk. Also, the current level of risk is often referred to as the residual level or the managed level of risk. The example in the box below provides an example of how inherently high-risk activities are reduced to a lower level of risk by the application of sensible and practical risk response options.

> *Crossing the road*
>
> Crossing a busy road would be inherently dangerous if there were no controls in place and many more accidents would occur. When a risk is inherently dangerous, greater attention is paid to the control measures in place, because the perception of risk is much higher. Pedestrians do not cross the road without looking and drivers are always aware that pedestrians may step into the road. Often, other traffic calming control measures are necessary to reduce the speed of the motorists or increase the risk awareness of both motorists and pedestrians.

Risk classification systems

Risks can be classified according to the nature of the attributes of the risk, such as timescale for impact, and the nature of the impact and/or likely magnitude of the risk. They can also

be classified according to the timescale of impact after the event occurs. The source of the risk can also be used as the basis of classification. In this case, a risk may be classified according to its origin, such as counterparty or credit risk.

A further way of classifying risks is to consider the nature of the impact. Some risks can cause detriment to the finances of the organization, whereas others will have an impact on the activities or the infrastructure. Further, risks may have an impact on the reputation of the organization or on its status and the way it is perceived in the marketplace.

Individual organizations will decide on the risk classification system that suits them best, depending on the nature of the organization and its activities. Also, many risk management standards and frameworks suggest a specific risk classification system. If the organization adopts one of these standards, then it will tend to follow the classification system recommended.

The risk classification system that is selected should be fully relevant to the organization concerned. There is no universal classification system that fulfils the requirements of all organizations. It is likely that each risk will need to be classified in several ways in order to clearly understand its potential impact. However, many classification systems offer common or similar structures, as will be described in later chapters.

Risk likelihood and magnitude

Risk likelihood and magnitude are best demonstrated using a risk map, sometimes referred to as a risk matrix. Risk maps can be produced in many formats. Whatever format is used for a risk map, it is a very valuable tool for the risk management practitioner. The basic style of risk map plots the likelihood of an event against the magnitude or impact should the event materialize.

Figure 1.1 is an illustration of a simple risk matrix, sometimes referred to as a heat map. This is a commonly used method of illustrating risk likelihood and the magnitude (or severity) of the event should the risk materialize. The use of the risk matrix to illustrate risk likelihood and magnitude is a fundamentally important risk management tool. The risk matrix can be used to plot the nature of individual risks, so that the organization can decide whether the risk is acceptable and within the risk appetite and/or risk capacity of the organization.

Throughout this book, a standard format for presenting a risk map has been adopted. The horizontal axis is used to represent likelihood. The term likelihood is used rather than frequency, because the word frequency implies that events will definitely occur and the map is registering how often these events take place. Likelihood is a broader word that includes frequency, but also refers to the chances of an unlikely event happening. However, in risk management literature, the word probability will often be used to describe the likelihood of a risk materializing.

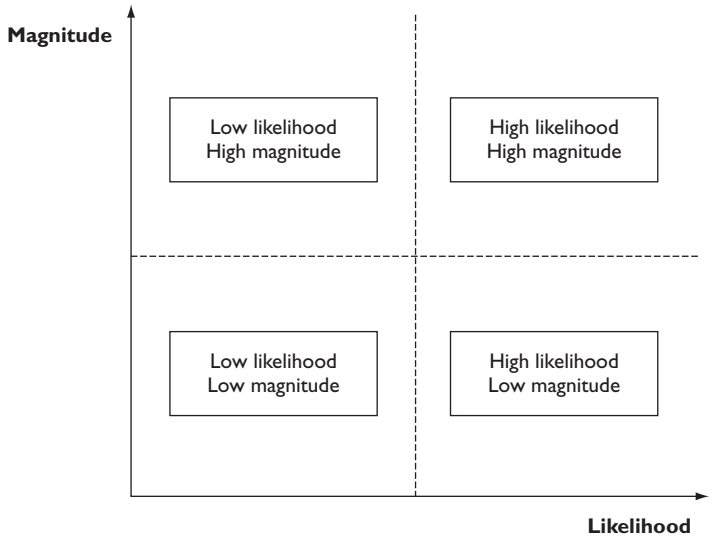

Figure 1.1 Risk likelihood and magnitude

The vertical axis is used to indicate magnitude in Figure 1.1. The word magnitude is used rather than severity, so that the same style of risk map can be used to illustrate hazard, control and opportunity risks. Severity implies that the event is undesirable and is, therefore, related to hazard risks.

Figure 1.1 maps likelihood against the magnitude of an event. However, the more important consideration for risk managers is not the magnitude of the event, but the impact or consequences. For example, a large fire could occur that completely destroys a warehouse of a distribution and logistics company. Although the magnitude of the event may be large, if the company has produced plans to cope with such an event, the impact on the overall business may be much less than would otherwise be anticipated.

The magnitude of an event may be considered to be the inherent level of the event and the impact can be considered to be the risk-managed level. Because the impact (or consequences) of an event is usually more important than its magnitude (or severity), then every risk matrix used in the remainder of this book will plot impact against likelihood, rather than magnitude against likelihood.

The risk matrix will be used throughout this book to provide a visual representation of risks. It can also be used to indicate the likely risk control mechanisms that can be applied. The risk matrix can also be used to record the inherent, current (or residual) and target levels of the risk.

Colour coding is often used on the risk matrix to provide a visual representation of the importance of each risk under consideration. As risks move towards the top right-hand corner of the

risk matrix, they become more likely and have a greater impact. Therefore, the risk becomes more important and immediate and effective risk control measures need to be introduced.

As a practical example of risk management in action at strategic level, consider the uncertainties embedded in the merger involving Delta Airlines and Northwest Airlines. This illustrates that organizations take strategic decisions that involve high levels of risk and uncertainty. There will be considerable uncertainties relating to whether all of the benefits outlined below can be delivered in practice.

Uncertainty in strategic decisions

An agreement has been reached and, barring any roadblocks from antitrust authorities, Delta Airlines and Northwest Airlines are merging and will operate under the Delta Airlines name. Delta Airlines released information outlining the basic elements of the deal and the ramifications it foresees for the new airline and its passengers.

The list of benefits it sees by merging

- Combining Delta and Northwest will create a global US carrier that can compete with foreign airlines that continue to increase service to the United States.
- Customers and communities will benefit from access to a global route system and a more financially stable airline.
- More destinations will result in more schedule options and more opportunities to earn and redeem frequent flyer miles.
- Delta customers will benefit from Northwest's routes to Asian markets and Northwest's customers will benefit from Delta's routes to other markets.
- Delta and Northwest complementary common membership in the SkyTeam alliance will ease the integration risk that has complicated some airline mergers.

2

Impact of risk on organizations

Risk importance

Following the events in the world financial system during 2008, all organizations are taking a greater interest in risk and risk management. It is increasingly understood that the explicit management of risks brings benefits. By taking a proactive approach to risk and risk management, organizations will be able to achieve the following three areas of improvement:

- Operations will become more efficient because events that can cause disruption will be identified in advance and actions taken to reduce the likelihood of these events occurring, reducing the damage caused by these events and containing the cost of the events that can cause disruption to normal efficient production operations.
- Processes will be more effective, because consideration will have been given to selection of the processes and the risks involved in the alternatives that may be available. Also, process changes that are delivered by way of projects will be more effectively and reliably delivered.
- Strategy will be more efficacious in that the risks associated with different strategic options will be fully analysed and better strategic decisions will be reached. Efficacious refers to the fact that the strategy that will be developed will be fully capable of delivering the required outcomes.

It is no longer acceptable for organizations to find themselves in a position whereby unexpected events cause financial loss, disruption to normal operations, damage to reputation and loss of market presence. Stakeholders now expect that organizations will take full account of the risks that may cause disruption within operations, late delivery of projects or failure to deliver strategy.

The exposure presented by an individual risk can be defined in terms of the likelihood of the risk materializing and the impact of the risk when it does materialize. As risk exposure

increases, then likely impact will also increase. Throughout this book, the term impact is used in preference to the alternative word, consequences. This is because the term impact is preferred in business continuity planning evaluations.

Injury to key player

A sports club will wish to reduce the chances of a key player being absent through injury. However, key players do get injured and the club will need to consider the impact of such an event in advance of it happening. If the injury is serious, the player may be absent for a significant length of time. There is likely to be a substantial impact, which will be most obvious on the pitch where the success of the team is likely to be reduced. However, other consequences may also result and these could include the loss of revenue from the sale of shirts and other merchandise with that player's name and number. Arrangements to reduce the potential for loss of income should also be considered.

Impact of hazard risks

Hazard risks undermine objectives, and the level of impact of such risks is a measure of their significance. Risk management has its longest history and earliest origins in the management of hazard risks. Hazard risk management is closely related to the management of insurable risks. Remember that a hazard (or pure) risk can only have a negative outcome.

Hazard risk management is concerned with issues such as health and safety at work, fire prevention, damage to property and the consequences of defective products. Hazard risks can cause disruption to normal operations, as well as resulting in increased costs and poor publicity associated with disruptive events.

Hazard risks are related to business dependencies, including IT and other supporting services. There is increasing dependence on the IT infrastructure of most organizations and IT systems can be disrupted by computer breakdown or fire in server rooms, as well as virus infection and deliberate hacking or computer attacks.

Theft and fraud can also be significant hazard risks for many organizations. This is especially true for organizations handling cash or managing a significant number of financial transactions. Techniques relevant to the avoidance of theft and fraud include adequate security procedures, segregation of financial duties, and authorization and delegation procedures, as well as the vetting of staff prior to employment.

Attachment of risks

Although most standard definitions of risk referred to risks as being attached to corporate objectives, Figure 2.1 provides an illustration of the options for the attachment of risks. Risks are shown in the diagram as being capable of impacting the key dependencies that deliver the core processes of the organization. Corporate objectives and stakeholder expectations help define the core processes of the organization. These core processes are key components of the business model and can relate to operations, projects and corporate strategy.

The intention of Figure 2.1 is to demonstrate that significant risks can be attached to features of the organization other than corporate objectives. Significant risks can be identified by considering the key dependencies of the organization, the corporate objectives and/or the stakeholder expectations, as well as by analysis of the core processes of the organization.

In the build-up to the recent financial crisis, banks and other financial institutions established operational and strategic objectives. By analysing these objectives and identifying the risks that could prevent the achievement of them, risk management made a contribution to the achievement of the high-risk objectives that ultimately led to the failure of the organizations. This example illustrates that attaching risks to attributes other than objectives is not only possible but may well have been desirable in these circumstances.

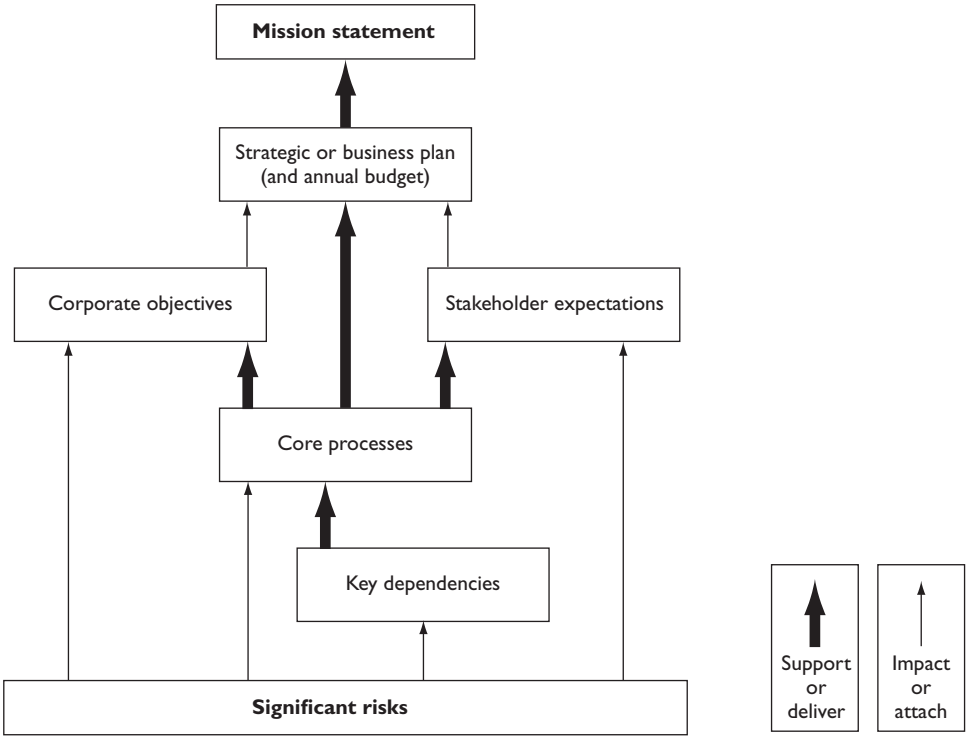

Figure 2.1 Attachment of risks

It is clearly the case that risks are greater in circumstances of change. Therefore, linking risks to change objectives is not unreasonable, but the analysis of each objective in turn may not lead to robust risk recognition/identification. In any case, business objectives are usually stated at too high a level for the successful attachment of risks.

To be useful to the organization, the corporate objectives should be presented as a full statement of the short, medium and long-term aims of the organization. Internal, annual, change objectives are usually inadequate, because they may fail to fully identify the operational (or efficiency), change (or competition) and strategic (or leadership) requirements of the organization.

The most important disadvantage associated with the 'objectives-driven' approach to risk and risk management is the danger of considering risks out of the context that gave rise to them. Risks that are analysed in a way that is separated from the situation that led to them will not be capable of rigorous and informed evaluation. It can be argued that a more robust analysis can be achieved when a 'dependencies-driven' approach to risk management is adopted.

It remains the case that many organizations continue to use an analysis of corporate objectives as a means of identifying risks, because some benefits do arise from this approach. For example, using this 'objectives-driven' approach facilitates the analysis of risks in relation to the positive and uncertain aspects of the events that may occur, as well as facilitating the analysis of the negative aspects.

If the decision is taken to attach risks to the objectives of the organization, then it is important that these objectives have been fully and completely developed. Not only do the objectives need to be challenged to ensure that they are full and complete, but the assumptions that underpin the objectives should also receive careful and critical attention.

Core processes will be discussed later in this book and may be considered as the high level processes that drive the organization. In the example of a sports club, one of the key processes is the operational process 'delivering successful results on the pitch'. Risks may be attached to this core process, as well as being attached to objectives and/or key dependencies.

Although risks can be attached to other features of the organization, the standard approach is to attach risks to corporate objectives. One of the standard definitions of risk is that it is something that can impact (undermine, enhance or cause doubt) the achievement of corporate objectives. This is a useful definition, but it does not provide the only means of identifying significant risks.

Risk and reward

Another feature of risk and risk management is that many risks are taken by an organization in order to achieve a reward. Figure 2.2 illustrates the relationship between the level of risk and

the anticipated size of reward. A business will launch a new product because it believes that greater profit is available from the successful marketing of the new product. In launching a new product, the organization will put resources at risk because it has decided that a certain amount of risk taking is appropriate. The value put at risk represents the risk appetite of the organization with respect to the activity that it is undertaking.

When an organization puts value at risk in this way, it should do so with the full knowledge of the risk exposure and it should be satisfied that the risk exposure is within the appetite of the organization. Even more important, it should ensure that it has sufficient resources to cover the risk exposure. In other words, the risk exposure should be quantified, the appetite to take that level of risk should be confirmed and the capacity of the organization to withstand any foreseeable adverse consequences should be clearly established.

Not all business activities will offer the same return for risk taken. Start-up operations are usually high risk and the initial expected return may be low. Figure 2.2 demonstrates the probable risk–return development for a new organization or a new product. The activity will commence in the bottom right-hand corner as a start-up operation, which is high risk and low return.

As the business develops, it is likely to move to a higher return for the same level of risk. This is the growth phase for the business or product. As the investment matures, the reward may remain high, but the risks should reduce. Eventually, an organization will become fully mature and move towards the low-risk and low-return quadrant. The normal expectation in very mature markets is that the organization or product will be in decline.

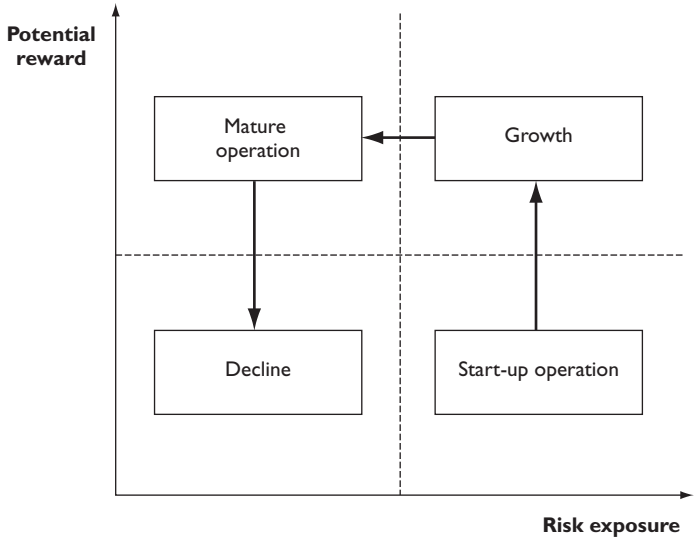

Figure 2.2 Risk and reward

The particular risks that the organization faces will need to be identified by management or by the organization. Appropriate risk management techniques will then need to be applied to the risks that have been identified. The nature of these risk responses and the nature of their impact will be considered in a later chapter.

The above discussion about risk and reward applies to opportunity risks. However, it must always be the case that risk management effort produces rewards. In the case of hazard risks, it is likely that the reward for increased risk management effort will be fewer disruptive events. In the case of project risks, the reward for increased risk management effort will be that the project is more likely to be delivered on time, within budget and to specification/quality. For opportunity risks, the risk–reward analysis should result in fewer unsuccessful new products and a higher level of profit or (at worst) a lower level of loss for all new activities or new products.

Risk versus reward

In a Formula 1 Grand Prix, the Ferrari team decided to send a driver out on wet-weather tyres, before the rain had actually started. Wet-weather tyres wear out very quickly in dry conditions and make the car much slower. If the rain had started immediately, this would have proved to be a very good decision.

In fact, the rain did not start for four or five laps, by which time the driver had been overtaken by most other drivers and his set of wet-weather tyres were ruined in the dry conditions. He had to return to the pits for a further set of new tyres more suited to the race conditions. In this case, a high-risk strategy was adopted in anticipation of significant rewards. However, the desired rewards were not achieved and significant disadvantage resulted.

Risk and uncertainty

Risk is sometimes defined as uncertainty of outcomes. This is a somewhat technical, but nevertheless useful definition and it is particularly applicable to the management of control risks. Control risks are the most difficult to identify and define, but are often associated with projects. The overall intention of a project is to deliver the desired outcomes on time, within budget and to specification.

For example, when a building is being constructed, the nature of the ground conditions may not always be known in detail. As the construction work proceeds, more information will be available about the nature of the ground conditions. This information may be positive news that the ground is stronger than expected and less foundation work is required. Alternatively, it may be discovered that the ground is contaminated or the ground is weaker than expected

or that other potentially adverse circumstances exist, such as archaeological remains being discovered.

Given this uncertainty, these risks should be considered to be control risks and the overall management of the project should take account of the uncertainty associated with these different types of risk. It would be unrealistic for the project manager to assume that only adverse aspects of the ground conditions will be discovered. Likewise, it would be unwise for the project manager to assume that conditions will be better than he has been advised, just because he wants that to be the case.

Because control risks cause uncertainty, it may be considered that an organization will have an aversion to these risks. Perhaps, the real aversion is to the potential variability in outcomes. A certain level of deviation from the project plan can be tolerated, but it must not be too great. Tolerance in relation to control risks can be considered to have the same meaning as in the manufacture of engineering components, where the components must be of a certain size, within acceptable tolerance limits.

Attitudes to risk

Different organizations will have different attitudes to risk. Some organizations may be considered to be risk averse, whilst other organizations will be risk aggressive. To some extent, the attitude of the organization to risk will depend on the sector and the nature and maturity of the marketplace within which it operates, as well as the attitude of the individual board members.

Risks cannot be considered outside the context that gave rise to the risks. It may appear that an organization is being risk aggressive, when in fact, the board has decided that there is an opportunity that should not be missed. However, the fact that the opportunity is high risk may not have been fully considered.

One of the major contributions from successful risk management is to ensure that strategic decisions that appear to be high risk are actually taken with all of the information available. Improvement in the robustness of decision-making processes is one of the key benefits of risk management.

Other key factors that will determine the attitude of the organization to risk include the stage in the maturity cycle, as shown in Figure 2.2. For an organization that is in the start-up phase, a more aggressive attitude to risk is required than for an organization that is enjoying growth or one that is a mature organization in a mature marketplace. Where an organization is operating in a mature marketplace and is suffering from decline, the attitude to risk will be much more risk averse.

It is because the attitude to risk has to be different when an organization is a start-up operation compared with a mature organization, that it is often said that certain high-profile businessmen are very good at entrepreneurial start-up, but are not as successful in running mature businesses. Different attitudes to risk are required at different parts of the business maturity cycle.

Chicken farmer

Consider the example of a very successful breeder and reseller of chicken in a mature marketplace involving little risk and steady and manageable growth prospects. The CEO saw an opportunity to transform his family's company. Overturning the family tradition of avoiding debt, he borrowed $500,000 and set about fundamentally changing the operation from a chicken farmer and reseller to a fully automated chicken raising and retail operation.

It is not surprising that many great CEOs and founders had a strong propensity for risk – without taking at least some calculated risks, the businesses would not have flourished and more importantly lasted. Some had nothing to lose, but for others, there was a tremendous amount at stake – both personally and professionally.

Like vision, an appetite for risk taking is considered almost a prerequisite for success. Knowing when to be a risk taker and opportunistic is critical to being able to successfully take advantage of the times. It can also be disastrous when the context of the times changes sharply. The same act performed too soon or too late or in the wrong scene may make a person a fool rather than a hero. That analysis fully applies to risk taking in business.