irm

Fundamentals of Risk Management

Understanding, evaluating and implementing effective risk management

Paul Hopkin

KoganPage

Fundamentals of Risk Management

THIS PAGE IS INTENTIONALLY LEFT BLANK

Fundamentals of Risk Management

Understanding, evaluating and implementing effective risk management

Paul Hopkin

LONDON PHILADELPHIA NEW DELHI

First published in Great Britain and the United States in 2010 by Kogan Page Limited.

120 Pentonville Road
London N1 9JN
United Kingdom
www.koganpage.com

525 South 4th Street, #241
Philadelphia PA 19147
USA

4737/23 Ansari Road
Daryaganj
New Delhi 110002
India

ISBN 978 0 7494 5942 0
E-ISBN 978 0 7494 5943 7

British Library Cataloguing-in-Publication Data

A CIP record for this book is available from the British Library.

Library of Congress Cataloging-in-Publication Data

Hopkin, Paul.
Fundamentals of risk management : understanding, evaluating, and implementing effective risk management / Paul Hopkin.
p. cm.
Includes index.
ISBN 978-0-7494-5942-0 -- ISBN 978-0-7494-5943-7 (ebook) 1. Risk management. I. Title.
HD61.H567 2010
658.15'5--dc22
2009046006

Typeset by Saxon Graphics Ltd, Derby
Printed and bound in India by Replika Press Pvt Ltd

Dedication

Michael, David and Kathy

THIS PAGE IS INTENTIONALLY LEFT BLANK

Contents

Figures

Tables

THIS PAGE IS INTENTIONALLY LEFT BLANK

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.

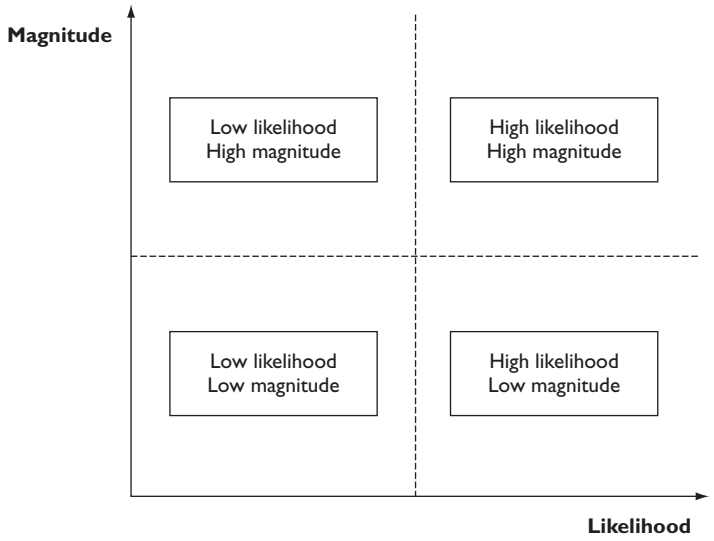


Figure 1.1 Risk likelihood and magnitude

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.

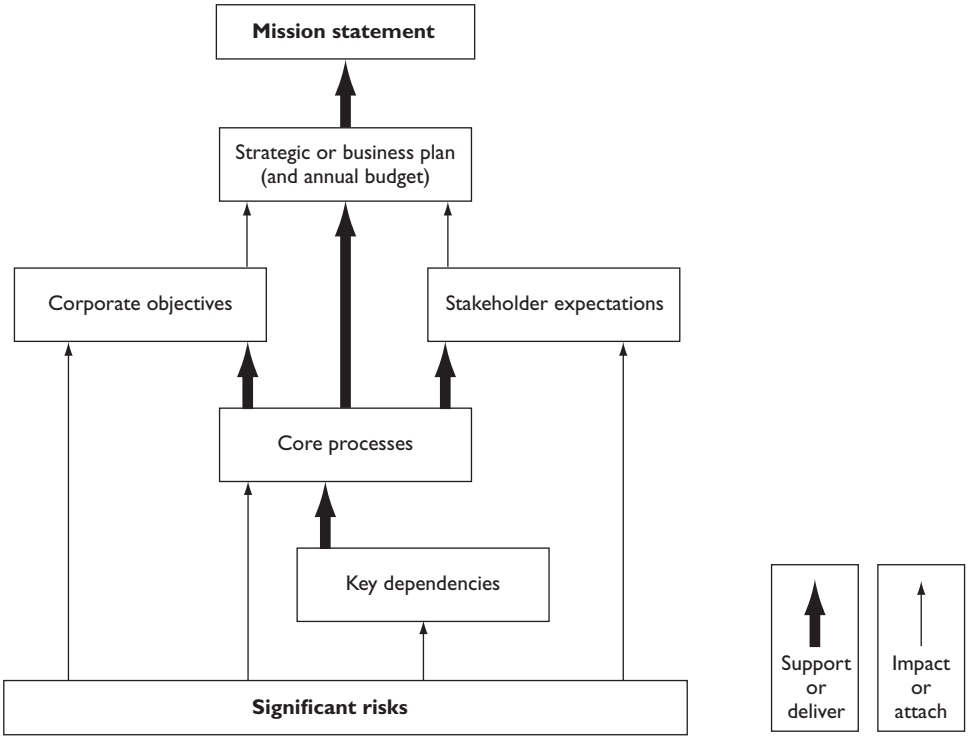


Figure 2.1 Attachment of risks

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.

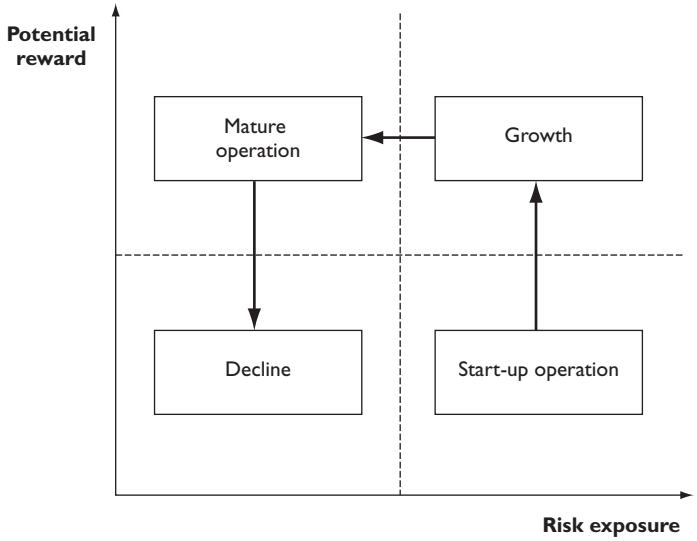


Figure 2.2 Risk and reward

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.

3
Types of risks

Timescale of risk impact

Risks can be classified in many ways. Hazard risks can be divided into many types of risks, including risks to property, risks to people and risks to the continuity of the business. There are a range of formal risk classification systems and these will be considered in a later part of this book. Although it should not be considered to be a formal risk classification system, this part considers the value of classifying risks according to the timeframe for the impact of the risk.

The classification of risks as long, medium and short-term impact is a very useful means of analysing the risk exposure of an organization. These risks will be related to the strategy, tactics and operations of the organization, respectively. In this context, risks may be considered as related to events, changes in circumstances, actions or decisions.

In general terms, long-term risks will impact several years, perhaps up to five years, after the event occurs or the decision is taken. Long-term risks therefore relate to strategic decisions. When a decision is taken to launch a new product, the impact of that decision (and the success of the product itself) may not be fully apparent for some time.

Medium-term risks have their impact some time after the event occurs or the decision is taken, and typically this will be about a year later. Medium-term risks are often associated with projects or programmes of work. For example, if a new computer software system is to be installed, then the choice of computer system is a long-term or strategic decision. However, decisions regarding the project to implement the new software will be medium-term decisions with medium-term risk attached.

Short-term risks have their impact immediately after the event occurs. Accidents at work, traffic accidents, fire and theft are all short-term risks that have an immediate impact and immediate consequences as soon as the event has occurred. These short-term risks cause immediate disruption to normal efficient operations and are probably the easiest types of risks to identify and manage.

Insurable risks are quite often short-term risks, although the exact timing and magnitude/impact of the insured events is uncertain. In other words, insurance is designed to provide protection against risks that have immediate consequences. In the case of insurable risks, the nature and consequences of the event may be understood, but the timing of the event is unpredictable. In fact, whether the event will occur at all is not known at the time the insurance policy is taken out.

By way of example, consider the operation of a new computer software system in more detail. The organization will install the new software in anticipation of gaining efficiency and greater functionality. The decision to install new software and the choice of the software involves opportunity risks. The installation will require a project, and certain risks will be involved in the project. The risks associated with the project are control risks. After the new software has been installed, it will be exposed to hazard risks. It may not deliver all of the functionality required and the software may be exposed to various risks and virus infection. These are the hazard risks associated with this new software system.

Hazard, control and opportunity risks

We have already seen in Chapter 1 that risks can be divided into three categories: Definitions of these three types of risk are also given in Appendix A. They are:

- hazard risks;
- control risks;
- opportunity risks.

A common language of risk is required throughout the organization if the contribution of risk management is to be maximized. The use of a common language will also enable the organization to develop an agreed perception of risk. Part of developing this common language and perception of risk is to agree a risk classification system or series of such systems.

For example, consider people reviewing their financial position and the risks they currently face regarding finances. It may be that the key financial dependencies relate to achieving adequate income and managing expenditure. The review should include an analysis of the risks to job security and pension arrangements, as well as property ownership and other investments. This part of the analysis will provide information on the risks to income and the nature of those risks (opportunity risks).

Regarding expenditure, the review will consider spending pattern to determine whether cost cutting is necessary (hazard risks). It will also consider leisure time activities, including holiday arrangements and hobbies, and there will be some uncertainties regarding expenditure and the costs of these activities (control risks).

Hazard risks are the risks that can only inhibit achievement of the corporate mission. Typically, these are insurable type risks or perils, and will include fire, storm, flood, injury and so on. The discipline of risk management has strong origins in the management and control of hazard risks. Normal efficient operations may be disrupted by loss, damage, breakdown, theft and other threats associated with a wide range of dependencies, as shown in Table 3.1, and these may include (for example):

- people;
- premises;
- assets;
- suppliers;
- information technology (IT);
- communications.

Control risks are risks that cause doubt about the ability to achieve the mission of the organization. Internal financial control protocols are a good example of a response to a control risk. If the control protocols are removed, there is no way of being certain about what will happen. Control risks are the most difficult type of risk to describe, but later Parts of this book will assist with understanding.

Control risks are associated with uncertainty, and examples include the potential for legal non-compliance and losses caused by fraud. They are usually dependent on the successful management of people and successful implementation of control protocols. Although most organizations ensure that control risks are carefully managed, they may, nevertheless, remain potentially significant.

Opportunity risks are the risks that are (usually) deliberately sought by the organization. These risks arise because the organization is seeking to enhance the achievement of the mission, although they might inhibit the organization if the outcome is adverse. This is the most important type of risk for the future long-term success of any organization.

Many organizations are willing to invest in high-risk business strategies in anticipation of a high profit or return. These organizations may be considered to have a large appetite for opportunity investment. Often, the same organization will have the opposite approach to hazard risks and have a small hazard tolerance. This may be appropriate, because the attitude of the organization may be that it does not want hazard-related risks consuming corporate resources, when it is putting so much value at risk investing in opportunities.

Table 3.1 Categories of disruption

Category	Examples of disruption
People	Lack of people skills and / or resources Unexpected absence of key personnel Ill-health, accident or injury to people
Premises	Inadequate or insufficient premises Denial of access to premises Damage to or contamination of premises
Assets	Accidental damage to physical assets Breakdown of plant or equipment Theft or loss of physical assets
Suppliers	Disruption caused by failure of supplier Delivery of defective goods or components Failure of outsourced services and facilities
Information technology (IT)	Failure of IT hardware systems Disruption by hacker or computer virus Inefficient operation of computer software
Communications	Inadequate management of information Failure of internal or external communications Transport failure or disruption

Hazard tolerance

As discussed earlier in this part, organizations face exposure to a wide range of risks. These risks will be hazard risks, control risks and opportunity risks. Organizations need to tolerate a hazard risk exposure, accept exposure to control risks and invest in opportunity risks.

In the case of health and safety risks, it is generally accepted that organizations should be intolerant of these risks and should take all appropriate actions to eliminate them. In practice, this is not possible and organizations will manage safety risks to the lowest level that is cost-effective and in compliance with the law.

For example, an automatic braking system fitted to trains to stop them passing through red lights is technically feasible. However, this may represent an unreasonable investment for the train operating company. The consequences of trains going through red lights may be regarded as the risk exposure or hazard tolerance of the organization but the cost of introducing the automatic braking system may be considered to be prohibitively high.

A less emotive example is related to theft. Most organizations will suffer a low level of petty theft and this may be tolerable. For example, businesses based in an office environment will suffer some theft of stationery, including paper, envelopes and pens. The cost of eliminating this petty theft may be very large and so it becomes cost-effective for the organization to accept that these losses will occur. The approach to theft in shops may be very different in different retail sectors, as illustrated by the example below.

Security standards

An example can be seen in the operation of a security-conscious jewellery shop. Customers are allowed into the shop one at a time. They are recorded on CCTV as they wait to enter. Items are held securely, and customers are invited to ask to see specific items under the suspicious gaze of the shop assistants. Of course, some customers are put off, but equally the shops suffer negligible rates of shoplifting.

Contrast this with a supermarket, where there are no barriers on entry and customers are allowed to handle all of the items. There is CCTV monitoring the shops, and there are likely to be store detectives patrolling – but the object of the security is to deter rather than to prevent shoplifting. Shoplifting does occur, but at rates that are acceptable to the shop owners. Conversely, few potential customers are put off visiting the shop because of the measures.

Management of hazard risks

The range of hazard risks that can affect an organization needs to be identified by the organization. Hazard risks can result in unplanned disruption for the organization. Disruptive events cause inefficiency and are to be avoided, unless they are part of, for example, planned maintenance or testing of emergency procedures. The desired state in relation to hazard risk management is that there should be no unplanned disruption or inefficiency from any of the reasons shown in Table 3.1.

Table 3.1 provides a list of the events that can cause unplanned disruption or inefficiency. These events are divided into several categories, such as people, property, assets, suppliers, information technology and communications. For each category of hazard risks, the organization needs to evaluate the types of incidents that could occur, the sources of those incidents and their likely impact on normal efficient operations.

Management of hazard risks involves analysis and management of three aspects of the hazard risk. This will be discussed in more detail in a later Part of this book. In summary, the organi-

zation should look at the necessary actions to prevent the loss occurring, limit the damage that the event could cause and contain the cost of recovering from the event.

Hazard management is traditionally the approach adopted by the insurance world. Organizations will have a tolerance of hazard risks. The approach should be based on reducing the likelihood and magnitude/impact of hazard losses. Insurance represents the mechanism for limiting the financial cost of losses.

When an organization considers the level of insurance that it will purchase, the hazard tolerance of the organization needs to be fully analysed. Organizations may be willing to accept a certain cost of motor accidents as a financial cost that will be funded from the day-to-day profit and loss of the organization. This will only be tolerable up to a certain level and the organization will need to determine what level is acceptable. Insurance should then be purchased to cover losses that are likely to exceed that level.

Uncertainty acceptance

When undertaking projects and implementing change, an organization has to accept a level of uncertainty. Uncertainty or control risks are an inevitable part of undertaking a project. A contingency fund to allow for the unexpected will need to be part of a project budget, as well as contingent time built into project schedules. When looking to develop appropriate responses to control risks, the organization must make necessary resources available to identify the controls, implement the controls and respond to the consequences of any control risk materializing.

The nature of control risks and the appropriate responses depend on the level of uncertainty and the nature of the risk. Uncertainty represents a deviation from the required or expected outcome. When an organization is undertaking a project, such as a process enhancement, the project has to be delivered on time, within budget and to specification. Also, the enhancement has to deliver the benefits that were required. Deviation from the anticipated benefits of a project represents uncertainties that can only be accepted within a certain range.

Control management is the basis of the approach to risk management adopted by internal auditors and accountants. The UK Turnbull Report will be mentioned later in this book, and it concentrates on internal control with little reference to risk assessment. Control management is concerned with reducing the uncertainty associated with significant risks and reducing the variability of outcomes.

There are dangers if the organization becomes too concerned with control management. The organization should not become obsessed with control risks, because it is sometimes suggested that over-focus on internal control and control management suppresses the entrepreneurial effort.

Opportunity investment

Some risks are taken deliberately by organizations in order to achieve their mission. These risks are often marketplace or commercial risks that have been taken in the expectation of achieving a positive return. These opportunity risks can otherwise be referred to as commercial, speculative or business risks. Opportunity risks are the type of risk with potential to enhance (although they can also inhibit) the achievement of the mission of the organization. These risks are the ones associated with taking advantage of business opportunities.

All organizations have some appetite for seizing opportunities and are willing to invest in them. There will always be a desire for the organization to have efficient operations, effective processes and efficacious strategy. Opportunity risks are normally associated with the development of new or amended strategies, although opportunities can also arise from enhancing the efficiency of operations and implementing change initiatives.

Every organization will need to decide what appetite it has for seizing new opportunities and the level of investment that is appropriate. For example, an organization may realize that there is a requirement in the market for a new product that its expertise would allow it to develop and supply. However, if the organization does not have the resources to develop the new product, then it may be unable to implement that strategy and it would be unwise for the organization to embark on such a potentially high-risk course of action.

It will be for the management of the company to decide whether they have an appetite for seizing the perceived opportunity. Just because the organization has that appetite, it does not mean that it is the correct thing to do. The board of the company should therefore be aware of the fact that, although they may have an appetite for seizing the opportunity, the organization might not have the risk capacity to support that course of action.

Opportunity management is the approach that seeks to maximize the benefits of taking entrepreneurial risks. Organizations will have an appetite for investing in opportunity risks. There is a clear link between opportunity management and strategic planning. The desire is to maximize the likelihood of a significant positive outcome from investments in business opportunities.

The example below related to personal lifestyle decisions considers risk factors by classifying them as controllable and uncontrollable. Although the example relates to personal health risk factors, consideration of whether business risks are within the control of the organization or not is an important component of successful business risk management.

Heart disease risk factors

Controllable risk factors for heart disease and stroke are those that can be changed through diet, physical activity and no tobacco use. These risk factors are in contrast to those that are uncontrolled, such as age, gender, race or genetic traits. Having one or more uncontrollable risk factors does not mean a person will have a heart attack or stroke; however, with proper attention to those risk factors that are controllable, one may reduce the impact of those risk factors that cannot be controlled or changed.

Controllable risk factors for heart disease or stroke include high blood pressure, high blood cholesterol, type-2 diabetes and obesity. Healthy lifestyle habits, such as developing good eating habits, increasing physical activity and abstaining from tobacco use, are effective steps in both preventing and improving the controllable risk factors.

4

Development of risk management

Origins of risk management

Risk management has a variety of origins and is practised by a wide range of professionals. One of the early developments in risk management was in the United States out of the insurance management function. The practice of risk management became more widespread and better co-ordinated because the cost of insurance in the 1950s had become prohibitive and the extent of coverage limited. Organizations realized that purchasing insurance was insufficient, if there was also inadequate attention to the protection of property and people. Insurance buyers therefore became concerned with the quality of property protection, the standards of health and safety, product liability issues and other risk control concerns.

This combined approach to risk financing and risk control developed in Europe during the 1970s and the concept of total cost of risk became important. As this approach became established, it also became obvious that there were many risks facing organizations that were not insurable. The tools and techniques of risk management were then applied to other disciplines, as discussed later in this chapter.

The maturity of the risk management discipline is now such that the links with insurance are much less strong. Insurance is now seen as one of the risk control techniques, but it is only applicable to a portion of hazard risks. Risks related to finance, commercial, marketplace and reputational issues are recognized as being hugely important, but outside the historical scope of insurance. The range of different approaches to risk management is illustrated by the definitions of risk management as set out in Table 4.1.

Table 4.1 Definitions of risk management

Organization	Definition of risk management
ISO Guide 73 BS 31100	Coordinated activities to direct and control an organization with regard to risk
Institute of Risk Management (IRM)	Process which aims to help organizations understand, evaluate and take action on all their risks with a view to increasing the probability of success and reducing the likelihood of failure
HM Treasury	All the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress
London School of Economics	Selection of those risks a business should take and those which should be avoided or mitigated, followed by action to avoid or reduce risk
Business Continuity Institute	Culture, processes and structures that are put in place to effectively manage potential opportunities and adverse effects

The increasing importance of risk management can be explained by the list of issues set out in Table 4.2. Many of these issues demonstrate that the application of risk management has moved a long way from the origins in the insurance world. Nevertheless, the insurance origins of risk management remain vitally important and are still the part of the approach to hazard management.

This chapter considers the nature of risk management and the established stages that build into the risk management process. Historically, the term risk management has been used to describe an approach that was applied only to hazard risks. The discipline is now developing in a way that will enable risk management to make a contribution to the improved management of control risks and opportunity risks.

Risk management has well-established stages that make up the risk management process, as described in Table 4.3. These stages build into valuable risk management activities, each of which makes an important contribution. There are many ways of representing the risk management process, and each of the standards mentioned later in this part provides a slightly different description.

Table 4.2 Importance of risk management

Managing the Organization

Variable cost or availability of raw materials
Cost of retirement/pension/social benefits
Desire to deliver greater shareholder value
Greater transparency required from organizations
Pace of change in business ever increases
Impact of e-commerce on all aspects of business life
Increased reliance on information technology (IT) systems
Increasing importance of intellectual property (IP)
Greater supply chain complexity/dependency
Reputation becomes more and more important
Reputational damage – especially to worldwide brands
High-profile losses and failures ruin reputations
Regulatory pressures continue to increase
Changes/variation in national legislative requirements
Joint ventures becoming more common

Changes in the Marketplace

Changing commercial and marketplace environment
Globalization of customers, suppliers and products
Increased competition in the marketplace
Greater customer expectations, often led by competitors
Need to respond more rapidly to stakeholder expectations
More volatile markets with less customer loyalty
Diversification leads to working in unfamiliar areas
Constant need to make bold strategic decisions
Short-term success required, without long-term detriment
Product innovation and continuous improvements
Rapid changes in (consumer) product technology
Threats to world/national economy
Threat of influenza or other pandemics
Potential for international organized crime
Increasing occurrences of civil unrest/political risks
Extreme weather events resulting in population shift

Table 4.3 7Rs and 4Ts of (hazard) risk management

1. Recognition or identification of risks and identification of the nature of the risk and the circumstances in which it could materialize.
2. Ranking or evaluation of risks in terms of magnitude and likelihood to produce the 'risk profile' that is recorded in a risk register.
3. Responding to significant risks, including decisions on the appropriate action regarding the following options:
   - tolerate;
   - treat;
   - transfer;
   - terminate.
4. Resourcing controls to ensure that adequate arrangements are made to introduce and sustain necessary control activities.
5. Reaction planning and/or event management. For hazard risks, this will include disaster recovery or business continuity planning.
6. Reporting and monitoring of risk performance, actions and events and communicating on risk issues, via the risk architecture of the organization.
7. Reviewing the risk management system, including internal audit procedures and arrangements for the review and updating of the risk architecture, strategy and protocols.

Figure 4.1 provides a simple diagrammatic representation of the risk management process. This basic explanation of the risk management process is referred to as the 7Rs and 4Ts of hazard risk management. The activities associated with risk management are as follows:

- recognition of risks;
- ranking of risks;
- responding to significant risks;
- resourcing controls;
- reaction (and event) planning;
- reporting of risk performance;
- reviewing the risk management system.

Risk management can improve the management of the core processes of an organization by ensuring that key dependencies are analysed, monitored and reviewed. Risk management tools and techniques will assist with the management of the hazard risks, control risks and opportunity risks that could impact these key dependencies.

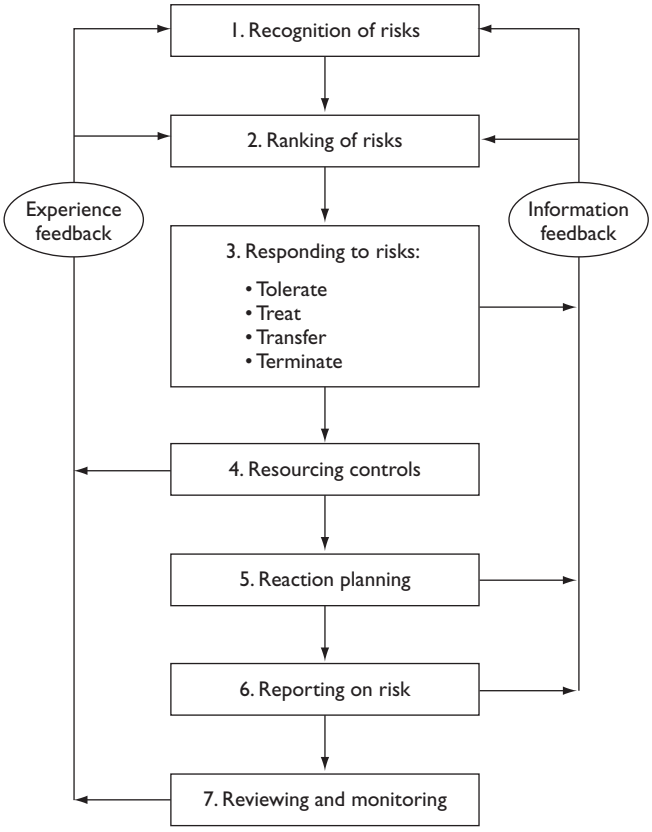


Figure 4.1 7Rs and 4Ts of (hazard) risk management

Insurance origins of risk management

The corporate risk management role in the United States during the 1950s became an extension of insurance purchasing decisions. During the 1960s, contingency planning became more important to organizations. There was also an emphasis beyond risk financing to loss prevention and safety management. During the 1970s, self-insurance and risk retention practices developed within organizations. Captive insurance companies also started to develop. Contingency plans then developed into business continuity planning and disaster recovery plans.

At the same time during the 1960s and 1970s, there were considerable developments in the risk management approach adopted by occupational health and safety practitioners. During the 1980s, the application of risk management techniques to project management developed substantially. Financial institutions continued to develop the application of risk management tools and techniques to market and credit risk during the 1980s. During the 1990s,

the financial institutions further broadened their risk management initiatives to include structured consideration of operational risks.

Also, during the 1980s, treasury departments began to develop the financial approach to risk management. There was recognition by finance directors that insurance risk management and financial risk management policies should be better co-ordinated. During the 1990s, risk financing products emerged that combined insurance with derivatives. At the same time, corporate governance and listing requirements encouraged directors to place greater emphasis on enterprise risk management (ERM) and the first appointment of a chief risk officer (CRO) occurred at that time.

During the 2000s, financial services firms have been encouraged to develop internal risk management systems and capital models. There has been a rapid growth of CRO positions in energy companies, banks and insurance companies. Boards are now investing more time in ERM due to the Sarbanes–Oxley Act of 2002 in the United States. More detailed risk reporting and other corporate governance requirements have also been introduced.

However, the financial crisis of 2008 called into question the contribution that risk management can make to corporate success, especially in financial institutions. There is no doubt that the application of risk management tools and techniques failed to prevent the global financial crisis. This failure was a failure to correctly apply risk management processes and procedures, rather than inherent defects in the risk management approach.

Specialist areas of risk management

Risk management is a constantly developing and evolving discipline. As well as its origins in the insurance industry and in other branches of hazard management, risk management has strong connections with the credit and treasury functions. Additionally, other specialist areas of risk management have developed over the past decades, including:

- project risk management;
- clinical/medical risk management;
- energy risk management;
- operational risk management.

All of the above specialist areas of risk management have contributed considerably to the development and application of risk management tools and techniques. Project risk management is an area where the application of risk management tools and techniques is particularly well developed. As discussed earlier, project risk management has its emphasis on the management of uncertainty or control risks.

Clinical risk management has been developing for some time. This area of risk management is primarily concerned with patient care, especially during surgical operations. The cost of medical malpractice claims and the inevitable delay in making insurance payments has resulted in risk management systems being introduced. Particular aspects of clinical risk management include greater attention to making patients aware of the risks that may be associated with the procedure they are about to undertake.

It is also important that surgeons report incidents that occur during the surgery. Considerable emphasis has been placed in clinical risk management on the need to report, in an accurate and timely manner, details of any incidents that occur in the operating theatre. There are many publications available on clinical risk management, and a great deal of work has been put into establishing the necessary systems and procedures to cover this specialist area of risk management.

As well as project and clinical risk management, risk management tools and techniques have also been applied in a range of specialist industries. In particular, risk management techniques have been applied in the finance and energy sectors. Risk management in the finance sector focuses on operational risks, as well as market, credit and other types of financial risks. It is in the finance sector that the title Chief Risk Officer was first developed.

The energy sector has also seen an increase in the attention paid to risk management tools and techniques. For some organizations in the energy sector, risk management is mainly concerned with the future price of energy and with exploration risk. Therefore, the risk management approach is similar to the activities of the treasury function, where hedging and other sophisticated financial techniques form the basis of the risk management effort.

Enterprise risk management

Another area where the risk management discipline has developed in recent times is the approach that is referred to as enterprise or enterprise-wide risk management (ERM). This approach to risk management will be discussed in more detail in a later Part. The main feature that distinguishes ERM from what might be considered more traditional risk management is the more integrated or holistic approach that is taken in ERM. In many ways, it can be considered to be a unifying philosophy that draws together management of all types of risks, rather than a new or different approach.

A good example of the ERM approach is the pharmaceutical industry. If a person is reliant on a particular medication, then it is vitally important that the medication is constantly available. From the point of view of the pharmaceutical company, this means that a core process for the organization must be the 'constant availability of medication' process.

If the pharmaceutical company takes this approach, it will look at the risks that could affect this core process or stakeholder expectation on an enterprise-wide basis. This will involve analysis of the supply chain, evaluation of manufacturing activities and analysis of the delivery arrangements. The overall question that needs to be answered is what could prevent the continuous supply of medication. Risks to the continuous supply will include unavailability of ingredients, disruption to manufacturing activities, contamination of the product, breakdown in supply transportation arrangements and disruption to distribution.

This enterprise-wide approach has considerable advantages, because it analyses the potential for disruption to the overall stakeholder expectation. Health and safety, for example, is then viewed as a component in ensuring that staff are always available so that the overall process will not be disrupted, rather than (or perhaps as well as) a separate hazard management issue.

Levels of risk management sophistication

This chapter describes the different styles of risk management that are currently practised. More professions and disciplines are now involved in risk management than in previous years. This adds diversity to the development of the risk management discipline.

At first, an organization may be aware of a new risk and the need to take appropriate action. In that case, there will be a need for the organization to *reform* in response to the hazard risk. As the organization responds to the risk, it will seek to *conform* with the appropriate risk control standards. After this stage, the organization may realize that there are benefits to be obtained from the risk. The organization will then have the ability to *perform* and view the risk as an opportunity risk, as illustrated in Figure 4.2.

As a simple example, a publisher might realize that it was not fully complying with equal opportunities legislation, because there was no ethnic minority representation within the workforce. The company will identify the actions necessary in order to reform its procedures, so that it complies with legal requirements.

Having achieved compliance, the publisher should become aware that a significant proportion of the workforce comes from ethnically diverse backgrounds. The company should see this diversity in its workforce as a benefit that will enable it to perform better in the marketplace by exploring opportunities to produce and publish new magazines that appeal to a more ethnically diverse readership.

The stages of reform to conform to perform represent levels of risk management sophistication. However, it is not necessary for a risk or the practice of risk management to progress from hazard to control to opportunity. In fact, risks can regress in certain circumstances. At any one time, a particular risk will be of a specific type in an organization. Benefits can be

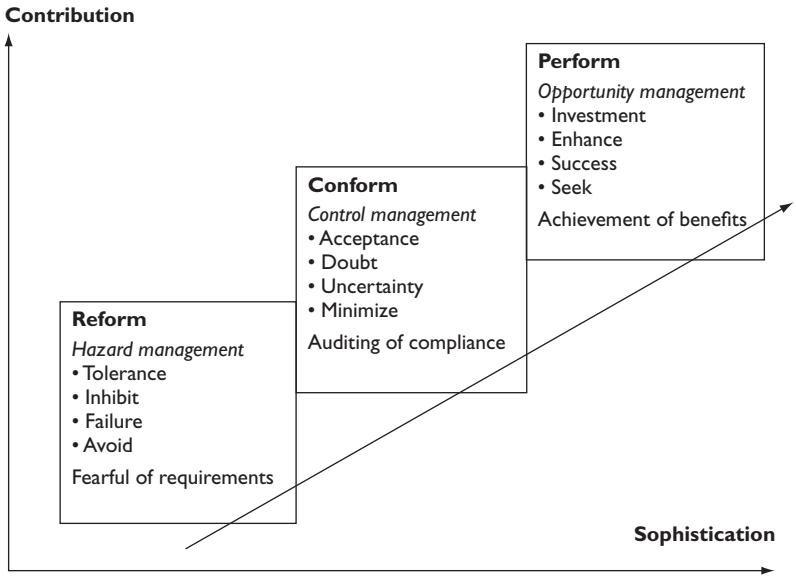


Figure 4.2 Risk management sophistication

obtained from the successful management of that risk at whatever level of sophistication is appropriate at the time. In summary, risk management need only be as sophisticated as the organization requires in order to bring benefits.

Although the three levels of risk management sophistication illustrated in Figure 4.2 represent an improved approach to risk management, there is a danger that organizations will become obsessed with risk management to the point that important decisions are not taken. At this point, it may be said that too much attention and concern about risk and risk management will cause the organization to *deform* its operations. In summary:

- awareness of non-compliance – REFORM;
- actions to ensure compliance – CONFORM;
- achieve business opportunities – PERFORM;
- inactivity caused by obsession – DEFORM.

As the level of sophistication increases and risk management professionals become aware of the alternative approaches to risk management, they should value the contribution that can be made by other approaches. The development in risk management approach can be summarized as follows:

- Hazard management specialists may find that there has been a trend towards a desire to retain more insurable risks (and buy less insurance) as a result of a more holistic approach to risk management.

- Control management specialists must not squeeze entrepreneurial spirit and effort out of the organization.
- Strategic planners must recognize that risk management tools and techniques can contribute to better strategic decisions and the successful exploitation of business opportunities.

Risk maturity models

Increases in risk management effectiveness can also be measured by the use of risk maturity models. The level of risk management sophistication provides an indication of the benefits that can be achieved from risk management. The level of risk maturity in the organization is a measure of the quality of risk management activities and the extent to which they are embedded within the organization.

Risk maturity models can be used to measure the current level of risk culture within the organization. The greater the level of risk maturity, the more embedded risk management activities will become within the routine operations undertaken by the organization. The hallmarks of successfully embedded risk management are considered in a later chapter.

Risk maturity models will also be considered in more detail in a later chapter. Risk maturity is not the same as considering the level of sophistication that an organization achieves in respect to risk management. An organization may have limited expectations of risk management, but nevertheless have a very mature approach to the way in which it seeks to obtain the available benefits.

The level of risk maturity within an organization is an indication of the way in which risk processes and capabilities are developed and applied. In an immature organization, informal risk management practices will take place. However, there is likely to be a blame culture in existence when things go wrong and a potential lack of accountability for risk. Also, resources allocated to manage risks may be inappropriate for the level of risk involved.

When explicit risk management is in place, there will be attempts to keep the processes dynamic, relevant and useful. There is likely to be open dialogue and learning so that information is used to inform judgements and decisions about risks. There will be confidence that innovation and risk taking can be managed, with support when things go wrong.

When an organization becomes obsessed with risk, there will be over-dependence on process and this may limit the ability to manage risk effectively. There will be over-reliance on information at the expense of good judgement, and dependence on process to define the rationale behind decisions. Individuals may become risk averse for fear of criticism and procedures are followed only to comply with requirements, not because benefits are sought.

5
Principles and aims of risk management

Principles of risk management

Risk management operates on a set of principles, and there have been several attempts to define these principles. British Standard BS 31100 sets out 11 risk management principles and the international standard ISO 31000 also includes a detailed list of the suggested principles of risk management. The following list is a consolidated version of these documents. It is suggested that a successful risk management initiative will be:

- Proportionate to the level of risk within the organization;
- Aligned with other business activities;
- Comprehensive, systematic and structured;
- Embedded within business processes;
- Dynamic, iterative and responsive to change.

This provides the acronym PACED and provides a very good set of principles that are the foundations of a successful approach to risk management within any organization. A more detailed description of the PACED principles of risk management is set out in Table 5.1. The approach to risk management is based on the idea that risk is something that can be identified and controlled.

The above statement of principles relates to the essential features of risk management. These principles describe what risk management should be in practice. Some lists of principles also include information on what risk management should do or deliver. It is useful to separate the principles of risk management into two separate lists: what risk management should be, as listed above; and what it should deliver, as listed below:

- Compliance with laws and regulations;
- Assurance regarding the management of significant risks;

Table 5.1 Principles of risk management

Principle	Description
Proportionate	Risk management activities must be proportionate to the level of risk faced by the organization.
Aligned	Risk management activities need to be aligned with the other activities in the organization.
Comprehensive	In order to be fully effective, the risk management approach must be comprehensive.
Embedded	Risk management activities need to be embedded within the organization.
Dynamic	Risk management activities must be dynamic and responsive to emerging and changing risks.

- Decisions that pay full regard to risk considerations;
- Efficiency, Effectiveness and Efficacy in operations, projects and strategy.

This provides the acronym CADE3 and confirms that outputs from risk management will lead to less disruption to normal efficient operations, reduction of uncertainty in relation to change and improved decisions in relation to evaluation and selection of alternative strategies. In other words, a key part of risk management is improved organizational decision making.

The resources available for managing risk are finite and so the aim is to achieve an optimum response to risk, prioritized in accordance with an evaluation of the risks. Risk is unavoidable and every organization needs to take action to manage it in a way that it can justify to a level that is acceptable. The appropriate range of responses to a risk will depend on the nature, size and complexity of the risk.

Importance of risk management

Table 4.2 gives a number of examples that illustrate the importance of risk management. Risk management has become increasingly high profile in recent times, because of the global financial crisis and the number of high profile corporate failures across the world that preceded it. Also, risk management has become more important because of increasing stakeholder expectations and the ever-increasing ease of communication.

As well as assisting with better decision making and improved efficiency, risk management can also contribute to the provision of greater assurance to stakeholders. This assurance has two important components. The directors of any organization need to be confident that risks have

been identified and that appropriate steps have been taken to manage risk to an appropriate level.

Also, there is greater emphasis on accurate reporting of information by organizations, including risk information. Stakeholders require detailed information on company performance, including risk awareness. The Sarbanes–Oxley Act of 2002 (SOX) in the United States has accuracy of financial reporting as its main requirement. SOX brings the issue of the accurate reporting of results to a higher priority (section 404), whilst also requiring full and accurate disclosure of all information about the organization (section 302).

Although Sarbanes–Oxley is a specific piece of legislation that only applies in certain circumstances, the principles that it contains are vitally important to all risk management practitioners. Accordingly, later parts of this book consider risk assurance and accurate reporting as integral parts of the overall risk management process.

Risk management activities

Risk management is a process that can be divided into several stages. The IRM Risk Management Standard provides one representation of the stages involved in the risk management process. Alternative illustrations of the risk management process can be found in the British Standard BS 31100, the International Standard ISO 31000 and in other publications. These standards will be considered in more detail in Chapter 6.

Figure 4.1 (page 40) illustrates the stages in the (hazard) risk management process. The terminology that is used to describe the stages in the risk management process has been deliberately selected, so that the process can be represented as the 7Rs and 4Ts of hazard risk management. Table 4.3 provides more information on each of the stages illustrated in Figure 4.1.

ISO Guide 73 and British Standard BS 31100 describe the risk management process as the systematic application of management policies, procedures and practices to the tasks of communicating, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk. However, it could be argued that the setting of policies, procedures and practices, together with the tasks of communicating, consulting and establishing that context are actually part of the risk management framework, rather than the risk management process itself.

Within this book, the risk management process is taken as a narrow set of activities, described above as identifying, analysing, evaluating, treating, monitoring and reviewing risk. This provides a clear distinction between the risk management process and the framework that supports this process. Descriptions of the risk management process together with the risk management framework are required in order to produce a comprehensive risk management standard.

There has been much discussion about whether a single risk management process and/or diagram can be used to describe the management of hazard risks, control risks and opportunity risks. This book uses different terminology to describe the three types of risks and, therefore, Figure 4.1 and Table 4.3 are used to illustrate the stages in the hazard risk management process only.

There are a number of options when responding to hazard risks. These are often represented as the 4Ts of hazard risk management, and these risk response options will be considered in more detail in a later part of this book. In summary, the options for responding to hazard risks are:

- tolerate;
- treat;
- transfer;
- terminate.

Efficient, effective and efficacious

Insurable or hazard risks can have an immediate impact on operations. Therefore, the initial application of risk management principles was to ensure continuation of normal efficient operations.

As risk management has developed, emphasis has been placed on project management and the delivery of programmes to provide enhancements to business processes. Processes must be effective in that they deliver the results that are required. For example, there is limited value in having a software program that is efficient if it does not deliver the range of functions that are required.

Strategic decisions are the most important that an organization has to make. Risk management delivers improved information so that strategic decisions can be made with greater confidence. The strategy that is decided by an organization must be capable of delivering the results that are required. Such a strategy may be described as efficacious. There are many examples of organizations that selected an incorrect strategy or failed to successfully implement the selected strategy. Many of these organizations suffered corporate failure.

Strategy should be designed to take advantage of opportunities. For example, a sports club may identify the possibility of selling more products to its existing customer base. Some clubs will establish a travel agency for fans of the club who travel overseas, together with the provision of associated travel insurance. Also, there is the possibility of creating a club credit card that will be managed by a new finance subsidiary.

Having identified these possibilities, the club will need to look at the risks associated with these potential opportunity investments and devise a suitable programme of projects to implement the selected strategies. Ensuring that adequate account is taken of risk during all of these activities will increase the chances of selecting the correct efficacious strategy, designing the appropriate effective processes and, ultimately, ensuring efficient and profitable operations.

Organizations that have efficient operations and effective processes but an incorrect overall strategy will fail. This will be the case, however good the risk management processes are at operational and project level. Incorrect strategy has resulted in more corporate failures than inefficient operations or ineffective processes.

Perspectives of risk management

In a rapidly developing discipline like risk management, there is scope for different practitioners to become intolerant towards the approach adopted by others. Internal control specialists who believe that risk management is all about the management of uncertainty and the achievement of corporate objectives should not become intolerant of the more traditional insurance risk management approach. There is no value in one group of specialists being dismissive of the approach adopted by others and being unwilling to utilize the expertise that is available in another group.

In any case, there is no single style of risk management or approach to risk management that offers all the answers. Clearly, the various styles that can be adopted should operate as complementary approaches within an organization. The integrative approach to risk management accepts that the organization must tolerate certain hazard risks and must have an appropriate appetite for investment in opportunity risks. Risk management tools and techniques should be brought to achieve the following:

- Hazard management makes outcomes less negative.
- Control management reduces the spread of possible outcomes.
- Opportunity management makes outcomes more positive.

Hazard management will make the outcome of any hazard event less negative. Within the context of hazard management, insurance represents the mechanism for restricting the financial cost of losses when a risk materializes. Risk control and loss management techniques will reduce the expected losses and should ensure that the overall cost is contained. The combination of insurance and risk control/loss management will reduce the actual cost of hazard losses and this will inevitably (and correctly) cause the hazard tolerance of the organization to reduce. More of the risk capacity of the organization will then be available for opportunity investment.

Control management reduces the range of possible outcomes from any event. Control management is based on the established techniques of internal financial control, as practised by internal auditors. The main intention is to reduce losses associated with inadequate control management at the same time as reducing the range of possible outcomes. This is the contribution that internal control should make to the overall approach to risk management within an organization.

Opportunity management seeks to make positive outcomes more likely and more substantial. As part of the opportunity management approach, the organization should also look at possibilities for increasing the revenue from the product or service. In not-for-profit organizations, opportunity management should facilitate the delivery of better value for money.

These reward enhancement options can be discussed at strategy meetings and some options may be adopted, including the introduction of bonus and incentive schemes for staff and management. Clearly, in light of the lessons learnt from the global financial crisis, these incentive schemes should be balanced and should not reward excessive risk taking.

Implementing risk management

This chapter has considered the principles of risk management that describe what risk management should be and what it should deliver. Although organizations may realize that there are benefits from implementing risk management, the successful implementation has to be undertaken as an initiative or project. Appendix B sets out a detailed consideration of the stages involved in the successful implementation of an enterprise-wide risk management initiative.

There will be a more detailed consideration of the barriers and enablers for implementation of risk management in a later Part. The most important point to make is that the support of senior management and (ideally) the sponsorship of a board member is essential. Also, an implementation plan to address the concerns of employees and other stakeholders is needed. Although risk management is vital to the success of an organization, many managers may need to be persuaded that the suggested implementation approach is correct.

It is important to note that all activities and functions undertaken by managers should not be claimed by the risk manager as being undertaken in the name of risk management. Not all activities in the organization will be driven by risk management, even if all decisions, processes and activities have risks embedded within them.

6
Risk management standards

Scope of risk management standards

There are a number of established risk management standards and frameworks. The first such standard was developed by the standards body in Australia in 1995, which has been followed by those being developed in Canada, Japan, the UK and the United States. Standards have also been developed by other national standards bodies, as well as by government departments across the world.

The overall approach of each of these standards is similar. The standard that had the widest recognition was the Australian Standard AS 4360 (2004). AS 4360 was withdrawn in 2009 in favour of ISO 31000. The ERM version of the COSO standard is also widely applied in many organizations. British Standard BS 31100:2008 'Risk management – Code of practice' was published in October 2008.

The latest addition to the available standards is the international standard ISO 31000:2009 'Risk management – Principles and guidelines', which was published in the latter part of 2009. Although some standards are better recognized than others, organizations should select the approach that is most relevant to their particular circumstances.

It is important to distinguish between a risk management standard and a risk management framework. A risk management standard sets out the overall approach to the successful management of risk, including a description of the risk management process, together with the suggested framework that supports that process.

In simple terms, a risk management standard is the combination of a description of the risk management process, together with the recommended framework. The key features of a risk management framework are described later. Table 6.1 provides a summary of the most widely used risk management standards and frameworks.

Table 6.1 Risk management standards

Standard	Description	Reference
ISO 31000	Standard published by the International Standards Organization (2009)	Figure 6.5
British Standard BS 31100	Standard published by British Standards Institution (2008)	Figure 6.4
Institute of Risk Management (IRM)	Standard produced jointly by AIRMIC, Alarm and the IRM (2002).	Figure 6.1
COSO ERM	Framework produced by the Committee of Sponsoring Organizations of the Treadway Committee (2004)	Figure 6.3
Turnbull Report	Framework produced by the Financial Reporting Council (2005)	Chapter 6
Orange Book	Standard produced by HM Treasury of the UK Government (2004)	Chapter 6
CoCo (Criteria of Control)	Framework produced by the Canadian Institute of Chartered Accountants (1995)	Figure 31.1

One of the best-established and most widely used risk management standards was produced by the IRM in 2002 in co-operation with AIRMIC and Alarm. The IRM Standard is a high level approach aimed at non-risk-management specialists and it has been translated into many languages. The Australian Standard and the COSO standard/framework are designed for use primarily by specialist risk management practitioners. The IRM Standard is available as a free download from the IRM website, and the risk management process used in it is reproduced in Figure 6.1.

For organizations that are listed on the New York stock exchange, the approach outlined in the COSO Internal Control framework (1992) is recognized by the Sarbanes–Oxley Act of 2002 (SOX). The requirements of SOX also apply to subsidiaries of US-listed companies around the world. Therefore, the COSO approach is internationally recognized and, in many circumstances, mandated. It is worth noting that SOX requires the approach described in the COSO Internal Control framework (1992). This is not the same as the COSO ERM framework (2004) described later, although the COSO ERM framework does contain all of the elements of the earlier Internal Control version.

The COSO Internal Control framework has become the most widely used internal control framework in the United States and it has been adapted and/or adopted by numerous countries and businesses around the world. An enterprise risk management (ERM) version of the

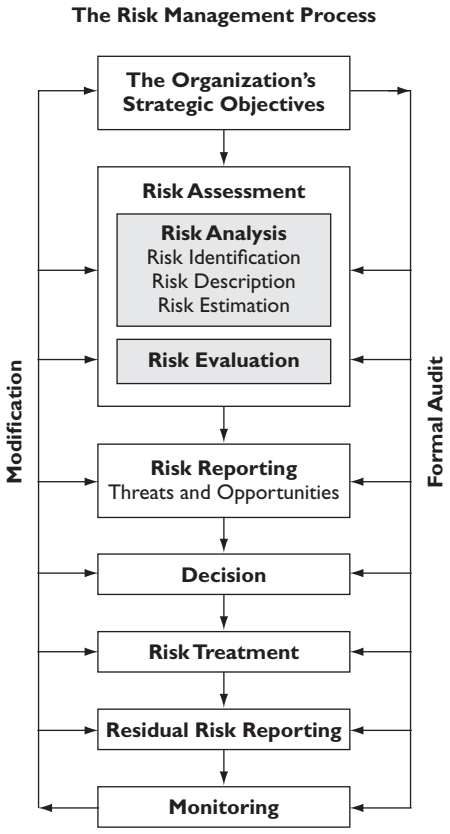


Figure 6.1 IRM risk management process
IRM/AIRMIC/ALRAM 2002

COSO framework was produced in 2004 and this has both risk management and internal control within scope.

Apart from the British, ISO and COSO standards, a number of others are also well regarded and in widespread use. The UK's Turnbull guidance was updated in 2005 and is considered by the Securities and Exchange Commission (SEC) in the United States to be an acceptable alternative to the COSO Internal Control framework for Sarbanes–Oxley compliance. The updated Turnbull guidance can be found as a free download from the website of the Financial Reporting Council.

As well as the established standards and frameworks, a considerable amount of guidance on risk management has been published by various government departments. HM Treasury in the UK has published the highly respected 'Orange Book', which contains a significant amount of useful information on risk management tools and techniques. Many of the ideas and concepts presented in the Orange Book are referenced throughout this volume.

Some of the available standards were developed by risk management professionals, whilst others were developed by accountants or auditors. There are three distinct approaches followed in the various standards:

- 'risk management' approach followed by ISO 31000, British Standard BS 31100 and the IRM Standard;
- 'internal control' approach developed by COSO Internal Control framework and by the Turnbull Report;
- 'risk-aware culture' approach developed by the Canadian Institute of Chartered Accountants, known as the CoCo framework.

Risk management process

A simple representation of the risk management process is provided by Figure 4.1 (page 40) and a similar process is contained in all of the established risk management standards. Many of the standards distinguish between the risk management process and the framework that supports the process. However, this distinction is not always clear in many of the established risk management standards/frameworks.

The best-established risk management approaches are the IRM Standard, ISO 31000, BS 31100, and the COSO ERM framework. All four provide a description of a risk management framework, but more emphasis is placed on the risk management process in the IRM Standard, ISO 31000 and BS 31100. The COSO approach does not provide the same clear distinction between the framework and the risk management process itself and is mainly concerned with framework considerations.

Several countries have developed their own internal control and risk management standards as part of their requirements for being listed on a stock exchange. Typically, these are frameworks similar to COSO Internal Control in approach, and this is certainly the case with the Turnbull requirements that exist in the UK.

Although there are many ways of representing the risk management process, the basic steps are all similar. There can be difficulties with the terminology that is used to describe the various steps, and Appendix A provides definitions of basic terms, as well as cross-referencing the different terminologies that can be used.

Risk management framework

There are many risk management standards and risk management frameworks that have been produced by various organizations. It is generally acknowledged that a standard is a document

that produces information on both the risk management process and the risk management framework.

Within many risk management standards, risk management activities should take place within the context of the business environment, the organization and the risks faced by the organization. In order for the context to be described and defined, a framework is required to support the process. ISO 31000 places particular emphasis on context and states that consideration should be given to the internal context, external context and risk management context when undertaking risk management activities.

All of the established risk management standards refer to the risk management framework, although this is represented in different ways. In order to provide a simple explanation of the scope of the risk management framework, the acronym Risk Architecture, Structure and Protocols (RASP) has been developed. Figure 6.2 illustrates the key features of a risk management framework that is built around and supports the risk management process.

Part 2 of this book describes the risk architecture, strategy and protocols (RASP) in more detail. It is the risk architecture strategy and protocols that define the framework within which the risk management process takes place. These three components of architecture, strategy and protocols are required for successful risk management activities. There needs to be a clear understanding of the risk management process, followed by a clear definition of the framework that supports the process. Also, the risk-aware culture within the organization needs to be strong.

In supporting the risk management process, the risk management framework needs to facilitate communication and the flow of risk information. Because the framework is a supportive structure, it is shown in Figure 6.2 as a series of components built around and supporting the risk management process.

For example, an organization might decide to follow the structure of the IRM Risk Management Standard. The company would then have to set up a framework that includes the

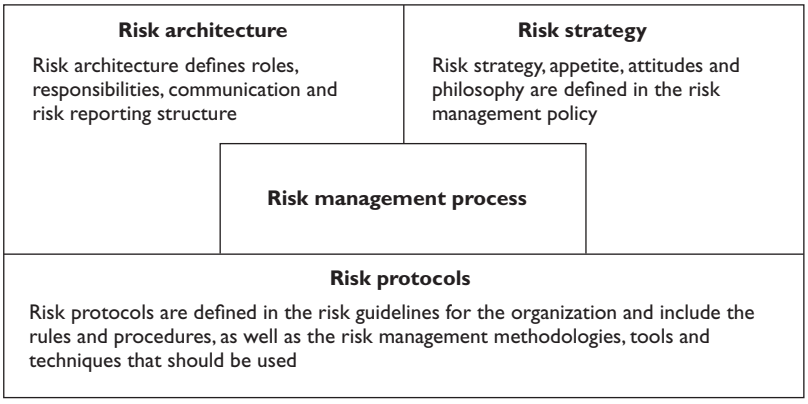


Figure 6.2 Components of an RM framework

structure, responsibilities, administration, reporting and communication components of risk management. All of these procedures will then be recorded in a risk management policy.

COSO ERM cube

An Enterprise Risk Management (ERM) version of the COSO framework was produced in 2004 and this has both risk management and internal control within scope. Details of the COSO ERM framework are provided on the COSO website and there is a free download of the executive summary of COSO ERM. The COSO ERM approach suggests that enterprise risk management is not strictly a serial process, where one component affects only the next. It is considered to be a multidirectional, iterative process in which almost any component can and does influence all other components.

In the COSO ERM framework, there is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them. The relationship is depicted in a three-dimensional matrix, in the form of a cube, which is reproduced as Figure 6.3.

The COSO ERM cube is a very influential risk management framework and it consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process. A brief description of the COSO ERM components is set out in Table 6.2.

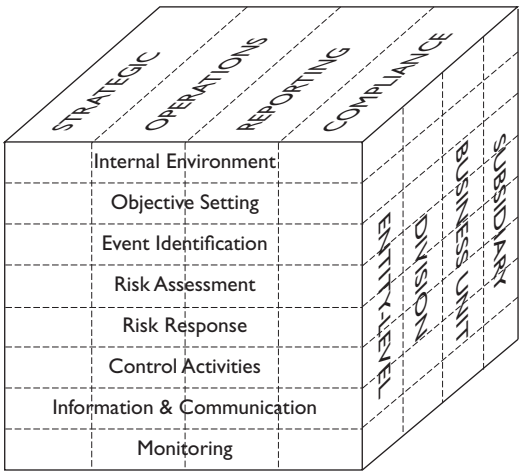


Figure 6.3 COSO ERM framework
COSO's ERM 'Cube Diagram'

Table 6.2 COSO ERM framework

- Internal environment – The internal environment encompasses the tone of an organization and sets the basis for how risk is viewed and addressed.
- Objective setting – Objectives must exist before management can identify potential events affecting their achievement.
- Event identification – Internal and external events affecting achievement of objectives must be identified, distinguishing between risks and opportunities.
- Risk assessment – Risks are analysed, considering likelihood and impact, as a basis for determining how they should be managed.
- Risk response – Management selects risk responses – avoiding, accepting, reducing, or sharing risk.
- Control activities – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- Information and communication – Relevant information is identified, captured, and communicated so that people can fulfil their responsibilities.
- Monitoring – The entirety of enterprise risk management is monitored and modifications made as necessary.

COSO ERM describes the framework by stating: 'within the context of the established mission or vision of an organization, management establishes strategic objectives, selects strategy and sets aligned objectives cascading through the enterprise.' This enterprise risk management framework is geared to achieving corporate objectives, set out in four risk categories:

- Strategic: high-level goals, aligned with and supporting its mission.
- Operations: effective and efficient use of its resources.
- Reporting: reliability of reporting.
- Compliance: compliance with applicable laws and regulations.

Features of RM standards

The main risk management standards that have been developed are the IRM Standard, ISO 31000, British Standard BS 31100 and the COSO ERM framework.

British Standard BS 31100:2008, entitled 'Risk Management – Code of Practice', was published in October 2008. It emphasizes the requirement for a risk management framework to support the separately described risk management process. In particular, British Standard BS 31100 states that the risk management process should provide a systematic, effective and efficient way by which risks can be managed at different levels throughout the organization.

The risk management framework is described in the British Standard in some detail. In fact, most of the standard is made up of a description of the risk management framework, together with a detailed part on how to develop risk management activities. The risk management framework is set out in Figure 6.4. It is a continuous cycle of review and improvement. BS 31100 also proposes a version of the risk management process and this is also presented as a continuous cycle of activities represented by the following five stages:

- identify;
- assess;
- respond;
- report;
- review.

British Standard BS 31100 describes the risk management framework as a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organization. The foundations include the objectives, a mandate and commitment to managing risk (strategy); the organizational arrangements include plans, relationships, accountabilities, resources, processes and activities (architecture). The risk management framework is embedded within the organization's overall strategic and operational policies and practices (protocols).

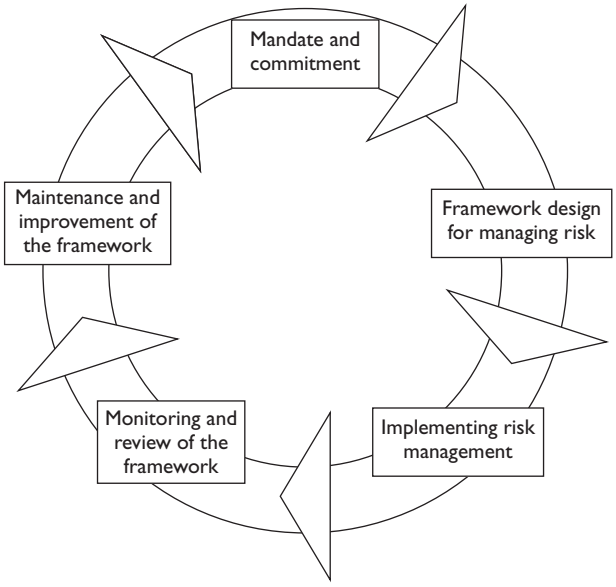


Figure 6.4 Risk management framework from BS 31100

BS 31100 also seeks to address the upside of risk by presenting the response 'seek risk' as one of the risk response options. The British Standard explains that 'risks with desirable potential consequences can make an activity more attractive and lead an organization to seek that activity, just as risks with undesirable potential consequences can motivate avoidance.' The British Standard goes on to add that 'there are more potential opportunities than is sometimes appreciated, but appropriate focus, procedures and language can allow them to be identified and included in decision-making.'

The International Standards Organization (ISO) published ISO 31000 entitled 'Risk management – Principles and guidelines' in the latter part of 2009. The diagram used to illustrate the risk management process in ISO 31000 is reproduced in Figure 6.5. It could be argued that Figure 6.5 contains elements of the risk management framework, as well as the key stages of the risk management process.

In addition to developing ISO 31000 and the guide to risk management terminology 'Guide 73', work is also being undertaken on the production of a Final Draft International Standard (FDIS) on risk assessment techniques. FDIS 31010 'Risk Management – Risk Assessment Techniques' reflects current good practices in the selection and utilization of risk assessment techniques.

Standards institutions around the world have a requirement for routine review of standards every four years. Therefore, the existing standards, as well as those additional standards that are being developed, will be subject to review on a regular basis. This will ensure that the advice and guidance given in the various standards will remain up to date and in line with current practice.

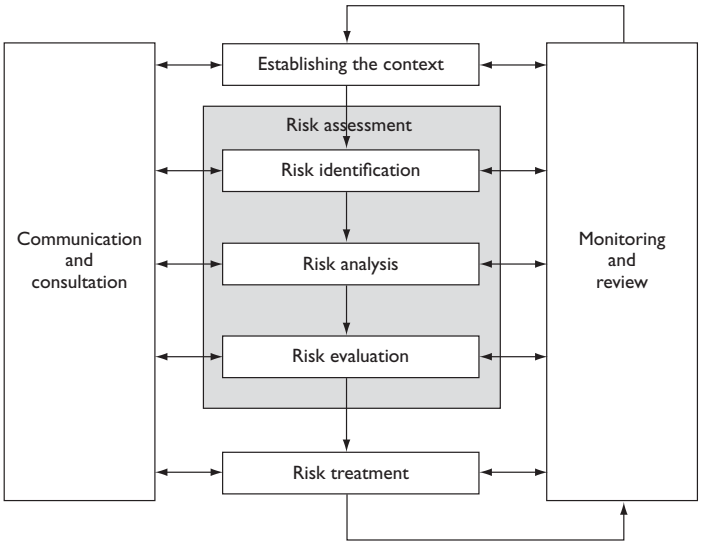


Figure 6.5 Risk management process from ISO 31000

This figure taken from draft standard ISO/FDIS 31000:2009 Risk Management – Principles and Guidelines, is reproduced with the permission of the International Organization for Standardization, ISO. This draft standard can be obtained from any ISO member and from the website of the ISO Central Secretariat at the following address: www.iso.org. Copyright remains with the ISO.

In addition to risk management standards, there are also a number of internal control standards in existence. These internal control frameworks have a different emphasis and are outside the scope of this book, with the exception of the Criteria of Control (CoCo) framework produced by the Canadian Institute of Chartered Accountants. The approach in the CoCo standard is considered briefly below and evaluated in more detail in the final part of this book. The approach in CoCo is based on the evaluation of the culture or the internal control environment of the organization.

Control environment approach

The approach adopted by the Canadian Criteria of Control (CoCo) framework produced by the Canadian Institute of Chartered Accountants is based on the idea that the risk culture of the organization is the most important consideration. If the risk culture is correct, then the successful management of risks should follow. The CoCo framework states that:

> *A person performs a task, guided by an understanding of its purpose (the objective to be achieved) and supported by capability (information, resources, supplies and skills). The person will need a sense of commitment to perform the task well over time. The person will monitor his or her performance and the external environment to learn about how to do the task better and about changes to be made. The same is true of any team or work group. In any organization of people, the essence of control is purpose, commitment, capability and monitoring and learning.*

The COSO ERM framework refers to the control environment as the internal environment. This can be considered to be equivalent to the control environment that is considered in the CoCo framework. CoCo provides a structured means of analysing the control environment that enables a quantitative assessment of the control environment, so that the features for improvements can be identified.

The CoCo framework is considered in more detail in Part 6 of this book. Although there are different versions of the CoCo questions, the following are the headings that are normally used in order to evaluate the risk-aware culture within an organization using a CoCo approach:

- purpose, vision and mission;
- commitment to integrity and ethical values;
- capability, authority and responsibilities;
- learning and development of competence.

Case study

Barclays Bank – risk management objectives

Barclays' approach to risk management involves a number of fundamental elements that drive our processes across the Group:

The Principle Risks Policy covers the Group's main risk types, assigning responsibility for the management of specific risks, and setting out the requirements for control frameworks for all of the risk types. The individual control frameworks are reinforced by a robust system of review and challenge and a governance process of aggregation and broad review by businesses and risk across the Group.

The Group's Risk Appetite sets out the level of risk that the Board is willing to take in pursuit of its business objectives. This is expressed as the Group's appetite for earnings volatility across all businesses from credit, market, and operational risk. It is calibrated against our broad financial targets, including income and impairment targets, dividend coverage and capital levels. It is prepared each year as part of the Group's Medium-Term Planning process, and combines a top-down view of the Group's risk capacity with a bottom-up view of the risk profile requested and recommended by each business.

Barclays Risk methodologies include systems that enable the Group to measure, aggregate and report risk for internal and regulatory purposes. As an example, our credit grading models produce Internal Ratings through internally derived estimates of default probabilities. These measurements are used by management in an extensive range of decisions, from credit grading, pricing and approval to portfolio management, economic capital allocation and capital adequacy processes.

Risk management is a fundamental part of business activity and an essential component of its planning process. To keep risk management at the centre of the executive agenda, it is embedded in the everyday management of the business.

Barclays ensures that it has the functional capacity to manage the risk in new and existing businesses. At a strategic level, our risk management objectives are:

- To identify the Group's material risks and ensure that business profile and plans are consistent with risk appetite.
- To optimise risk/return decisions by taking them as closely as possible to the business, while establishing strong and independent review and challenge structures.
- To ensure that business growth plans are properly supported by effective risk infrastructure.
- To manage risk profile to ensure that specific financial deliverables remain possible under a range of adverse business conditions.
- To help executives improve the control and co-ordination of risk taking across the business.

Annual Report and Review 2008

Part 2

Risk strategy

Learning outcomes for Part 2

- list the main parts of a risk management policy and describe the importance of each part;
- explain the key components of the risk architecture, strategy and protocols (RASP) for an organization and how these fit together;
- outline the range of risk documentation and records that could be required and describe the function of each different type;
- describe the nature, contents and use of a risk register and provide examples of the use of risk registers;
- outline the key roles and responsibilities for risk management in relation to job roles and key departments, including the role of CRO;
- describe a suitable risk architecture for a range of organizations, including the importance of risk committees and risk communication;
- describe the key features of a risk-aware culture (LILAC) and how the key components can be measured;

- describe the components of evaluating risk maturity of an organization (4Ns) and the benefits associated with greater risk maturity;
- outline the importance of risk training and risk communication, including the use of risk management information systems (RMIS).

Part 2 Further reading

British Standard BS 31100 (2008) Risk management – Code of practice, www.standardsuk.com.
Health and Safety Executive (2005) A review of safety culture and safety climate literature for the development of the safety culture, inspection toolkit Research Report 367, www.hse.gov.uk.
Institute of Risk Management A Risk Management Standard (2002), www.theirm.org.

7
Risk management policy

Risk architecture, strategy and protocols

This part provides information on the risk architecture, strategy and protocols (RASP) for an organization. The most important component of the RASP is the risk management policy. The RM policy will set out the overall strategy of the organization towards risk management, define risk management roles and responsibilities and set out the protocols that should be followed. Table 7.1 sets out key features of the risk architecture, strategy and protocols in more detail.

The risk architecture, strategy and protocols create the risk framework that supports the risk management process. British Standard BS 31100 provides notes on the risk management framework that state that it should include the objectives, mandate and commitment to manage risk (strategy), and the organizational arrangements that include plans, relationships, accountabilities, resources, processes and activities (architecture), and that the framework should be embedded within the organization's overall strategic and operational policies and practices (protocols).

Most large organizations will document their risk protocols as a set of risk management guidelines. The range of guidelines that are required will vary according to the size and complexity of the organization. The types of documentation that will need to be kept are as follows:

- risk management administration records;
- risk response and improvement plans;
- event reports and recommendations;
- risk performance and monitoring reports.

One of the standard documents produced by organizations as part of their risk management initiatives is the risk register. Risk registers can be produced for a variety of operational, project and strategic purposes. The likely format of the risk register is discussed in Chapter 8 and the basic format is illustrated in Table 8.1.

Table 7.1 Risk management framework

Risk management architecture
- Committee structure and terms of reference
- Roles and responsibilities
- Internal reporting requirements
- External reporting controls
- Risk management assurance arrangements

Risk management strategy
- Risk management philosophy
- Arrangements for embedding risk management
- Risk appetite and attitude to risk
- Benchmark tests for significance
- Specific risk statements/policies
- Risk assessment techniques
- Risk priorities for the present year

Risk management protocols
- Tools and techniques
- Risk classification system
- Risk assessment procedures
- Risk control rules and procedures
- Responding to incidents, issues and events
- Documentation and record keeping
- Training and communications
- Audit procedures and protocols
- Reporting/disclosures/certification

The working relationship between risk management and internal audit is critically important. Risk management expertise rests in the assessment of risk and the identification of existing and additional controls. Internal audit has its expertise in the evaluation of controls and the testing of their efficiency and effectiveness. Successful implementation of a risk management initiative will require close co-operation and understanding between risk management and internal audit. The RASP should set out the details of how this close co-operation will be achieved in practice.

The risk architecture defines how information on risk is communicated throughout the organization. The risk strategy defines the overall objectives that the organization is trying to achieve with respect to risk management. The risk protocols are the systems, standards and procedures that are put in place in order to fulfil the defined risk strategy.

Risk management policy for a council

The council is aware that some risks will always exist and will never be eliminated; it recognizes that it has a responsibility to manage risks (both positive and negative) and supports a structured, systematic and focused approach to managing them by approval of the risk management strategy.

In this way the council will:
- demonstrate effective corporate governance;
- better achieve its corporate objectives;
- enhance the value of services it provides to the community.

The objectives of the council's risk management strategy are to:
- integrate risk management into the culture of the council;
- manage risk in accordance with best practice;
- anticipate and respond to changing social and legislative requirements;
- prevent injury, damage and losses, and reduce the cost of risk;
- raise awareness of risk with all involved with delivery of council services.

These objectives will be achieved by:
- establishing clear roles, responsibilities and reporting lines;
- providing opportunities for shared learning on risk management;
- offering a framework to direct resources to identified priority risk areas;
- reinforcing the importance of risk management as part of every task;
- increasing awareness of employees by offering training;
- incorporating risk management into business planning;
- incorporating risk considerations into partnerships and projects;
- monitoring risk management arrangements on an ongoing basis.

Risk management policy

The risk management policy sets out the risk strategy, and an illustration of suitable contents for a risk management policy is set out in Table 7.2. The risk management policy should facilitate successful implementation of risk management in the organization. The policy should confirm the protocols for undertaking the activities, as set out in the risk guidelines for the organization. The risk guidelines may be produced as a separate set of documents, so that they can be more easily updated.

Table 7.2 Risk management policy

A risk management policy should include the following sections:

- Risk management and internal control objectives
- Statement of the attitude of the organization to risk (risk strategy)
- Description of the control environment
- Level and nature of risk that is acceptable
- Risk management organization and arrangements (risk architecture)
- Arrangements for communicating risk information
- Standard procedures for risk recognition and rating (risk assessment)
- List of documentation for analysing and reporting risk (risk protocols)
- Risk mitigation requirements and control mechanisms
- Allocation of risk management roles and responsibilities
- Criteria for monitoring and benchmarking risks
- Allocation of appropriate resources
- Risk priorities and performance targets
- Risk management calendar of the coming year

The risk management policy should set out the strategy that the organization is seeking to achieve with respect to risk management, together with the systems and procedures that will be put in place to monitor performance, as well as the means for reporting and communicating on risk management. It will, in effect, define the context within which risk management activities take place.

A range of risk management guidelines will need to be produced, and a typical set of guidelines is listed in Table 7.3. The risk guidelines provide more information on how the risk protocols should be interpreted and how they should be delivered. The detailed risk guidelines will set out:

- risk assessment procedures;
- risk control objectives;
- risk resourcing arrangements;
- reaction planning requirements;
- risk assurance systems.

Table 7.3 Risk management protocols

1. Risk assessment procedures
   - Turnbull procedures
   - Response to significant risks
   - Projects and CapEx approvals
   - Procedures for strategy and budgets
2. Risk control objectives
   - Brand management guidelines
   - Health and safety at work
   - Environmental protection
   - Contract risk management
3. Risk resourcing arrangements
   - Opportunity management
   - Project resource allocation
   - Insurance programme
   - Captive insurance company
4. Reaction planning requirements
   - Loss and claims management
   - Disaster and recovery planning
   - Cost containment procedures
   - Risk management record keeping
5. Risk assurance systems
   - Maintenance of risk register
   - Corporate RM committee
   - Terms of reference for audit committee
   - Control self-certification arrangements

The framework or risk architecture that has been set up to achieve adequate management of risks should also be presented in the risk management policy. It will then be for the individual companies within the group to operate within the established framework and arrange their own additional policies, procedures and protocols as necessary. Specifically, the risk management policy should include details of at least the following:

- the board member responsible for risk management;
- language and perception of risk in the organization;
- framework for identifying significant risks;
- role of the risk manager and internal auditors;

- terms of reference for the risk management committees;
- risk management structure or architecture.

Many organizations find that it is necessary to update the risk management policy each year. This is undertaken for a number of reasons, including the desire to ensure that risk management activities and the overall risk management approach is in line with current best practice. Updating the risk management policy every year also gives the organization the opportunity to identify the risk priorities for the coming year and ensure that appropriate attention is paid to the significant risks.

Issuing the risk management policy every year also ensures that the board pays appropriate attention to risk management and that the organization understands that it is a dynamic activity that requires constant management attention.

Risk management architecture

The risk management structure of an organization can be described as the risk architecture. The risk architecture sets out lines of communication for reporting on risk management issues and events. It is vital that the risk architecture reinforces the fact that the responsibility for managing risks remains with the owner of that risk.

So that risk management can be fully embedded into the processes and operations of an organization, a clear statement of risk management responsibilities is required. Also, as part of the analysis of each significant risk, risk management responsibilities need to be clearly allocated to the following aspects of managing that risk:

- development of risk strategy and standards;
- implementation of the agreed standards and procedures;
- auditing compliance with the agreed standards.

The risk architecture can be represented diagrammatically as a means of identifying the committees with risk management responsibilities and the relationships between those committees. The importance of the risk architecture of an organization will be discussed later in this Part and examples of typical risk architectures will be provided.

Risk management strategy

It is important for an organization to have a clearly establish strategy in relation to risk management. The strategy needs to be based on the overall approach of the organization to risk

and risk management. An important component of that risk strategy will be the arrangements for ensuring risk management input into strategy, projects and operations.

In order to establish the risk management strategy, important decisions will need to be made about the risk appetite of the organization. Risk appetite will be discussed in more detail in a later chapter. The risk appetite will be based on the opportunity investment, control acceptance and the hazard tolerance of the organization.

It is important that the risk appetite is within the total risk capacity of the organization. Decisions will need to be taken on how the risk capacity will be calculated. Also, thought will need to be given to how the total risk exposure of the organization will be recorded and used in decision-making processes. Measurement of the total risk exposure of an organization is an important feature of operational risk management, as discussed in a later chapter.

There are important decisions to be made in relation to the risk processes that will be adopted by the organization, as well as decisions about the design and implementation of the risk management initiative that will be undertaken in order to fulfil the requirements of the risk strategy.

Risk management protocols

The risk management policy will set out responsibilities for risk as well as the arrangements for implementing the policy. Risk management protocols will be set out in a series of risk guidelines and these are described in a later chapter.

Procedures and protocols for undertaking the assessment of risks to strategy, projects and operations will need to be established in writing. The organization will also need to produce guidance on the frequency and nature of risk reports and who is responsible for compiling the information.

Typically, the risk management protocols will need to be reviewed on an annual basis, so that they are kept up to date. The risk protocols should also describe the extent of record keeping that is required. The range of risk management documentation that may be necessary is extensive and Table 7.4 provides an overview of the types of documents that may be appropriate.

Table 7.4 Types of RM documentation

Risk administration
- Risk management policy (and priorities)
- Specific risk statements (health and safety policy)
- Terms of reference of the risk/audit committees
- Risk protocols and procedures
- Risk awareness training records

Risk response
- Results of risk assessments (risk register)
- Risk control standards
- Risk improvement recommendations
- Risk assurance reports
- Business continuity plans/disaster recovery plans

Event reports
- Loss/claim reports and recommendations
- Legal and litigation reports
- Enforcement action/customer complaints
- Incident and near-miss investigations
- Business performance reports/key performance indicators

Risk performance
- Control risk self-assessment (CRSA) returns
- Audit procedures and protocols
- Internal audit reports
- Unit risk management reports
- External disclosure reports

Risk management guidelines

Table 7.3 indicates the extent of risk management guidelines that may need to be produced by an organization. This should not be seen as an exhaustive list and other types of guidelines may be necessary, depending on the exact nature of the organization and the risk strategy that it is following.

Preparation of a risk management policy is a good opportunity for an organization to establish detailed procedures on a range of risk management topics, as well as setting out the risk

management priorities for the following year. For example, many organizations produce an annual health and safety and/or environmental policy and this should be an integral part of the risk management documentation.

Many organizations face significant risks that need routine or even constant management attention. This is particularly true in the case of hazard risks, where the health and safety policy, business continuity plans and disaster recovery plans (for example) need to be routinely updated.

For many organizations, the risk guidelines will be established in writing. Other organizations will operate a more informal means of embedding risk management into management activities. The risk guidelines will often include details of the risk management structure in place in the organization. Also, details of the risk strategy and risk protocols will need to be included in the risk guidelines. The guidelines should also include details of the (internal) control responsibilities of managers.

The structure described in Table 7.3 reinforces the importance of the activities involved in the risk management process. Each of these activities produces several outputs, and the required outputs can be discussed in the risk guidelines.

The guidelines need not include a set of risk-control or loss-control standards, but should describe how risk control decisions will be taken, implemented and audited. In fact, the risk guidelines for a diverse group of companies cannot include physical control requirements and standards. Each unit, division or department should set its own standards for risk control, including health and safety, fire safety, physical security, information security and environmental protection. This may be appropriate because of the diverse nature of the different units within the organization.

The risk guidelines should define the means by which embedded risk management is to be achieved in the organization. The setting of strategy, standards and procedures needs to be undertaken within the framework of the risk guidelines. The format for the risk guidelines will depend on the organization and the nature of the risks that it faces. Typically, these guidelines will contain information on at least the following:

- financial and authorization procedures;
- insurance arrangements;
- managers' control responsibilities;
- project risk management;
- incident reporting and investigation;
- event and reaction planning;
- physical risk control objectives and responsibilities.

8

Risk management documentation

Record of risk management activities

Table 7.4 sets out the range of risk management documentation that may need to be kept by an organization. In order to successfully embed risk management, it is necessary to maintain a range of risk management records. These records will include details of various risk management activities, including:

- risk management administration;
- risk response and improvement plans;
- event reports and recommendations;
- risk performance and certification reports.

Embedded risk management will be achieved when the cycle of risk management activities is fully aligned with the planning cycle of the organization. A primary purpose of risk guidelines is to help managers understand the risk management framework of the organization. This understanding will ensure that managers pay appropriate attention to risk implications when making decisions.

The risk guidelines for the organization also provide practical guidance to managers on how to fulfil their risk management responsibilities. Keeping necessary records will allow the organization to demonstrate the successful implementation of the risk guidelines. The risk administration documentation should extend to (at least) the items listed in Table 7.4.

It is not the intention that the keeping of risk management records should become overly bureaucratic or burdensome. However, adequate records need to be kept so that the information is available for decision making, necessary advice for managers is available and confirmation can be provided to auditors that necessary controls have been correctly implemented. The importance of record keeping is highlighted below.

Importance of records

There are many benefits to be gained from implementing records management. Records management is a key driver in increasing organizational efficiency and offers significant business benefits. Records management:

- reduces the time spent by staff looking for information;
- facilitates the effective sharing of information;
- reduces the unnecessary duplication of information;
- identifies how long records need to be kept;
- optimizes the legal admissibility of records to defend malicious litigation;
- supports risk management and business continuity planning.

In short, records management improves control over information assets, frees up staff time and other resources, and helps protect individuals and the organization from various risks. Records management means that too much reliance is not placed on the memories of a few individuals.

Risk response and improvement plans

The only reason for undertaking a risk assessment is so that current controls can be validated and the need for any further actions to improve control of risk can be identified. The risk register is the means of recording information on current controls and details of intended additional controls. It is important that the risk register should not become a static document. It should be treated as a dynamic element and considered to be the risk action plan for a unit or the organization as a whole.

As well as risk response plans, information will also need to be recorded about the responsibility for individual controls. If additional controls are required, then the deadline, as well as the responsibility, for the implementation of those improved controls should be recorded.

A later part of this book considers risk response options in more detail. For hazard risks and control risks, the risk register is the location for recording details of the significant threats. Detailed analysis of risk improvement plans will be required. Often, risk improvement plans will require capital expenditure, and this may need to be approved via the expenditure authorization procedures in the organization.

It has become standard practice to produce a risk register for projects, especially for construction and software projects. Risks to construction and software projects can create a lot of uncertainty and the risks will usually be control risks. Again, the record of the actions taken to minimize the uncertainty should be a dynamic one, and further actions should be planned.

Event reports and recommendations

Event reports, analysis and recommendations are related to recording details of the events that occur and managing the consequences of those events. Details of incident investigations and analysis of the performance of business operations, together with risk improvement recommendations, are all covered by this type of risk management documentation. Risk improvement recommendations address significant control weaknesses and aim to eliminate the potential for future material or significant failures.

Recording of events is an important activity, especially in relation to hazard risks. Also, recording and analysing events during a project will be vitally important. Event reports are most relevant to hazard and control risks. Annual evaluation of risk performance will also give rise to reports that require detailed analysis. Evaluation of risk performance is an important role for internal audit.

Clinical risk management is a well-developed branch of the risk management discipline. Accurate record keeping is vital in order to identify that appropriate risk mitigation actions have been put in place, as well as to provide records of any clinical mishaps that occur. The box below provides an overview of the importance of record keeping in relation to managing clinical risk.

Managing clinical risk

Even if all adverse clinical events could be avoided, the legal cost of malpractice litigation cannot be eliminated. While very few negligent injuries lead to claims, there are many negligence claims in cases where there was no injury and no negligence. This means that, if the right risk management processes and systems are in place, hospitals and doctors should be able to rebut allegations of negligence in these circumstances and successfully argue that no compensation payment should be made.

The implementation of risk management activities in hospitals is the immediate responsibility of hospital management. Nevertheless, doctors have a vital role to play by developing an understanding of the importance of risk management and helping to devise a practical approach to recording that procedures have been followed and any incidents have been recorded.

Risk performance and certification reports

Risk performance and certification reports include consideration and analysis of preliminary reports of the results of operations, as well as more formal declarations and certified reports to stakeholders. In some cases, certification of the results of operations of the organization will be undertaken as a formal attestation of the results of operations. This approach is required by the Sarbanes–Oxley Act in relation to financial reporting.

This attestation will often be undertaken by a third party, such as an external auditor. Such an attestation could also relate to an evaluation of the effectiveness of the control activities. Certification of performance is considered in more detail in Part 6 of this book.

Management will be interested in receiving details of risk performance. This will be especially important when the organization is exposed to a portfolio of risks that bring the total risk exposure close to the limit of the risk appetite and/or risk capacity of the organization. For example, an organization may have budgeted for a certain level of loss in relation to hazard risks. If this budget is challenging, then careful monitoring of losses will be required in order to ensure that the exposure to the specific type of hazard risk is not being exceeded.

The hazard tolerance may be limited and so the organization will need to monitor hazard losses very carefully. For example, a transport company will need to monitor the number of motor vehicle accidents and the breakdown frequencies related to the vehicles run by the company.

Designing a risk register

The use of risk registers has become established practice for many risk managers. There are disadvantages associated with the use of risk registers, including the danger that the information recorded in the risk register will not be used in a dynamic way. The risk register could become a static record of risk status, rather than the risk action plan for the organization.

A risk register is defined in the ISO Guide 73 as the 'document used for recording risk management process for identified risks'. The guide adds that the purpose of the risk register is to facilitate ownership and management of each risk. Typically, the risk register will cover the significant risks facing the organization or the project. It will record the results of the risk assessment related to the process, operation, location, business unit or project under consideration.

When a risk assessment is undertaken of strategic options, it is more usual for the risk assessment to be used as part of the decision-making process. Typically, this information will not be recorded in the format of a risk register, but will be presented to the decision maker as part of the full range of information available for making that strategic decision.

The purpose of the risk register is to form an agreed record of the significant risks that have been identified. Also, the risk register will serve as a record of the control activities that are currently undertaken. It will also be a record of the additional actions that are proposed to improve the control of the particular risk.

Other information about risks will also be included in the risk register. Although there is no fixed format for this document, Table 8.1 provides an outline of a basic format for a risk register. It may not be necessary to include all of the risk description information set out in the table in the risk register, as this could make it a complex and clumsy document.

Table 8.1 Format for a basic risk register

Risk index	Risk description	Current level of risk			Controls in place
		Likelihood	Magnitude	Overall rating	
1.	Serious traffic accident involving the transport of fuel/explosives. Anticipate fatalities and evacuation of 1-km radius, depending on substances involved. Potential for release of up to 30 tonnes of liquid fuel into local environment.	Low	High	Medium	• Police emergency plans • Highway Agency plans • Local authority emergency plan • Company emergency response • Liaison with the family of staff • Notification to customers
2.	Storm-force winds affecting transport routes for up to 6 hours. Anticipate that most roads in the vicinity will be closed or restricted. Journey times will be extended and late deliveries probable.	Medium	Medium	Medium	• Police emergency plans • Highway Agency plans • Investigate weather forecast • Liaison with the family of staff • Notification to customers

Risk registers can be compiled in a number of formats, depending on the type of risk assessment that is being recorded. Table 8.2 provides an example of a partially completed risk register for a sports club and Table 8.3 provides an example of a risk register for a hospital.

Table 8.2 Risk register for a sports club

Risk index	Risk description	Existing control measures	Current level	Further actions planned	Owner
Financial risks					
1.1	Insufficient funds for suitable new players	•	High	•	
1.2	Pension fund inadequate to meet liabilities	•	Medium	•	
Infrastructure risks					
2.1	Loss of highly respected young manager	•	High	•	
2.2	Building of the new stadium is delayed	•	Low	•	
Reputational risks					
3.1	Complaints that merchandise is too expensive	•	Low	•	
3.2	Club supporters riot at an away game	•	Medium	•	
Marketplace risks					
4.1	New range of merchandise is unattractive	•	High	•	
4.2	Fans favour other activities rather than club attendance	•	Low	•	

Table 8.3 Risk register for a hospital

Risk index	Risk description	Current level of risk			Risk rating
		Likelihood	Magnitude	Overall rating	
1.	The roofs on operating theatres 3 and 4 are leaking because of poor condition, resulting in disruption to the surgery lists and non-achievement of waiting times.	High	High	High	Ingress of water can lead to loss of theatre facility, with cancelled operations, loss of key activity and threat to waiting time targets. With high incidence of rain, it is likely that between 1 and 7 days surgery time will be lost. Problems in the last 2 years suggest that the failure will occur twice per year.
2.	Progress towards achievement of standards in children's care will remain unsatisfactory due to failure to implement action plan for improved facilities, resulting in children receiving care below the national standards.	Medium	Medium	Medium	The perception of patients of the current environment is good and the level of care provided is good. Robust action needs to be taken to ensure that standards do not become unsatisfactory.

At its most simple, the risk register can be stored as a document held on computer. However, there are many more sophisticated forms of risk registers, including records of significant risks held on databases. Where quantification of exposure is required, then a simple risk register held as a document is unlikely to be sufficient. This is true of systems for recording operational risks, where quantification of risk exposure is required.

Using a risk register

A well-constructed and dynamic risk register is at the heart of a successful risk management initiative. However, there is a danger that the risk register may become a static document that records the status of risk management activities at a moment in time. The practical implications of this are that senior management may consider that attending a risk assessment workshop and producing a risk register fulfils their risk management obligations and no ongoing actions are required.

It is better to think of the risk register as a risk action plan that records the status of the organization with respect to risk management, but also provides a record of the critical controls that are in place, together with the details of any additional controls that need to be introduced. In producing such a risk action plan, the responsibility for undertaking the actions identified will be clearly established.

The next part considers the options for the use of a risk management information system (RMIS) to record the information held in the risk register. Also, the information held in the risk register may be available on the intranet of the organization and this will help with risk understanding and communication. In some organizations, the risk register is given the status of a controlled document to be used by Internal Audit as one of the key reference documents for undertaking an audit of risk management activities.

Even if this is not the case, the information set out in the risk register should be very carefully considered and constructed. For example, the risks set out in the register need to be precisely defined so that the cause, source, event, magnitude and impact of any risk event can be clearly identified. Also, the existing control activities, together with any additional controls that are proposed, must be described in precise terms and accurately recorded.

Risk control activities should be described in sufficient detail for the controls to be auditable. This is especially important when the risk register relates to the routine operations undertaken by the organization. Risk registers should also be produced for projects and to support strategic decisions.

A project risk register has to be a very dynamic document. An example of a project risk register is provided in Table 8.4. Details of the risks faced by the project, as recorded in the risk register, should be discussed at every project review meeting. As well as risk registers being relevant to projects, they should also support business decisions. In this case, the precise format of a risk register may be less formal. When a strategic decision has to be taken at board level, the risk assessment of that strategy should be attached to the proposal. This risk assessment could include both the risks of undertaking the strategy and an analysis of the risks associated with not undertaking the proposed strategy.

Table 8.4 Project risk register

Risk index	Risk description	Current level of risk			Action to be taken
		Likelihood	Magnitude	Overall rating	
1.	Project management arrangements unable to deliver project.	High	High	High	Clear project management structure in place, with executive team established to oversee project. Smaller project team runs project on day-to-day basis with expert support, as required. Clear links between various management functions to ensure co-ordinated approach.
2.	Project resources inadequate with insufficient staff to support project.	Medium	Medium	Medium	Project management team established with support from other staff departments, including HR and Finance.
3.	Project resources has insufficient funds for the necessary external professional technical advice.	Low	High	Medium	Sufficient budget identified to fund external advice.
4.	Project not co-ordinated with other developments in organization.	Low	Low	Low	Project management team also oversees related projects with cross-representation on other groups.

Finally, a risk register should be attached to a business plan as a record of the risks that could impact the achievement of that business plan. Table 8.5 shows a partially completed simple risk register in a format that could be attached to a business plan. Simple examples of the risks that could result in the business plan not being achieved are set out in this illustration.

Table 8.5 Risk register attached to a business plan

Risk index	Circumstance	Assessment and controls	Current level of risk			Action and assurance
			Likelihood	Magnitude	Overall risk	
1.1	Loss of grant funding	•	High			Negotiations are in hand and final settlement figure should soon be notified.
1.2	Job upgrade costs	•	Medium			Provision has been made in reserves and any additional costs will be met from existing budgets.
1.3	Overtime claims	•	Medium			Heads of department should enforce the rules concerning overtime payments as a result of job upgrades.
1.4	Mileage claims	•	Low			Heads of department should ensure that only essential journeys are undertaken.

For example, a sports club may wish to record risks to reputation in the risk register. There could be particular concerns regarding the reputation of the club, so that the board will require a detailed evaluation of the reputational risks related to:

- success on the pitch;
- legal compliance;
- supply of ethical goods at a fair price.

When considering reputational issues, the level of control that is required will be evaluated, together with responsibility for managing the brand. The club will also make sure that existing controls and any additional controls are described in a way that will ensure that implementation of the controls can be fully audited.

The board will probably wish to see the risk register on at least a quarterly basis and more frequently if significant changes occur. This will ensure that the risk register remains a dynamic document and is kept fully up to date. This will also ensure the necessary actions are taken and reported to the board.

9

Risk management responsibilities

Allocation of responsibilities

Everybody working for the organization will need to be made aware of their risk management responsibilities, as will contractors and suppliers. There are many professional people in large organizations who have an understanding of risk and a substantial contribution to make to the successful management of the priority significant risks. Unfortunately, there is not always a common view of risk management or the issues that are important to the organization.

Ownership of core processes, key dependencies and risks is important, because it enables the risk management and audit committees (see Chapter 4) to monitor actions and responsibilities. This ownership is important for all risks, although the audit committee will only monitor the priority significant risks.

Any confusion of responsibilities and reporting structure must be eliminated. There needs to be clear statements of responsibilities for the following aspects of the management of each priority significant risk:

- setting required risk standards;
- implementing risk standards;
- monitoring risk performance.

A detailed set of responsibilities will ensure that the roles of risk owners, process owners, internal audit, risk manager, specialist risk management functions, members of staff, contractors and outsourced operations as well as all others are clearly defined and understood.

Information on ownership of each priority significant risk should be included in the risk register. It is important that the activities of the risk manager, risk management committee, audit committee, internal auditors and others do not reduce local ownership of significant risks. Managers must see ownership of risks as integral to the management of core processes and

business activities, not as a separate issue that is the responsibility of specialist professional risk management and/or internal audit practitioners.

Risk management and internal audit

There needs to be a close working relationship between risk management and internal audit. The responsibilities allocated to each of these functions will vary according to the nature, type and size of the organization. This is an important working relationship, because successful management of risk depends on four important risk-based outputs, which can be summarized as CADE3:

- Compliance with appropriate standards, laws and regulations;
- Assurance for the management team and other stakeholders;
- Decisions regarding strategy based on the best information available;
- Efficient processes, Effective processes and Efficacious strategy.

It is clear that if these outputs are to be successfully delivered, all stakeholders need to work together, and that includes co-operation between risk management and internal audit. The range of activities that are related to risk management and internal audit are explored in a later Part of this book. In particular, the important contribution made by internal audit and a range of activities that the internal audit department undertake is considered in more detail in Part 6.

Range of responsibilities

Table 9.1 sets out examples of the range of risk management responsibilities of line management, the main functional departments and individual employees involved in risk management. The risk management professionals involved will include the following individuals (at least), depending on the size of the organization:

- insurance risk manager;
- corporate treasurer;
- finance director;
- internal auditor;
- compliance manager;
- health, safety and environment manager;
- business continuity manager.

Table 9.1 Risk management responsibilities

1. Main risk management responsibilities for the CEO:
   - Determine strategic approach to risk
   - Establish the structure for risk management
   - Understand the most significant risks
   - Consider the risk implications of poor decisions
   - Manage the organization in a crisis
2. Main RM responsibilities for the location manager:
   - Build risk-aware culture within the location
   - Agree risk management performance targets for the location
   - Evaluate reports from employees on risk management matters
   - Ensure implementation of risk improvement recommendations
   - Identify and report changed circumstances/risks
3. Main RM responsibilities for individual employees:
   - Understand, accept and implement RM processes
   - Report inefficient, unnecessary or unworkable controls
   - Report loss events and near-miss incidents
   - Co-operate with management on incident investigations
   - Ensure that visitors and contractors comply with procedures
4. Main risk management responsibilities for the risk manager:
   - Develop the risk management policy and keep it up to date
   - Facilitate a risk-aware culture within the organization
   - Establish internal risk policies and structures
   - Co-ordinate the risk management activities
   - Compile risk information and prepare reports for the board
5. Main RM responsibilities for specialist risk management functions:
   - Assist the company in establishing specialist risk policies
   - Develop specialist contingency and recovery plans
   - Keep up to date with developments in the specialist area
   - Support investigations of incidents and near misses
   - Prepare detailed reports on specialist risks
6. Main risk management responsibilities for internal audit manager:
   - Develop a risk-based internal audit programme
   - Audit the risk processes across the organization
   - Provide assurance on the management of risk
   - Support and help develop the risk management processes
   - Report on the efficiency and effectiveness of internal controls

Externally, insurance brokers, insurance companies, accountancy firms and external auditors also have a contribution to make to the improved management of risk in their client organizations. It is important that risk management professionals work together. However, it is also important that the benefits of risk management are embedded into the core processes of the organization.

There is a need to ensure that management of risks receives a sufficiently high profile. It will normally be a board member who sponsors risk management awareness at the board and presents risk management reports to it. Typically, the risk manager will report to that board member, in the role of guardian of the risk architecture, strategy and protocols (GRASP).

One of the most important responsibilities to be allocated is that of 'risk owner'. ISO Guide 73 defines risk owner as 'person with authority and accountability to make the decision to treat, or not to treat a risk'. The guide also states that anyone who has accountability for an objective also has accountability for the risks associated with the objective and the implementation of the controls to manage those risks.

Statutory responsibilities of management

There has been a developing trend in many countries towards ensuring greater clarity in regard to the obligations of company directors. The general duties of directors have developed in the common law over many years in most countries. The Companies Act 2006 in the UK has consolidated the common law duties of directors and codified the general duties, as follows:

- act in accordance with allocated responsibilities;
- act in accordance with the constitution of the company;
- promote the success of the company;
- exercise independent judgement;
- exercise reasonable care, skill and diligence;
- avoid/declare conflicts of interest;
- not accept benefits from third parties.

The responsibilities of directors are important in relation to risk management and adequate management of risk will assist in the successful fulfilment of these obligations. Risk management is particularly important in promoting the success of the organization and exercising reasonable care, skill and diligence. Directors of organizations need a good understanding of risk management so that they will be in a better position to fulfil their statutory and other duties.

Usually, board directors will be either executive directors or non-executive directors of the organization. In certain organizations, such as charities and most government departments, executive directors will meet separately as an 'executive committee' and the non-executive directors will form a 'board of governors'. Typically, executive directors will be full-time employees of the organization with a specific area of responsibility.

Non-executive directors have an important role to play in risk management within the organization. However, this role will normally be restricted to audit, assurance and compliance activities. It may be inappropriate for non-executive directors to become involved in the management of the individual risks, because of the conflict with non-executive audit responsibilities and because executive directors are in a better position to understand and deal with the risks that the organization faces.

The box below provides an example of the role and expectations of non-executive directors. In general, non-executive directors should not become directly involved in the day-to-day management of the organization. In most cases, their role is to assist with the formation of strategy and the monitoring of performance. Implementation of strategy is the responsibility of executive directors.

Role of non-executive directors

The role of the non-executive director has the following specific key elements:

- Strategy – constructively challenge and help develop proposals on strategy.
- Performance – scrutinize the performance of management.
- Risk – challenge the integrity of the financial information.
- Controls – seek assurance that financial controls and systems of risk management are robust and defensible.
- People – determine the appropriate level of remuneration for the executive directors and have a prime role in succession planning.
- Confidence – seek to establish and maintain confidence in the conduct of the company.
- Independence – be independent in judgement and promote openness and trust.
- Knowledge – be well informed about the company and the external environment in which it operates, with a strong command of relevant issues.

Role of the risk manager

The typical historical role of the insurance risk manager is set out in Table 9.2. Historically, the risk manager has been involved in assessing overall risk policy with endorsement from the board. Decisions on insurance risk management issues and the provision of statistical analysis of insurance losses have been part of these historical responsibilities.

The insurance risk manager needs to evaluate the current status of risk management and reflect on the current state of the insurance market. Increases in insurance rates and a more sophisticated approach to risk financing have affected the amount of insurance purchased by large organizations. In many cases, there has been less insurance purchased and this has led to a reduced premium spend and a lower budget for the insurance risk management department.

There is no single established reporting position in the structure of an organization for the risk manager. At present, risk managers may report to human resources, the finance director or the company secretary. Sometimes, the risk manager is a report to the corporate treasurer and, occasionally, the chief executive officer (CEO).

There is still a need for a risk management facilitator and co-ordinator in most large organizations. This will enable the organization to apply risk management tools and techniques to a wider range of issues. Risks have historically been divided into insurable (pure) and non-insurable (speculative) risks. From a business success perspective, these are artificial divisions between types of risks.

Table 9.2 Historical role of the insurance risk manager

1. To establish the risk management strategy for protecting company property and people.
2. To co-ordinate the company insurance programme through the captive insurance company.
3. To work with the manager of the captive to maximize the contribution made by the captive insurance company.
4. To maintain key insurer relationships, monitor service providers and ensure cost-effective placement of insurance contracts.
5. To measure and monitor cost of risk performance of the group and individual group companies.
6. To ensure safe keeping and adequate retention of all insurance contracts and agreements.
7. To supervise the co-ordination of service provider activities and place the group and global insurances.
8. To co-ordinate the property survey programme, risk management procedures and incentive schemes.

The risk manager should be responsible for the corporate learning that has to take place so that the organization can understand the benefits of risk management. As guardian of the risk architecture, strategy and protocols (GRASP), the risk manager will be responsible for developing the strategy, systems and procedures by which the required risk management outcomes for the organization are achieved.

Historically, the insurance risk manager has probably not been involved in the strategic management and development of the organization. The broader role now required of a risk manager should lead to a greater involvement in project management and strategy formulation and delivery. The risk manager who enjoys a broad range of responsibilities will have a very challenging role within the organization. It will be a role that enables the risk manager to obtain a better level of understanding and involvement than most other roles or functions achieve.

Chief risk officer (CRO)

Perhaps, the title 'Risk Manager' has too many historical connections for it to be used as an appropriate description of what is now required. There is a need to find a new title and redefine the role of risk management at the same time.

Many organizations in the finance and energy sectors have identified the benefits of bringing the management of credit, market and operational risks together. It has been the case for some time in the finance sector that risk management has been separate from the purchase of insurance. The development of the role of chief risk officer (CRO) reporting directly to the CEO reflects this fact.

Given that one of the key principles of risk management is that the approach to risk should be proportionate to the level of risk faced by the organization, it is unlikely that the majority of organizations will need to appoint someone of the seniority of a CRO. Nevertheless, organizations should, when reviewing their risk management architecture, decide the appropriate range of responsibilities and level of seniority of the risk manager.

The introduction of the job title Chief Risk Officer (CRO) is not universal, but it is becoming common in the specialist finance and energy sectors. Guardian of the risk architecture, strategy and protocols (GRASP) is a superior description of the role that must be fulfilled.

The box below provides an overview of the developing role of the chief risk officer. For organizations where it is proportionate for a CRO to be appointed, the contribution that can be made by that individual will be substantial.

Chief risk officer

As champion of the ERM process, the CRO plays a key part in bringing together disparate risk management processes to ensure that limited company resources are applied effectively. The COSO ERM Framework defines the role of the CRO as working with other managers to establish effective risk management, monitoring progress, and assisting other managers in reporting relevant risk information up, down and across the organization.

Internal auditors should work with the CRO as part of their risk management duties. In this role, internal auditors are responsible for evaluating the accuracy of ERM reporting and providing independent and value-added recommendations to management about its ERM approach. The IIA International Standards specify that the scope of internal auditing should include evaluating the reliability of reporting effectiveness, efficiency of operations and compliance with laws and regulations.

10

Risk architecture and structure

Risk architecture

Table 8.1 (page 80) shows the risk architecture for a typical large corporate entity that is subject to the requirements of the Sarbanes–Oxley Act. This risk architecture should be set out in the risk management policy for the organization. Terms of reference of the various committees and a schedule of the activities should also be established, either in the risk management policy or in a calendar of risk management activities. This schedule of activities should be aligned with the other corporate activities in the organization.

For a large organization with non-executive directors, the audit committee should also be shown in the risk management architecture. The role of the audit committee and the role of the head of internal audit are important in fulfilling the risk management strategy of the organization.

For organizations subject to the requirements of the Sarbanes–Oxley Act, there will also be a requirement to ensure that all information disclosed by the company is accurate. In many large organizations, this requirement has resulted in the establishment of a disclosures committee. The role of the disclosures committee is to check the source and correctness of all information that is disclosed by the organization. Sarbanes-Oxley requires that financial information is evaluated to a higher level of scrutiny.

The risk architecture of an organization sets out the hierarchy of committees and responsibilities related to risk management and internal control. In the structure shown in Figure 10.1, the corporate risk management committee focuses on executive risk management activities.

Risk management responsibilities for activities at divisional or unit level should be allocated to divisional management. Divisional management is responsible for co-ordinating the identification of significant risks at divisional level, compiling the risk register for the division and ensuring that adequate controls are identified and implemented.

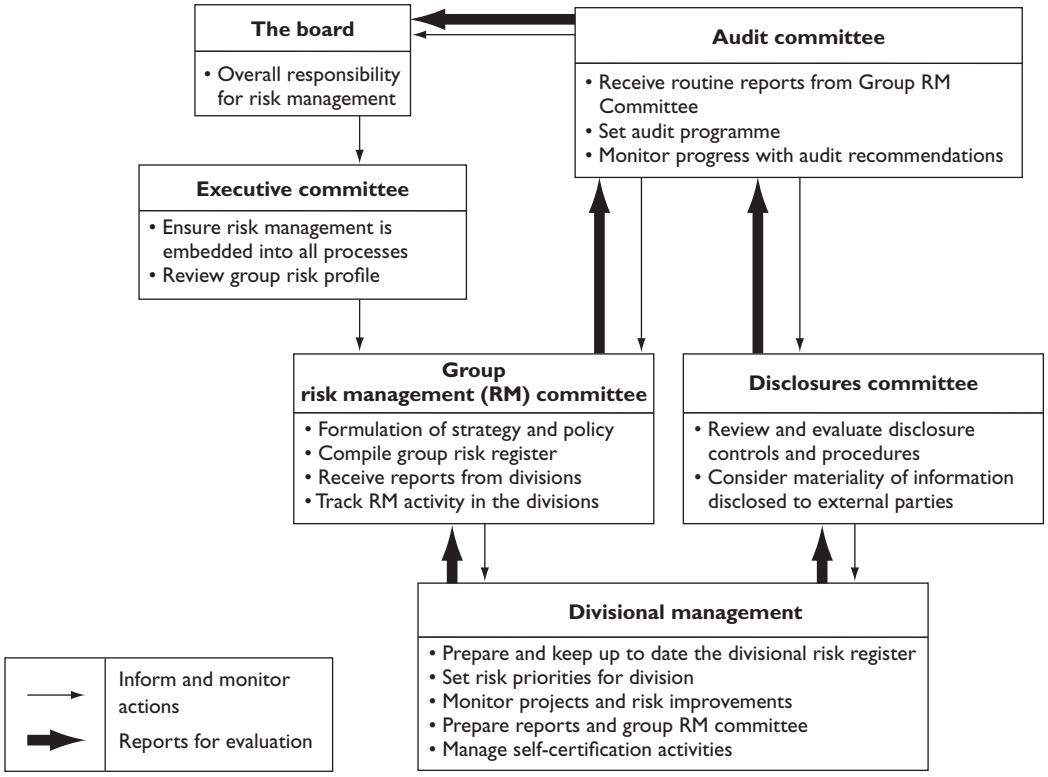


Figure 10.1 RM architecture for a large corporation

Divisional management should be provided with guidance from the group risk management committee. If there is a divisional committee, it should be required to send reports to the group risk management committee, so that the corporate or group overview of risk management priorities can be established.

For a public sector or charity organization, the risk architecture will be somewhat different. Figure 10.2 sets out a typical risk architecture for a charity. In this case, risk management activities are focused on the governance and risk committee. The flow of information and the control of risk management activities are illustrated by the arrows in Figure 10.2.

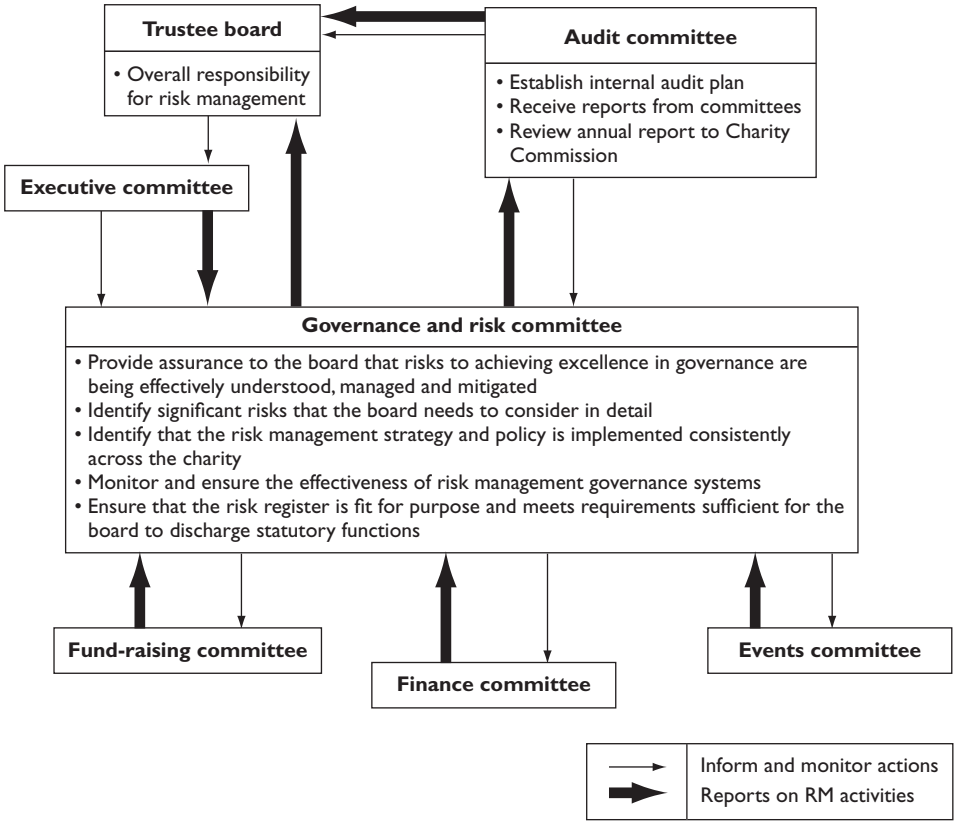


Figure 10.2 RM architecture for a charity

Corporate structure

There are many ways for risk management reporting lines to be established. The reporting structure should be proportionate to the level of risk and the complexity of the organization. For high-risk organizations, such as those in the finance sector, the risk committee is likely to be a direct sub-committee of the board. In these circumstances, it is likely that the risk committee will be chaired by the group finance director and it will have other senior representation from the board.

In general, the risk management committee should be an executive committee made up entirely of executive directors with no non-executive director membership. This is because the management of risk is an executive function and non-executive directors are primarily responsible for audit and risk assurance. Typically, the risk management committee will send reports to the audit committee, and that will be the opportunity for non-executive directors to evaluate risk performance and obtain risk assurance.

For organizations that are not operating in such a high-risk environment, it may not be necessary for the risk committee to be a direct report to the main board. In these circumstances, the risk committee may be a sub-committee of the executive committee or the operations committee. In all cases, the corporate structure for the management of risk should be proportionate to the level of risk within the organization and the size, complexity, nature and risk exposure of the organization.

However, there are no specified correct structures for the risk architecture of an organization. Provided that the risk committee delivers the required outputs, the membership and terms of reference will be for the organization to decide. Nevertheless, the general point remains that management of risk is an executive function, whereas audit activities should be led by non-executive directors.

Risk committees

Table 10.1 sets out typical responsibilities for a risk management committee (RMC). Most large organizations will already have an audit committee, chaired by a senior non-executive director. An option considered by many organizations is to extend the role of the audit committee to include all aspects of risk management or to establish a separate risk management group chaired by an executive director.

There is a strong justification for the RMC to be an executive group, rather than part of any existing non-executive audit committee. This is necessary because risks need to be managed in a proactive manner as an executive responsibility. The existing audit committee is likely to treat the management of risk as a non-executive (reactive) auditing of compliance. Separation of executive responsibility for the management of risk from non-executive responsibility for auditing and review of compliance will also be consistent with good corporate governance principles.

Some organizations have established the RMC as a sub-committee of the audit committee. If this is the case, actions need to be taken to ensure that risk is managed as an executive responsibility, rather than audited as a compliance/assurance issue. In fact, establishing RMC as a sub-committee of the audit committee could impair the work of RMC because of increased bureaucracy and an unhelpful emphasis on auditing and compliance, rather than proactive management of risks.

Membership of the RMC is another question that needs to be addressed. The fundamental decision to be taken in large organizations is whether the risk management committee should be a small senior executive group setting strategy and policy or whether it should be a knowledge-sharing group with representation from each of the units or departments within the organization. The answer will depend on the structure of the organization and the intended role of the committee.

Table 10.1 Responsibilities of the RM committee

To advise the board on risk management and to foster a culture that emphasizes and demonstrates the benefits of a risk-based approach to risk management
To make appropriate recommendations to the board on all significant matters relating to the risk strategy and policies of the company
To monitor the performance of the risk management systems and review reports prepared by relevant parties
To keep under review the effectiveness of the risk management infrastructure of the company, including: • assessment of risk management procedures in accordance with changes in the operating environment • consideration of risk audit reports on the key business areas to assess the level of business risk exposure • consideration of any major findings of any risk management reviews and the response of management • assessment of the risks of new ventures and other strategic, project and operational initiatives
To review the risk exposure of the company in relation to the risk appetite of the board and the risk capacity of the company
To consider the development of risk management and make appropriate recommendations to the board
To consider whether disclosure of information regarding risk management policies and key risk exposures is in accordance with financial reporting standards

The overall aim is to achieve a prioritized, validated and audited improvement in risk management standards in the organization. The RMC and the audit committee should, therefore, operate in a way that provides mutual support. However, combining the two committees into a single group, or placing one committee as superior to the other will not be the best way forward for most organizations.

Risk communications

Accurate communication on risk issues is vitally important. Internal communication within the organization will be undertaken through the risk architecture. This is the formal risk communication structure related to risk control activities and the collecting of information for external risk reporting purposes. For example, a road haulage company may wish to bring focus to the efficient operation of the organization and ensure that risk management receives appropriate attention.

In these circumstances, the company might decide to introduce a number of measurable loss-control programmes. The board of the company has requested a report at every board meeting on the number of road accidents, frequency of vehicle breakdowns, level of fuel consumption and reported incidents during deliveries. These reports will enable the board to benchmark the performance of the company, in comparison both with competitors and also with historical data for the company itself. In this case, the board is monitoring performance, whereas the management of the improved risk performance remains an executive responsibility to be delivered by line management.

Within some organizations, risk communication may also be more informal. Communication will take place during risk assessment workshops and at risk training courses. Communication arrangements are part of the risk culture and this is considered in more detail in a later Part of this book. External risk communications should be considered as having two components. Communication will need to take place with external stakeholders, including the media, the general public and pressure groups.

For example, if a road haulage company wishes to extend the vehicle storage depot, there will be a need to communicate with stakeholders, as well as local authority planning departments. The company will need to prepare arguments that provide an evaluation of any risks to the community that may increase when the depot is extended. The public perception of what is proposed and the impact on the vicinity may not be fully accurate. Accordingly, the company will need to prepare honest, open and detailed arguments that assure all interested parties that adequate risk control arrangements are in place.

The box below provides an example of risk communication in relation to nuclear and chemical industries in the United States. The lesson here is that the public perception of risk may not be aligned with the scientific evidence. The information presented by an organization needs to do more than present intellectual information. The communication should also address emotional concerns.

Risk communication

The formal development of risk communication as a subject began in the late 1970s with efforts by the nuclear and chemical industries in the United States to counteract widespread public concern about those technologies. It was believed that clear, understandable information was all that was needed to make people see that the risks were lower than many feared.

For decades this approach has failed, and most risk communication experts say it is inadequate. Perceptions of risk, and the behaviours that result, are a matter not only of the facts but also of our feelings, instincts and personal life circumstances. Communication that offers the facts but fails to account for the affective side of our risk perceptions is simply incomplete.

Risk communication is also commonly thought of as what to say under crisis circumstances, but this is inadequate. While it is certainly true that communication in times of crises is important in managing the public response, countless examples have taught that a great deal of the effectiveness of risk communication during a crisis is based on what was done beforehand.

Risk maturity

Table 10.2 sets out a system for determining the level of risk maturity within an organization with regard to risk management processes. This table sets out four levels of risk maturity, described as naive, novice, normalized and natural (4Ns). The characteristics of each of these levels are described in the table. Clearly, it is better for an organization to seek a higher level of risk maturity. However, the approach to achieving risk maturity in the organization should be proportionate to the level of risk that the organization faces.

The level of risk maturity within an organization will help define the level of sophistication that the organization has in its risk management activities. Figure 4.2 (page 44) discusses the level of sophistication of the contribution that risk management can make to company activities. The greater the level of risk management sophistication achieved by an organization, the greater the benefits. Achieving an improved level of maturity in relation to risk management processes does not necessarily guarantee that a greater level of sophistication will be achieved, or that a higher level of benefits will be obtained.

Nevertheless, achieving an improved level of risk maturity may be one of the strategic aims for risk management within the organization. If that is the case, an established framework for measuring risk maturity is required. It is important that the organization uses a risk maturity

Table 10.2 Four levels of risk maturity

Level 1 – Naive
Level 1 organizations are unaware of the need for the management of risk or do not recognize the value of structured approaches to dealing with uncertainty. Management processes are repetitive or reactive, with insufficient attempt to learn from the past or to prepare for future threats or uncertainties.
Level 2 – Novice
Level 2 organizations are aware of the potential benefits of managing risk, but have not implemented risk processes effectively and are not gaining the full benefits. The organization is either experimenting with the application of risk management or is operating a risk management process that has fundamental weaknesses.
Level 3 – Normalized
Level 3 organizations have built the management of risk into routine business processes and implement risk management throughout the organization. Generic risk management processes are formalized and the benefits are understood at all levels of the organization, although they may not be consistently achieved.
Level 4 – Natural
Level 4 organizations have a risk-aware culture with a proactive approach to risk management in all activities. As a result, the consideration of risk is inherent to routine processes. Risk information is actively used and communicated to improve processes and gain competitive advantage.

model that aligns with its own ambitions in relation to risk management maturity and provides a practical approach that can be embedded within the organization.

Several types of risk maturity approaches are in existence, including the Criteria of Control (CoCo) framework. The approach adopted by the Criteria of Control (CoCo) framework focuses very heavily on the importance of risk maturity. The approach of this internal control framework is that if the risk culture and the risk architecture, strategy and protocols are correct then good levels of risk management and internal control will be achieved. Another risk maturity model that is frequently used is the European Foundation for Quality Management (EFQM) model.

Alignment of activities

Risk management activities and the risk architecture, strategy and protocols should be aligned with the business processes within the organization. Risk information flows around the risk management framework and (if successful) this will produce various outputs. These outputs have already been described as compliance, assurance, decisions and efficiency/effectiveness/efficacy (CADE3).

Most risk management standards make reference to the upside of risk or discuss the management of opportunity risks. Project risk management, or the management of control risks, has become a separate discipline within risk management, and project risk management has become well developed, with separate guidance material.

When considering the contribution that risk management can make to the organization, it is important to decide whether the contribution will relate to strategy, projects and/or operations. This decision will enable the risk management activities within the organization to be aligned with the other business operations, processes and imperatives.

It is important that risk management activities are aligned with other operations, so that the risk management procedures can be fully embedded into the existing management procedures and activities within the organization. This will also ensure that risk management activities are undertaken in an efficient and embedded manner and are not seen as a separate activity detached from management of the organization.

11 Risk-aware culture

Styles of risk management

We have already seen that there are three (complementary) styles of risk management, related to the nature of the risk under consideration. Hazard management, control management and opportunity management define and describe the approach and, to some extent, the level of sophistication that is applied to risk management by an organization at a point in time.

Hazard risks will always have a negative outcome associated with the risk. The maximum exposure to the risk that is acceptable to the organization is the hazard tolerance. Control risks will have a cost associated with controlling the risks, and this cost can be described as the control acceptance. Opportunity risks have a range of possible outcomes from highly positive to highly negative. The intended and planned outcome is, of course, positive. The organization will be willing to put resources at risk in pursuit of opportunity risks, and this is the opportunity investment.

The type of risk under consideration helps determine the style of risk management that will be applied. However, some risks may need to be managed using all three styles of risk management, at different stages in the lifecycle of the risk. In summary, the three styles of risk management can be viewed as follows:

- hazard management, or the 'total cost of risk' approach of the insurance world (1980s);
- control management is based on internal control approach of internal auditors (1990s);
- opportunity management is the interface between risk management and strategic planning (2000s).

The hazard tolerance, control acceptance and opportunity investment are the values that the organization is willing to put at risk. These three components added together are the risk

appetite of the organization and represent the total acceptable risk exposure of the organization. The total risk exposure is the sum of the risk exposures for the individual risks and this actual risk exposure may differ from the risk appetite of the board and/or the risk capacity of the organization.

The insurance risk manager will normally manage motor vehicle risks as a loss minimization or 'total cost of risk' issue. The avoidance of internal fraud will normally be managed as an internal control issue and will be monitored and reviewed by the internal audit department. Risks associated with a merger or acquisition should be managed as an opportunity issue by the CEO or nominated senior executive.

Defining risk culture

The culture of an organization is difficult to define. However, it is generally accepted that it is a reflection of the overall attitude of every component of management within a company. The culture of an organization determines how individuals will behave in particular circumstances. It will define how an individual feels obliged to behave in all circumstances.

A good risk culture will be the product of individual and group values and of attitudes and patterns of behaviour. This will lead to a commitment to the risk management objectives of the organization. Organizations with a risk-aware culture are characterized by communication founded on mutual trust and a shared perception of the importance of risk management. There also needs to be a sharing of confidence in the selected control measures and a commitment to adhering to the established risk control procedures.

Table 11.1 sets out the suggested components of a risk-aware culture. These components are suggested by recent UK Health and Safety Executive (HSE) research as leadership, involvement, learning, accountability and communication. This makes the acronym LILAC. Creating a culture where effective risk management is an integral part of the way people work is a long-term aim for most organizations.

If an organization decides to raise awareness of security issues, it may decide to launch a campaign to focus on the risks and the relevant controls. The campaign should use more than one means of communication if it is to be successful. The awareness campaign could include all of the LILAC components and may extend to:

- risk awareness training;
- awareness poster campaigns;
- site inspections;
- arrangements for reporting defects;
- leaflets and brochures;

Table 11.1 Risk-aware culture

A risk-aware culture is achieved by LILAC:

Leadership	Strong leadership within the organization in relation to strategy, projects and operations
Involvement	Involvement of all stakeholders in all stages of the risk management process
Learning	Emphasis on training in risk management procedures and learning from events
Accountability	Absence of an automatic blame culture, but appropriate accountability for actions
Communication	Communication and openness on all risk management issues and the lessons learnt

- risk-reporting helpline;
- liaison with the local police;
- allocation of responsibilities.

Components of a risk-aware culture

A risk management initiative cannot be successful unless the culture of the organization is receptive to the initiative. In order to be receptive, a risk-aware culture is required in the organization. A high level of maturity in relation to leadership will require senior management to actively promote a risk-aware culture. This will include setting risk management performance targets and ensuring that the commitment of senior management to the risk-aware culture is clear. This will require verbal and written communications.

Involvement and participation of senior management is a necessary component of achieving a risk-aware culture. Involvement can be achieved by adequate training, so that ownership of risks is fully understood. Specialist risk functions should play an advisory or consultancy role. There should be feedback mechanisms in place to inform staff about any decisions that are likely to affect them.

The existence of a learning culture is vital to the success of a risk-aware culture. A learning culture enables organizations to learn, and to identify and change inappropriate risk behaviour. In-depth analysis of incidents and good communication of feedback enables a learning culture to develop. Workshops on risk issues are another key component of a learning culture.

Accountability is vitally important if the risk-aware culture is to be successful. However, it is not the same as a blame culture. The organization should ensure that it moves from a blame culture to a just culture based on accountability. When investigating incidents, management should demonstrate care and concern towards employees. Employees should feel that they are able to report issues and concerns without fear that they will be blamed or disciplined personally.

A risk-aware culture requires good communication of risk information from senior management. Good communication also requires that reports from all employees, as well as reports from outside the organization, are welcome and well received. Information on risk performance should be included in the communication processes.

Measuring risk culture

It can be difficult for an organization to measure risk culture. However, the risk culture of the organization is so important that measurements need to be taken. Audit committees will often ask how seriously a department or location takes risk management. In general, it will be easy to answer this question on a qualitative basis. However, quantitative measurements are required, so that areas of weakness can be identified and improvement actions planned.

The Canadian Criteria of Control (CoCo) framework represents a means for measuring the risk culture of the organization. Another measure of the risk culture is that the audit committee seeks to evaluate the level of risk assurance that is available from the particular unit or division under consideration.

Another means of measuring risk culture is to look at the level of risk maturity within the organization. Table 10.2 (page 102) describes the levels of risk maturity that can be achieved. Quantitative measures that indicate the level of risk maturity can be taken and areas for improvement can then be identified. The box below provides an example of risk awareness and the embedding of risk management into the culture of an organization.

Risk awareness

The embedding of risk management into the organization has been undertaken by following three routes: a risk awareness campaign; the implementation of new risk identification processes at directorate level, and the ongoing development of existing risk processes at a strategic level.

The primary aim of the awareness campaign was to make staff realize their responsibilities towards risk, whilst at directorate level the introduction of risk registers has been collaborative and inclusive. Strategically, further development of the corporate risk register aims to bring tighter control of risk and provides comprehensive evidence and assurance to the board that risks are managed.

Risk culture and risk strategy

The quality of a risk management policy and details of the requirements and procedures contained in the risk guidelines will give an indication of the risk culture of the organization. For many organizations, improvement in the risk culture is a valid strategic risk objective. This will be especially true when areas of weakness in the level of risk awareness have been identified.

When undertaking actions to improve the risk culture within an organization, it is important to acknowledge that improving the risk management processes must lead to improvements in risk management outputs. This, in turn, should have a positive impact that delivers greater benefits from risk management.

There is little point in improving the risk management processes as a means of improving the risk culture of the organization if the overall effectiveness of the risk management effort is not enhanced. There is a danger that enhancing and improving the risk management process in an organization is automatically assumed to have improved the risk culture.

It is possible for the risk management process to be enhanced without the risk culture of the organization being improved. Improvements to the risk management process may not deliver any additional benefits, whereas improvements to the risk culture should be expected to provide an enhanced level of risk assurance.

Establishing the context

ISO 31000 places considerable importance on context and this is illustrated in Figure 6.5 (page 61). Information is provided in the standard on the importance of the external context, internal context and risk management context for the organization. Context is closely related to risk management culture and the benefits that will be derived from enhanced risk management within the organization.

The Canadian Criteria of Control (CoCo) framework of internal control concentrates on the control environment in an organization. Additionally, the COSO ERM framework (2004) refers to the internal environment of the organization, rather than the control environment that was described in the COSO Internal Control framework (1995). The control environment and the internal environment are measures of the risk culture and the level of risk awareness within the organization.

An overall improvement in risk performance will be achieved through improvements in the internal context, risk management context, control environment or internal environment. The level of risk maturity, the achievement of a risk-aware culture and the fulfilment of the LILAC criteria set out in Table 11.1 are all means of improving the control or internal environment.

During the 1990s, a system called the balanced scorecard became a popular management tool. This is a management system that enables organizations to clarify their vision and strategy and translate them into action. Many large organizations use balanced scorecards as a means of establishing context for the various initiatives that are undertaken within the organization. The government agency used as the basis for Figure 19.2 (page 180) is an example of an organization that uses the balanced scorecard.

If an organization uses the balanced scorecard, it is sensible to use the same framework for risk management activities. By making risk management processes and procedures compatible with existing activities, the risk management requirements are more likely to be accepted and fulfilled. This represents an alignment of risk management activities with existing protocols, in order to embed risk management in the organization and create a more risk-aware culture.

12
Risk training and communication

Risk training and risk culture

As set out in Table 11.1 (page 106), the risk culture of the organization can be defined by leadership, involvement, learning, accountability and communication (LILAC). The LILAC headings also provide an indication of the components of a successful initiative to embed risk management in the organization. The involvement, learning, accountability and communication components of a risk-aware culture are all highly relevant to risk training and risk communication.

Appropriate risk management documentation will provide managers and staff with information on the involvement that is required and the level of accountability that the organization expects. A good level of learning and communication can be established by adequate risk training and this will enhance the risk-aware culture of the organization.

Consider the example of a publisher facing libel and slander risks. The company should prepare risk guidelines, including reference to awareness training for all staff. Comprehensive procedures for managing libel and slander risks should reflect the level of risk exposure. The level of attention paid to such risks will depend on each magazine title and the following framework may be appropriate:

- all journalists to be given basic libel and slander training;
- specific review procedures introduced for political titles;
- legal evaluation of every issue of a satirical magazine.

Training needs to be provided for staff in the revised procedures, and information should be included on the company intranet site. Managers and staff need to be encouraged to comment on the new procedures, so that they may be improved further as part of the learning culture within the company.

Risk training is a key part of learning and communication and it is essential for manager, staff and other stakeholder engagement. It should cover a wide range of topics and achieve a greater understanding of all the risk-related issues, as well as providing information on the control measures that are in place and the vital role played by staff in the successful implementation of these controls.

Risk information and communication

Component 7 of the US COSO ERM framework considers the importance of risk information and communication. Risk communication starts with the identification of the stakeholders that have an interest in the particular risk under consideration. Once the stakeholders have been identified, the nature of the risk information that needs to be communicated must be decided. Finally, the purpose of communicating risk information to each group of stakeholders should be analysed.

Stakeholders will already have a perception of risks, so risk communication should be provided against the background of that existing perception. The guidelines relevant to risk communication set out in Table 12.1 should be followed. These guidelines seek to establish rules for communicating risk issues to a broad range of stakeholders.

Table 12.1 Risk communications guidelines

- **Know the stakeholders**, by identifying both external and internal stakeholders and finding out their interests and concerns
- **Simplify the language** and presentation, although not the content if complex issues need to be communicated
- **Be objective** in the information provided and differentiate between opinions and facts
- **Communicate clearly** and honestly, taking account of the level of understanding of the audience
- **Deal with uncertainty** and discuss situations where not all information is available and indicate what can be done to overcome these problems
- **Be cautious when putting risks in perspective**, although comparing an unfamiliar risk with a familiar one can be helpful
- **Develop key messages** that are clear, concise and to the point, with no more than three messages communicated at any one time
- **Be prepared** to answer questions and agree to provide further information if it is not currently available

Clearly, these rules become more important when the communication about risk is with external bodies. Nevertheless, they provide a useful set of guidelines for risk communication with internal as well as external stakeholders. Internal stakeholders have additional reasons for being provided with risk information. There will normally be an expectation by the organization that managers and staff will play a role in the future management of the risk, whereas this may not always be the case for external stakeholders.

Shared risk vocabulary

Part of communicating successfully on risk matters is the development of a common language of risk. Appendix A provides the vocabulary that is used in this book, as well as making reference to the definitions used in ISO Guide 73, which provides internationally recognized terms related to risk management. However, it is sometimes necessary for the organization to develop its own risk vocabulary, for aspects that may be particular and unique to it. A common understanding of risk based on the use of terminology within the organization is more important than arguments about precisely what a term means to different risk management practitioners.

In fact, as part of aligning risk management effort and embedding risk considerations into routine operations, it may be appropriate for the risk manager to use the terminology already in place in an organization. Even if the vocabulary of the organization conflicts with strict risk management definitions, communication will be more successful if the established vocabulary is used.

In this book, a standard vocabulary has been used in order to assist with the introduction and explanation of concepts relevant to risk management. Sometimes, this vocabulary contradicts ISO Guide 73, but it has been used to aid communication and understanding. The subject of a risk vocabulary and agreeing definitions can take a great deal of time and effort, and compromise is usually required.

A common language and agreed definitions are important so that all parties to a discussion have the same understanding of the terminology being used. This is illustrated by the summary in the box below.

Language of risk

The first reason an organization needs a risk language is to underpin its risk culture. Everyone in the organization has a role in an effective risk management process. Most organizations have many layers (eg executives, line managers and employees) and 'silos' (eg technology, treasury, operations, quality management and compliance). A common language is needed to cut through the layers and break down the silos. Conversely, without a common language, the risk management team will spend too much time resolving communication issues at the expense of their primary responsibilities.

Risk information on an intranet

Risk information can be made available to stakeholders by a variety of means. Many organizations produce brief guides and leaflets for stakeholders to communicate the current risk issues and concerns. The appropriate means of communication will vary according to the nature of the stakeholder and the nature and complexity of the message to be communicated.

Formal means of risk communication exist where the organization has to report to financial stakeholders. When risk communication is required, a range of communication techniques can be used. A formal report to the stock exchange or to other financial stakeholders may be backed up by an informal video, slide presentation and/or a telephone conference call, as appropriate.

There is often an additional means of risk communication available to organizations. Many organizations have developed an intranet for use by staff and this can be used to cover risk and risk management information. For many large organizations, it is common for the intranet to be used to communicate health and safety information and business continuity plans.

Information can be provided on the intranet about the generic risk assessments that have been undertaken and the control measures that have been identified. The intranet can also be used to communicate urgent risk information, as well as providing updates on risk assessments, control measures and the current level of any particular risk.

Risk management information systems (RMIS)

The distribution of risk guidelines may be undertaken by way of a risk management information system (RMIS) software package. The RMIS could be placed on the intranet of the organization. The RMIS will also facilitate the collection and communication of risk information, including the reporting of events by local management as they occur. Typically, the RMIS could include a wide range of information, as summarized in Table 12.2.

RMIS have been used for some time to record details of insurance claims. In recent times, the use of a RMIS has become more sophisticated. It is now possible to record details of the risk exposure, risk control and risk action plans using such a software package. For RMIS that are used in connection with insurance, details of insurance policies, insurance claims procedures and insurance claims history can all be recorded and made available to authorized individuals. Such a system can also be used to pool risk exposure information and report accidents or other events that may lead to an insurance claim.

As well as information-recording RMIS systems, there are a number of software products that support risk management. These include software packages that can undertake various analytical processes and systems that can undertake risk analysis and dependency modelling reviews.

Table 12.2 Risk management information system (RMIS)

The following types of information may be handled, stored, managed, distributed and communicated using a risk management information system (RMIS):

- Risk management policy and protocols
- Risk profile data, values and information
- Emergency contact arrangements and contact details
- Insurance values and cost of risk data
- Insurance claims handling and management protocols
- Historical loss/claims experience/information
- Insurance policy coverage and other information
- Risk management action plans (risk register)
- Risk improvement plans and implementation
- Business continuity plans and responsibilities
- Disaster recovery plans and responsibilities
- Corporate governance arrangements and reports

It is generally accepted that the application of a RMIS software tool to an enterprise risk management (ERM) initiative can be very helpful. However, the disadvantage that is often encountered is that entering a substantial amount of risk data onto a computer database can be very time consuming. However, the benefits of having the data available for detailed analysis can make the effort worthwhile.

Risk information needs to be shared throughout an organization to enhance risk awareness and ensure improved risk performance. It is almost always the case that individuals within an organization will have the best understanding of the risks, as well as detailed practical knowledge of the actions that should be taken to mitigate risk events. Communication is also important to share information about incidents that have occurred, including lessons that were learnt and the actions that were taken to ensure that the event is not repeated.

An analysis of the advantages and disadvantages of RMIS are set out in the box below. In general, RMIS become more valuable when the risks are complex or the amount of data that needs to be recorded is substantial.

Risk management information system (RMIS)

Without more advanced RMIS technology, risk managers are limited to recording the exposure data and loss experience of the company relevant to the ERM initiative, using techniques like modelling and Monte Carlo simulations.

It is possible that the cost of developing a robust, ERM-supportive RMIS will exceed the benefits. The costs are immediate and tangible; the benefit is difficult to estimate or demonstrate. Risk managers already struggle with how to explain the value of a loss that is prevented or financed. Even if the risk reduction is significant, it is a potential future benefit, not an assured, immediate expense reduction.

Whether the risk assessments from RMIS are likely to lead to enough marginal benefits to offset the cost of data tracking and analysis depends on the risk profile of the company. Large firms stand to gain the most from RMIS, but as the cost of the computing tools needed to collect data and perform the sophisticated modelling continue to decrease, the benefits grow for all organizations.

Ultimately, RMIS may pay for itself by enabling an organization to avoid or effectively finance that one catastrophic loss that would otherwise slash the financial results of the company.

Consistent response to risk

One of the main reasons for communicating risk information and providing risk training is to ensure that a consistent response to similar risk events is always achieved. This can only be ensured by sharing information and experience. A consistent response is required in relation to hazard, control and opportunity risks. When an organization has an intranet, this is an ideal way of achieving a consistent response to risk by ensuring that appropriate information is readily available.

As well as a consistent response to individual risks, consistent risk protocols also need to be defined and communicated. Part of ensuring a consistent response to risk is to identify risks in advance and confirm the controls that will be in place for them. This approach is relevant to strategic, project and operational risks, and training and communication protocols should be introduced to increase the consistency of response to risk across the organization.

It should be a requirement of every organization that a risk assessment is attached to each capital expenditure request. This risk assessment should include both the risks that the project is seeking to manage and the risks within the project itself. The risks within the project may affect the ability to deliver the project on time, within budget and to specification.

Risk assessment attached to strategic analysis is also a vitally important issue and is part of ensuring a consistent response to risk. Production of an 'issues manual' as a means of communicating risk across the organization and ensuring a consistent response to risks may also be valuable. The issues manual will identify risks, circumstances and other events where a response is required. The provision of adequate information, supervision and training will ensure that consistent and appropriate risk management procedures are more likely to be followed.

Case study

Tesco – risk management responsibilities

Accepting that risk is an inherent part of doing business, our risk management systems are designed both to encourage entrepreneurial spirit and also provide assurance that risk is fully understood and managed. The Board has overall responsibility for risk management and internal control within the context of achieving the Group's objectives. Executive management is responsible for implementing and maintaining the necessary control systems. The role of Internal Audit is to monitor the overall internal control systems and report on their effectiveness to Executive management, as well as to the Audit Committee.

Key to delivering effective risk management is ensuring our people have a good understanding of the Group's strategy and our policies, procedures, values and expected performance. We have a structured internal communications programme that provides employees with a clear definition of the Group's purpose and goals, accountabilities and the scope of permitted activities for each business unit, as well as individual line managers and other employees.

We operate a balanced scorecard approach that is known within the Group as our Steering Wheel. This unites the Group's resources around our customers, people, operations, community and finance. The scorecard operates at every level within the Group, from ground level business units, through to country level operations. It enables the business to be operated and monitored on a balanced basis with due regard for all stakeholders.

The Group maintains a Key Risk Register. The Register contains the key risks faced by the Group including their impact and likelihood as well as the controls and procedures implemented to mitigate these risks. The content of the Register is determined through regular discussions with senior management and review by the Executive Committee and the full Board.

The risk management process is cascaded through the Group with every international CEO and local Boards maintaining their own risk registers and assessing their control systems.

The same process also applies functionally in those parts of the Group requiring greater overview. For example, the Audit Committee's Terms of Reference require it to oversee the Finance Risk Register. We also have a Corporate Responsibility Risk Register which specifically considers Social, Ethical and Environmental (SEE) risks. Oversight of these risks is the responsibility of the Corporate Responsibility Committee.

Annual Report and Financial Statements 2009

Part 3

Risk assessment

Learning outcomes for Part 3

- describe the importance of risk assessment as a critically important stage in the risk management process;
- outline the range of risk assessment techniques that are available and the advantages/disadvantages of each technique;
- describe the importance of risk classification systems and describe the key features of the best-established systems;
- provide examples of the use of a risk matrix, including using it to indicate the dominant risk response in each quadrant;
- use a risk matrix to indicate the risk appetite of an organization and whether the organization is risk averse or risk aggressive;
- describe the main components of loss control as loss prevention, damage limitation and cost containment and provide practical examples;
- demonstrate the use of loss-control actions to reduce the impact of an event that has a large magnitude before mitigation;

- outline the alternative approaches to defining upside of risk and the practical application of these approaches for strategy, projects and operations;
- outline the importance of business continuity planning and disaster recovery planning and provide practical examples;
- describe the approach taken during a business impact analysis and how the analysis supports business continuity planning;
- describe the key features of a business continuity plan, as set out in established business continuity standards, such as BS 25999.

Part 3 Further reading

British Standard BS 25999–1 (2006) Business continuity management Code of practice, www.standardsuk.com.

HM Treasury (2004) Orange Book: Management of risk – principles and concepts, www.hm-treasury.gov.uk.

International Standard IEC/FDIS 31010 (2009) Risk Management – Risk assessment techniques, www.iso.org.

Management Consultancies Association (2007) The upside of risk, www.mca.org.uk.

United States Government (2004) Every business should have a plan, www.ready.gov.

13
Risk assessment considerations

Importance of risk assessment

Risk recognition and risk rating together form the risk assessment component of the risk management process. Risk assessment involves the recognition of risks and the rating of them to determine the significant risks facing the organization, project or strategy. It is defined in British Standard BS 31100 as the overall process of risk identification, risk analysis and risk evaluation. Because the risk management input into strategy focuses on improved decision making, risk assessment is the main risk management input into strategy formulation.

Risks may be attached to corporate objectives, stakeholder expectations, core processes and key dependencies. Whichever of these features is selected as the starting point, risk assessment can be undertaken. The purpose of risk assessment is to identify the significant risks that could impact the selected feature.

Although risk assessment is vitally important, it is only useful if the conclusions of the assessment are used to inform decisions and/or to identify the appropriate risk responses for the type of risk under consideration. It should be considered as the starting point of the risk management process and it is certainly not an end in itself.

An important feature of undertaking a risk assessment is to decide whether the identified risk is going to be evaluated at the inherent level or at the current (or residual) level. Assessment of inherent risk is undertaken without taking account of the controls that are currently in place. This is the approach recommended by internal auditors, and ISO 31000 states that risk assessment should be undertaken at inherent and at residual level.

The benefit of undertaking assessment of inherent risk is that the difference between the current level and the inherent level can be identified. This will give an indication of the importance of the existing control measures and information is used by internal auditors to help identify critical controls and set audit priorities. Although this may be a useful approach, there can be considerable difficulties in identifying the value of the inherent level of risk.

Health and safety practitioners, for example, prefer to undertake risk assessment with the current controls in place. This can be a simpler process, although it relies on the assumption that the current controls will always work to the assumed effectiveness. For example, if an assessment of an x-ray machine is being undertaken, the safety person will assume that the enclosure or cabinet is in good order and the risk should be assessed on that basis. The internal auditor will more easily recognize that the enclosure or cabinet is a vitally important control factor that has to be subject to a routine inspection.

Approaches to risk assessment

There are several approaches that can be taken when planning how to undertake risk assessment. One of the key decisions will be who to involve in the risk assessment exercise. Sometimes risk assessments are undertaken by the board of directors as a top-down exercise. Risk assessments can also be undertaken by involving individual members of staff and local departmental management. This bottom-up approach is also valuable.

The opinion of the chief executive officer (CEO) is critically important, especially as it helps to define the overall attitude of the organization to risk. There is no doubt that the CEO will be able to provide a well-structured view of the significant risks faced by the organization. The disadvantage in relying on the opinion of the CEO is that the focus is likely to be on external risks. Although CEOs will be concerned about the financial management and infrastructure risks, these internal risks may not be their major concern or area of interest.

In general, the overall approach by the organization to risk assessments will be heavily influenced by the risk assessment techniques that are selected. Certain techniques require the involvement of specific individuals and require a particular approach to undertaking risk assessments. It is important that the approach that is adopted is consistent with the culture of the organization.

For example, if an organization does not normally hold meetings and workshops, then a workshop may not be the most appropriate approach to risk assessments. Likewise, if the culture of the organization relies heavily on reports and written papers, this may be the best way of conducting the risk assessments.

The use of voting software has become popular in recent times. For organizations such as media companies familiar with this technology, this may be a very appropriate way of undertaking risk assessments. However, for organizations that are not keen on technology, then the use of such tools may be seen as gimmicks that detract from the value of the workshop.

The use of the voting software can provide additional information in the risk assessment workshop. Not only is it possible to identify the majority position in relation to the likelihood and impact of a risk materializing, but it is also possible to identify the spread of opinions. If there

is a broad spread of opinions, this needs to be explored, because it could represent a possible misunderstanding of the nature of the risk being discussed.

Risk assessment techniques

There are a wide range of risk assessment techniques available and a Final Draft International Standard (FDIS) has recently been published providing detailed information on the full range of risk assessments techniques that can be used. Table 13.1 lists the main risk assessment techniques that are in common use and also provides a brief description of each of these techniques. Probably the most common risk assessment approaches are the use of checklists/questionnaires and the use of brainstorming sessions, normally during risk assessment workshops.

Table 13.1 Techniques for risk assessment

Technique	Brief description
Questionnaires and checklists	Use of structured questionnaires and checklists to collect information that will assist with the recognition of the significant risks
Workshops and brainstorming	Collection and sharing of ideas at workshops to discuss the events that could impact the objectives, core processes or key dependencies
Inspections and audits	Physical inspections of premises and activities and audits of compliance with established systems and procedures
Flowcharts and dependency analysis	Analysis of the processes and operations within the organization to identify critical components that are key to success
HAZOP and FMEA approaches	Hazard and operability studies and failure modes effects analysis are quantitative technical failure analysis techniques
SWOT and PESTLE analysis	Strengths, weaknesses, opportunities, threats (SWOT) and political, economic, social, technological, legal, environmental (PESTLE) analyses offer structured approaches to risk identification

Checklists and questionnaires have the advantage that they are usually simple to complete and are less time-consuming than other risk assessment techniques. However, this approach suffers from the disadvantage that any risk not referenced by appropriate questions may not be recognized as significant. A simple analysis of the advantages and disadvantages of each of the most common risk assessment techniques is set out in Table 13.2.

Table 13.2 Advantages and disadvantages of RA techniques

Technique	Advantages	Disadvantages
Questionnaires and checklists	• Consistent structure guarantees consistency • Greater involvement than in a workshop	• Rigid approach may result in some risks being missed • Questions will be based on historical knowledge
Workshops and brainstorming	• Consolidated opinions from all interested parties • Greater interaction produces more ideas	• Senior management tends to dominate • Issues will be missed if incorrect people involved
Inspections and audits	• Physical evidence forms the basis of opinion • Audit approach results in good structure	• Inspections are most suitable for hazard risks • Audit approach tends to focus on historical experience
Flowcharts and dependency analysis	• Useful output that may be used elsewhere • Analysis produces better understanding of processes	• Difficult to use for strategic risks • May be very detailed and time consuming
HAZOP and FMEA approaches	• Structured approach so that no risks are omitted • Involvement of a wide range of personnel	• Most easily applied to manufacturing operations • Very analytical and time-consuming approach
SWOT and PESTLE analysis	• Well-established techniques with proven results • SWOT analysis can be linked to strategic decisions	• Focused approach that may miss some categories of risk • Rigid structure restricts imaginative thinking

Given that risks can be attached to other aspects of an organization as well as or instead of objectives, a convenient and simple way of analysing risks is to identify the key dependencies faced by the organization. Most people within an organization will be able to identify the aspects of the business that are fundamentally important to its future success. Identifying the factors that are required for success will give rise to a list of the key dependencies for the organization.

Key dependencies can then be further analysed by asking what could impact each of them. If a hazard analysis is being undertaken then the question is: 'What could undermine each of these key dependencies?' If control risks are being identified, then the question can be asked: 'What would cause uncertainty about these key dependencies?' For an opportunity risk analysis, the question would be: 'What events or circumstances would enhance the status of each of the key dependencies?'

For many organizations, quantification of risk exposure is essential and the risk assessment technique that is chosen must be capable of delivering the required quantification. Quantification is particularly important for financial institutions and the style of risk management employed in these organizations is frequently referred to as operational risk management (ORM).

Risk workshops are probably the most common of the risk assessment techniques. Brainstorming during workshops enables opinions regarding the significant risks faced by the organization to be shared. A common view and understanding of each risk is achieved. However, the disadvantage can be that the more senior people in the room may dominate the conversation, and contradicting their opinions may be difficult and unwelcome.

Risk matrix

When a risk has been recognized as significant, the organization needs to rate that risk, so that the priority significant risks can be identified. Techniques for ranking risks are well established, but there is also a need to decide what scope exists for further improving control. Consideration of the scope for further cost-effective improvement is an additional consideration that assists the clear identification of the priority significant risks.

There are many different styles of risk matrix. The most common form of a risk matrix is one that demonstrates the relationship between the likelihood of the risk materializing and the impact of the event should the risk materialize. As well as likelihood and impact, other features of the risk can be represented on the risk map. For example, the scope for achieving further risk improvement is often represented using a risk map. In this case, the risk map will demonstrate the level of risk, in relation to the additional measures that can be taken to improve the management of that risk and thereby set a target level for it.

A risk is significant if it could have an impact in excess of the benchmark test for significance for that type of risk. Identification of potentially significant risks will be undertaken during a risk ranking exercise. It is necessary to decide the:

- magnitude of the event should the risk materialize;
- size of the impact that the event would have on the organization;
- likelihood of the risk materializing at or above the benchmark;
- scope for further improvement in control.

This will lead to the clear identification of the priority significant risks. Most organizations will find that the total number of risks identified in a workshop is between 100 and 200. After the risk rating has been completed, it is typical for the number of priority significant risks faced by the organization to be identified as between 10 and 20.

Risk perception

When undertaking risk assessment exercises, it is often the case that different attendees at the workshop will have different views of the risk. There are several ways of accommodating differing opinions. In some cases, voting software can be used in order to identify the majority view. This has the benefit that it is a simple means of identifying the average group position, at the same time as demonstrating the spread of opinions.

However, it is often beneficial to discuss why people have different views of a risk. By exploring why their views differ, it is often possible to reach an agreed common position. This will have the benefit that more appropriate control measures will then be identified and implemented.

Different views on the importance of a risk can be present at different levels of seniority within the organization. It is useful for the risk assessment process to draw opinions from all levels of management, so that different perspectives of a risk can be identified. Again, the benefits of this approach are better risk communication, fuller risk understanding and the identification of appropriate and practical control measures.

In order to understand the risks facing an organization and be able to undertake an accurate risk assessment, extensive knowledge of the organization is required. To complete an accurate risk assessment that correctly identifies the significant risks and then goes on to identify the critical controls is a time-consuming and resource-intensive exercise.

In relation to the public perception of risk, members of the public often only have access to incomplete information and are subject to strong arguments from lobbying and other special interest groups. Therefore, the public understanding and perception of risk may not be sufficiently informed or entirely objective. Journalists and news reporters have a duty to present news stories in an objective and unbiased manner, which may not be easy when the people

receiving the information do not have a full understanding of the risks involved. The BBC has produced advice for journalists when reporting on the matters concerned with risk:

> *Research carried out by BBC journalists indicated concern amongst scientific experts about the potential of media coverage to distort risk and create disproportionate fear. Using the following checklist can help ensure the context is clear and avoid distortion of the risk.*
>
> - *What exactly is the risk, how big is it, and who does it affect?*
> - *Can the audience judge the significance of any statistics or other research?*
> - *If you are reporting a change in the level of risk, have you clearly stated the baseline figure?*
> - *Is it more appropriate and measured to ask 'How safe is this?', rather than 'Is this 100 per cent safe?'?*
> - *If a contributor's view runs contrary to majority expert opinion, is that clear in our report, questions and casting of any discussion?*
> - *Have you considered the impact on public perceptions of risk if we feature emotional pictures and personal testimony?*
> - *Is there an everyday comparison that may make the size of the reported risk easier to understand?*
> - *Would information about comparative risks help the audience to put the risk in context and make properly informed choices?*
> - *Can the audience be given sources of further information?*

Risk appetite

Risk appetite is a vitally important concept in the practice of risk management. However, it is a very difficult concept to precisely define and apply in practice. Figure 13.1 provides an empirical illustration of risk appetite using a standard risk matrix. These figures illustrate the acceptability to the organization of different levels of risk. Figure 13.1 represents the risk appetite of a risk-averse organization.

Figure 13.2 illustrates a more risk-aggressive attitude. The organization represented in this figure has a greater risk appetite, simply because it has a more aggressive attitude to risk. By adopting a more aggressive attitude to risk, the organization will have fewer risks in the concerned zone. In this case, the 'universe of risk' for the organization will be very restricted.

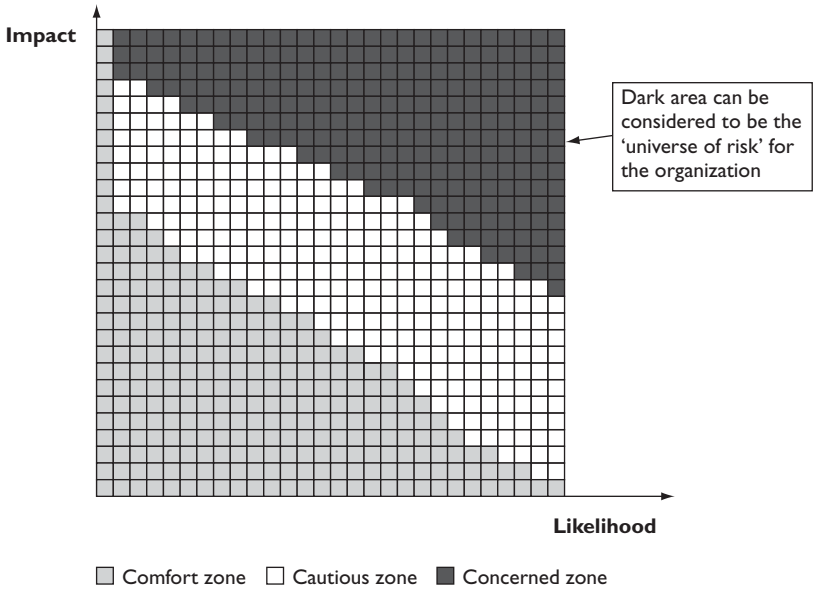


Figure 13.1 Risk appetite matrix (risk averse)

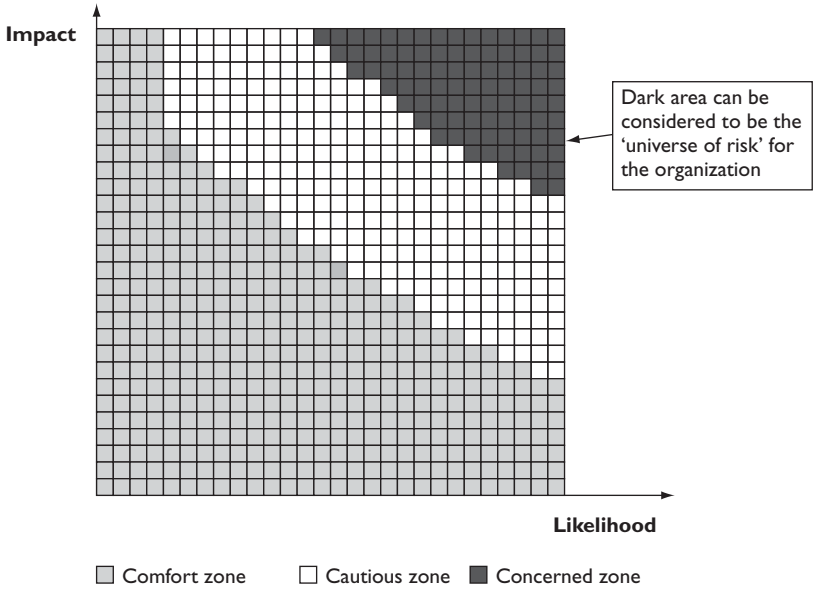


Figure 13.2 Risk appetite matrix (risk aggressive)

The dark area in each figure represents the risks that will be of concern to the organization. For a risk-aggressive organization, there are fewer risks of concern, so that the 'universe of risk' considered by the board will be very restricted. 'Universe of risk' is a phrase often used

by internal auditors to identify audit priorities. Working with such a closed or restricted universe of risk will increase the chances of an unidentified significant risk impacting the organization.

Both Figure 13.1 and Figure 13.2 illustrate that there will be a level of risk that the organization feels comfortable taking. This is because, regardless of the likelihood of the risk materializing, the impact is so small that it would not be significant if it did materialize. Likewise, there will be a likelihood of a risk materializing that is considered so remote that it is assumed that it will not occur, even though it would be very serious if it did. For example, most organizations do not consider the consequences of a jumbo jet crash landing on their site.

The global financial crisis is an example of circumstances where certain risks were considered so unlikely to occur that they could be ignored. Some banks were reliant on the wholesale money markets, but the possibility of these markets failing was considered to be too remote to require further analysis or to call for the development of contingency plans to respond to that situation.

Above these minimum levels of tolerable likelihood and impact, a range of risks can arise. Generally speaking, low likelihood/low impact risks will be tolerable, medium likelihood/medium impact risks will require some judgement before acceptance, and high likelihood/high impact risks will be intolerable.

Organizations will need to take a risk-by-risk approach when deciding whether a risk is acceptable. Different organizations will set tolerance levels differently and this will be an indication of risk appetite. Many organizations will take a cumulative review of risk where all risk exposures are added together, and this is a feature of the enterprise risk management approach. The organization will then be able to decide whether the overall exposure to risk is acceptable and within the risk appetite of the organization.

One of the fundamental difficulties with the concept of risk appetite is that, generally speaking, organizations will have an appetite to continue a particular operation, embark on a project or embrace a strategy, rather than a direct appetite for the risk itself. In other words, risk appetite and risk exposure should be considered as a consequence of business decisions rather than a driver of those decisions. The decision on risk appetite is normally taken within the context of other business decisions, rather than as a stand-alone decision. The standard advice in most risk management standards is that risk should not be managed out of context, so questions about the risk appetite can only be answered within the context of the strategy, project or operational activity that is being considered.

When considering risk perception and risk appetite, it is worth reflecting on the fact that certain individuals may be more concerned about a low-impact risk with a high probability of occurrence (such as a car crash) than they will about a high-impact risk that is unlikely to happen (such as an earthquake). This difference in approach is often reflected in the risk assessment process and can affect the way in which significant risks are prioritized.

When all the potentially significant risks have been identified, one approach is to ask how likely it is that each of those risks will materialize above the threshold test for significance. The risks can then be prioritized as high likelihood, medium likelihood and low likelihood. The alternative approach is to prioritize the potentially significant risks in order of the impact at the same likelihood. The risks will then be presented as high impact, medium impact and low impact.

There is a difference in approach and perception in these approaches. The first approach is based on concern about how likely it is that the risk will be significant while the second approach is based on concern about how much the risk would impact when it happens. Neither of these approaches is better than the other and it is a matter of risk appetite and risk perception as to which approach an individual board member (or the collective board itself) may prefer.

Buying a car

As an example that brings together the ideas of risk appetite and hazard, control and opportunity risks, consider the decision to buy a car. When deciding which car to buy, there is a need to evaluate hazard tolerance and acceptance of uncertainty, as well as the sum of money that will be invested in the opportunity of owning a new vehicle. Together, these components represent the risk appetite to buy and run a car. In order to achieve an upside of taking the risk of buying a car, the benefits obtained must exceed the costs involved.

If undertaking a risk-based evaluation of buying a car is to help with the decision-making process, the intended benefits of car ownership should be established. This is equivalent to identifying the objectives associated with car ownership.

The actual financial capacity and ability to run a car also needs to be considered. When buying a new vehicle, the buyer needs to make sure that the vehicle selected will not expose the buyer to more risk and cost more than anticipated. The risks that are associated with owning a vehicle include insurance, breakdown, repairs, accidents, servicing costs and insurance, as well as the purchase price and the anticipated annual depreciation.

Assume that the decision has been taken to buy a two-year-old prestigious car. The car will cost much less money than a new vehicle and the depreciation costs will be much less (opportunity risks). However, the repair and maintenance costs may be higher than for a new vehicle (control risks). The exposure to accidents, theft and repair costs will be similar for most vehicles (hazard risks).

Remember that the opportunity risks enhance the possible achievement of the benefits of owning a car. The control risks increase uncertainty or doubt about achieving these benefits and the hazard risks inhibit the achievement of the car ownership benefits.

14
Risk classification systems

Short, medium and long-term risks

Although it is not a formalized system, the classification of risks into short, medium and long term helps to identify risks as being related (primarily) to operations, tactics and strategy, respectively. This distinction is not clear-cut, but it can assist with further classification of risks. In fact, there will be some short-term risks to strategic core processes and there may be some medium-term and long-term risks that could impact operational core processes.

A short-term risk has the ability to impact the objectives, key dependencies and core processes, with the impact being immediate. These risks can cause disruption to operations immediately at the time the event occurs. Short-term risks are predominantly hazard risks, although this is not always the case. These risks are normally associated with unplanned disruptive events, but may also be associated with cost control in the organization. Short-term risks usually impact the ability of the organization to maintain efficient core processes that are concerned with the continuity and monitoring of routine operations.

A medium-term risk has the ability to impact the organization following a (short) delay after the event occurs. Typically, the impact of a medium-term risk would not be apparent immediately, but would be apparent within months, or at most a year after the event. Medium-term risks usually impact the ability of the organization to maintain effective core processes that are concerned with the management of tactics, projects and other change programmes. These medium-term risks are often associated with projects, tactics, enhancements, developments, product launch and the like.

A long-term risk has the ability to impact the organization some time after the event occurs. Typically, the impact could occur between one and five years (or more) after the event. Long-term risks usually impact the ability of the organization to maintain the core processes that are concerned with the development and delivery of efficacious strategy. These risks are related to strategy, but they should not be treated as being exclusively associated with opportunity

management. Risks that have the potential to undermine strategy and the successful implementation of strategy can destroy more value than risks to operations and tactics.

Purpose of risk classification systems

In order to identify all of the risks facing an organization, a structure for risk identification is required. Formalized risk classification systems enable the organization to identify where similar risks exist within the organization. Classification of risks also enables the organization to identify who should be responsible for setting strategy for management of related or similar risks. Also, appropriate classification of risks will enable the organization to better identify the risk appetite, risk capacity and total risk exposure in relation to each risk, group of similar risks or generic type of risk.

The FIRM risk scorecard provides such a structure, but there are many risk classification systems available. The FIRM risk scorecard builds on the different aspects of risk, including timescale of impact, nature of impact, whether the risk is hazard, control or opportunity, and the overall risk exposure and risk capacity of the organization. The headings of the FIRM scorecard provide for the classification of risks as being primarily Financial, Infrastructure, Reputational or Marketplace in nature.

The FIRM risk scorecard can also be used as a template for the identification of corporate objectives, stakeholder expectations and, most importantly, key dependencies. The scorecard is an important addition to the currently available risk management tools and techniques. It is compiled by analysing the way in which each risk could impact the key dependencies that support each core process. Use of the FIRM risk scorecard facilitates robust risk assessment by ensuring that the chances of failing to identify a significant risk are much reduced.

As with so many risk management decisions, it is for the organization to decide which risk classification system most fully satisfies its needs and requirements. As well as being classified according to the timescale of their impact, risks can also be grouped according to the nature of the risk, the source of the risk and/or the nature of the impact.

Examples of risk classification systems

Table 14.1 provides a summary of the main risk classification systems. These are the COSO, IRM standard, BS31100, FIRM risk scorecard and PESTLE. There are similarities in most of these systems, although PESTLE takes a slightly different approach. It should be noted that identifying risks as: 1) hazard, control or opportunity; 2) high, medium or low; and 3) short term, medium term and long term should not be considered to be formal risk classification systems.

Table 14.1 Risk classification systems

Standard or framework	COSO	IRM	BS 31100	FIRM Risk Scorecard	PESTLE
Classification headings	Strategic Operations Reporting Compliance	Financial Strategic Operational Hazard	Strategic Programme Project Financial Operational	Financial Infrastructure Reputational Marketplace	Political Economic Sociological Technological Legal Environmental

There are similarities in the way that risks are classified by the different risk classification systems. However, there are also differences, including the fact that operational risk is referred to as infrastructure risk in the FIRM risk scorecard. COSO takes a narrow view of financial risk, with particular emphasis on reporting. The different systems have been devised in different circumstances and by different organizations; therefore, the categories will be similar but not identical.

British Standard BS 31100 sets out the advantages of having a risk classification system. These benefits include helping to define the scope of risk management in the organization, providing a structure and framework for risk identification, and giving the opportunity to aggregate similar kinds of risks across the whole organization.

The British Standard states that the number and type of risk categories employed should be selected to suit the size, purpose, nature, complexity and context of the organization. The categories should also reflect the maturity of risk management within the organization. Perhaps the most commonly used risk classification systems are those offered by the COSO ERM framework and by the IRM risk management standard.

However, the COSO risk classification system is not always helpful and it contains several weaknesses. For example, strategic risks may also be present in operations and in reporting and compliance. Despite these weaknesses, the COSO framework is in widespread use, because it is the recognized and recommended approach for compliance with the requirements of the Sarbanes–Oxley Act.

The reporting component of the COSO internal control framework is specifically concerned with the accuracy of the reporting of financial data and is designed to fulfil the requirements of section 404 of the Sarbanes–Oxley Act. It is worth noting that the COSO ERM framework

(2004) is the broader version of COSO, and it also includes the requirements of the COSO Internal Control framework (1992).

FIRM risk scorecard

The four headings of the FIRM risk scorecard offer a classification system for the risks to the key dependencies in the organization. The classification system also reflects the idea that 'every organization should be concerned about its finances, infrastructure, reputation and commercial success'. In order to give a broader scope to commercial success, the headings of the FIRM risk scorecard are as follows:

F Financial;

I Infrastructure;

R Reputational;

M Marketplace.

The features of the FIRM risk scorecard are set out in Table 14.2. Financial and infrastructure risks are considered to be internal to the organization, while reputational and marketplace risks are external to the organization. Also, financial and marketplace risks can be easily quantified in financial terms, whereas infrastructure and reputational risks are more difficult to quantify.

The inclusion of reputational risks as a separate category of risk in the FIRM risk scorecard is not universally accepted. It is sometimes argued that damage to reputation is a consequence of other risks materializing and should not be considered as a separate risk category. However, if a broader view of risk is taken, it becomes obvious that reputation is vitally important. This is particularly important when organizations are seeking to use their brand name to enter additional markets, or achieve 'brand stretch' as it is sometimes called.

In any case, there is a broader argument that all risks are a consequence of the broader business decisions. Adopting a particular strategy, undertaking a project and/or continuing with the established operations all involve risks. If the organization did not undertake these strategic, change or operational activities, risks would not be present.

Table 14.2 Attributes of the FIRM risk scorecard

	Financial	Infrastructure	Reputational	Marketplace
Description	Risks that can impact the way in which money is managed and profitability is achieved	Risks that will impact the level of efficiency and dysfunction within the core processes	Risks that will impact desire of customers to deal or trade and level of customer retention	Risks that will impact the level of customer trade or expenditure and customer retention
Internal or external risk	Internal	Internal	External	External
Quantifiable	Usually	Sometimes	Not always	Yes
Measurement (performance indicator)	Gains and losses from internal financial control	Level of efficiency in processes and operations	Nature of publicity and effectiveness of marketing profile	Income from commercial and market activities
Performance gap	**Procedures** Failure of procedures to control internal financial risks	**Process** Failure of processes to operate without dysfunction	**Perception** Failure to achieve the desired perception of the organization	**Presence** Failure to achieve required presence in the marketplace
Control mechanisms	• CapEx standards • Internal control • Delegation of authority	• Process control • Loss control • Insurance and risk financing	• Marketing • Advertising • Reputation and brand protection	• Strategic and business plans • Opportunity assessment

PESTLE risk classification system

Table 14.3 provides an outline of the PESTLE risk classification system. PESTLE is an acronym that stands for political, economic, sociological, technological, legal and environmental risks.

In some versions of the approach, the final E is used to indicate ethical considerations (including environmental). This risk classification system is most applicable to the analysis of hazard risks and is less easy to apply to financial, infrastructure and reputational risks.

The PESTLE risk classification system is often seen as most relevant to the analysis of external risks. External risk in this context is intended to refer to the external context that is not wholly within the control of the organization, but where action can be taken to mitigate the risks. It is often suggested that the PESTLE risk classification system should be used in conjunction with an analysis of the strengths, weaknesses, opportunities and threats (SWOT) facing the organization. A SWOT analysis of each of the six PESTLE categories is recommended by the 'Orange Book'.

The advantage of the PESTLE risk classification system is that it provides a clear analysis of the issues that should be addressed within the external context. The PESTLE approach may be most applicable in the public sector, because the external factors analysed by the PESTLE approach are particularly relevant.

Table 14.3 PESTLE classification system

Category of risk	Description
Political	tax policy, employment laws, environmental regulations, trade restrictions and reform, tariffs and political stability.
Economic	economic growth/decline, interest rates, exchange rates and inflation rate, wage rates, minimum wage, working hours, unemployment (local and national), credit availability, cost of living, etc.
Sociological	cultural norms and expectations, health consciousness, population growth rate, age distribution, career attitudes, emphasis on safety, global warming.
Technological	technology changes that impact your products or services, new technologies, barriers to entry in given markets, financial decisions like outsourcing and supply chain.
Legal	changes to legislation may impact employment, access to materials, quotas, resources, imports/exports, taxation etc.
Environmental	ecological and environmental aspects, although many of these factors will be economic or social in nature.

Advantages and disadvantages of a PESTLE analysis

Advantages of a PESTLE analysis are as follows:

- simple framework;
- facilitates an understanding of the wider business environment;
- encourages the development of external and strategic thinking;
- enables an organization to anticipate future business threats and take action to avoid or minimize their impact;
- enables an organization to spot business opportunities and exploit them fully.

Disadvantages of a PESTLE analysis are as follows:

- some users over-simplify the amount of data used for decisions;
- needs to be undertaken on a regular basis to be effective;
- requires different people being involved, each having a different perspective;
- access to quality external data sources can be time consuming and costly;
- pace of change makes it increasingly difficult to anticipate developments that may affect an organization in the future;
- risk of capturing too much data is that it may make it difficult to see priorities;
- can be based on assumptions that subsequently prove to be unfounded.

Hazard, control and opportunity risks

Categorizing risks according to a single risk classification system is not always helpful. It may not be sufficient to simply understand the timescale of impact, especially when the nature of the impact is more important. It is for this reason that there will always be difficulties with a simple system for categorizing risks. It is for each organization to identify the risk classification system(s) that suits its particular needs and the nature of the risks facing the organization.

Risks need to be classified according to the source or impact as well as being classified according to the timescale of the impact. Therefore, a combination of the FIRM risk scorecard and the classification of risks as hazard, control and opportunity risks is required in order to provide a complete picture.

It is possible to design a personal risk matrix that classifies risks according to the FIRM risk scorecard and also classifies risks according to whether they are short term, medium term or long term. This will provide an issues grid that will assist with the identification of all possible

significant risks, using a format that can be easily understood. An example of a completed grid is set out in Table 14.4, which presents the issues that could face an individual, so that the risks can be identified.

Table 14.4 Personal issues grid

Dependency	Long term	Medium term	Short term
Financial risks	Procedures gap: How well do your procedures manage your finances?		
1. Investments	Pension arrangements Property purchase	Share purchase Business opportunities	Betting habits Insurance arrangements
2. Expenditure	Accommodation Holiday pattern	Car purchase Rail season ticket Credit card ownership	Shopping behaviour Travel arrangements
Infrastructure risks	Process gap: How well does your body facilitate your processes?		
3. Health	Family history Personal lifestyle Vegetarianism	Medical treatment Dieting Weight gain	Exercise Alcohol and drugs Illness or accident
4. Emotional	Marriage and children Ethnic origins Sexuality	Friendships Cosmetic surgery	Hobbies Sex
Reputational risks	Perception gap: How are you perceived by your peer group?		
5. Personal	Personality Neighbourhood Criminal behaviour	Mood and temperament Charity work	Clothes Personal hygiene Charity donations
6. Professional	Intelligence Behaviour patterns	Qualifications Redundancy Changing jobs	Attending training Continuous learning
Marketplace risks	Presence gap: What is your presence in the marketplace?		
7. Occupation	Career selection Education	Society memberships Presenting training	Society activities
8. Income	Ambition Seniority	Extra part-time work Sale of shares	Selling possessions Casual work

Table 14.4 illustrates the balance of operational, project and strategic issues for each of the four headings of the FIRM risk scorecard. It can be seen that hazard risks are closely related to infrastructure issues and strategic risks are more likely to arise in relation to issues concerned with the marketplace.

The risk classification systems discussed in this chapter are most easily applied to the analysis of hazard risks, except that the IRM Standard and the COSO framework offer strategic risk as a separate risk category. It will be for an organization to decide whether a category of strategic risks is helpful and necessary. The FIRM risk scorecard offers a means of classifying strategic and project risks according to the main impact associated with the risk, should it materialize.

As with other core processes in an organization, classification of risks facing projects is essential, so that the appropriate response to each risk can be identified. Given that the requirements of any project are that it should be delivered on time, within budget and to specification, these components offer a means of classifying project risks. Separate lists could be devised of risks that threaten the timescale, risks that threaten the budget and risks that will affect the final specification, performance or quality of the project outcome.

15
Risk likelihood and impact

Application of a risk matrix

Table 14.4 (page 138) set out the range of issues that could be faced by an individual. Using this 'issues grid', individuals would be able to identify the priority significant risks that they face. These risks are illustrated in the risk matrix shown in Figure 15.1. Having placed the various risks on a risk matrix, the relative importance of the risks can easily be identified. An overall view can then be taken as to whether the risk profile (or risk exposure) is within acceptable limits and within the risk appetite and risk capacity of the individual.

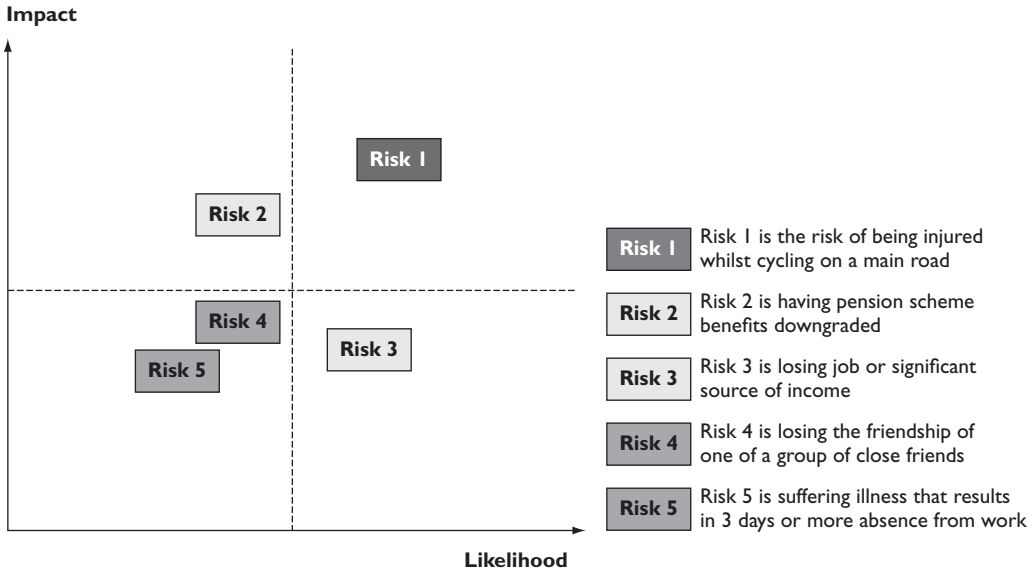


Figure 15.1 Personal risk matrix

Large organizations frequently make use of a risk matrix as a means of summarizing their risk profile. The risk matrix is very useful and can be used for a range of applications. It can also be used to identify the type of risk response that is most likely to be employed. Figure 15.2 illustrates the occasions when each of the responses tolerate, treat, transfer and terminate are most likely to be employed for the current level of risk.

Impact is not the same as magnitude, because a risk may have a high magnitude in terms of the size of the event, but the impact may be smaller. For example, a road transport company may suffer the complete loss of one of its vehicles but, depending on the exact circumstances, this may have a very small overall impact on the business. This will be especially true if the company did not have sufficient work to fully utilize the type of vehicle involved in the loss.

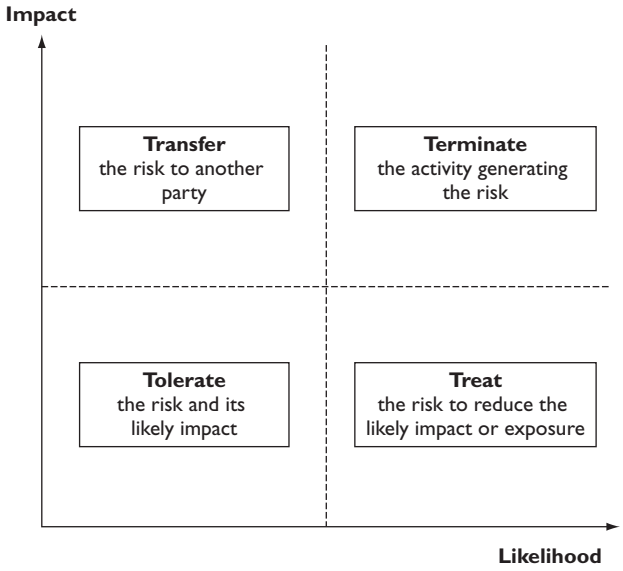


Figure 15.2 Risk matrix and the 4Ts of hazard management

Inherent and current level of risk

Many risk management practitioners assess risk at its current (also referred to as residual) level. However, internal auditors prefer to undertake an assessment of the risk at its inherent level. As discussed in Chapter 13, there are advantages in considering the inherent level of a risk when undertaking a risk assessment. Considering the inherent level will enable the effect of individual control measures to be identified. Figure 15.3 illustrates the effect of controls on the level of risk. Control 1 reduces the risk from the inherent level to an intermediate level and it can be seen that this control has its main effect on the likelihood of the risk materializing.

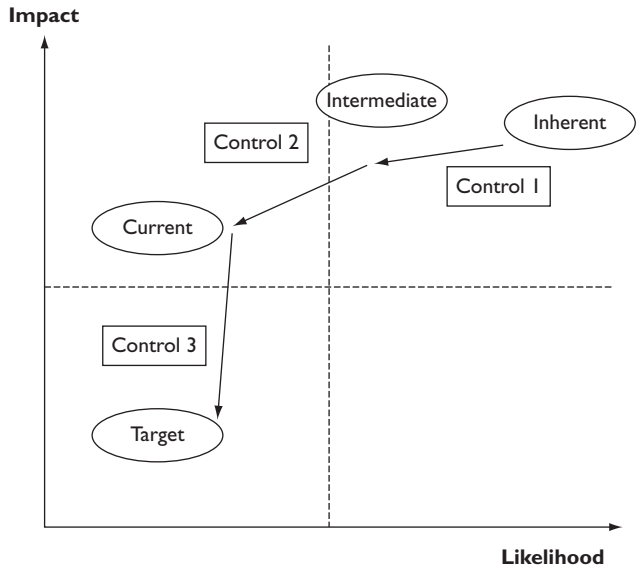


Figure 15.3 Inherent, current and target levels of risk

Control 2 in Figure 15.3 also has a beneficial effect on the level of the hazard risk illustrated in this diagram. The main effect of Control 2 is to reduce the likelihood of the risk materializing, but there is also some benefit in terms of a reduced impact. Control 3 has a significant effect on the impact of the risk, but little effect on the likelihood of it materializing.

There are three levels of risk that are important on the risk matrix shown in Figure 15.3. The inherent or gross level is the level of risk that would be present if there were no controls in place. The current level is the level at which the risk exists at the time of the risk assessment, when Controls 1 and 2 only are in place. This is often referred to as the residual level of risk. The problem with describing the current level as the residual level is that there is an implication that the level of risk is static and that the organization cannot take any further risk mitigation action.

Use of the phrase 'current level' gives a much more dynamic feel to the risk management process and so the phrase is used throughout this book. However, the level of risk that is of interest to risk managers is the target level. This is illustrated in Figure 15.3 by the introduction of Control 3. Control 3 will reduce the impact of the risk, so that the target level of risk is within the bottom left-hand quadrant of the risk map, or the tolerate/comfort zone.

Control confidence

The intended effect of an individual control measure is illustrated in Figure 15.3. It is not possible for an organization to be absolutely confident that controls will always be fully implemented and will be as effective as expected or required. Controls will need to be audited in order to be confident that the control selected has been properly designed and implemented and is producing the desired effect.

The level of control confidence can also be illustrated on a risk matrix. If the effectiveness of a control is uncertain, a greater variability of the outcome may be expected. This can be demonstrated on a risk matrix by using a circle or ellipse to represent a risk, instead of representing the risk as a single point on the risk matrix. By doing this, the level of uncertainty or variability in the outcome can be illustrated both in relation to the likelihood and impact of the event to materializing.

An important consideration when undertaking a risk assessment and when evaluating the effectiveness of risk management in general, and risk control measures in particular, is the level of confidence that should be placed on a particular control. Two questions need to be asked: 'How confident are we that this is the correct control?' and 'How confident are we that it is fully implemented and effective in practice?' When there is limited confidence in the effectiveness of a control, it will be the role of internal audit to test the control and provide information on the likely level of variability of outcome, should the risk materialize.

It is the responsibility of internal auditors to check that the correct controls have been selected and that they are working correctly in practice. Internal auditors refer to effective and efficient controls respectively when reviewing these points. Undertaking the testing of controls is a key function fulfilled by internal audit and the importance of the testing of controls should also be recognized by risk management practitioners.

Management needs to receive assurance of adequate control and this can come from internal audit activities, or measurement of the outputs of processes and projects, as well as from management reports. The responsibility for designing and implementing controls and auditing the effectiveness and efficiency of controls should be allocated within the risk management documentation.

4Ts of risk response

Figure 4.2 (page 44) provided a diagram of the risk management process. This diagram set out the stages of the risk management process in relation to the management of hazard risks. The options presented for risk response can be described as the 4Ts of hazard management, and these are tolerate, treat, transfer and terminate.

It is possible to illustrate the 4Ts of risk response on a simple risk matrix and this is done in Figure 15.2 (page 141). This diagram suggests that in each of the four quadrants of the risk matrix, one of the 4Ts will be dominant. Tolerate will be the main response for the low likelihood/low impact risks. Treat will be the dominant response for high likelihood/low impact risks. Transfer will be the dominant response for high impact/low likelihood risks and terminate will be the dominant response for high impact/high likelihood risks.

Figure 15.2 provides a simple graphical representation of the dominant risk response in each of the four quadrants of a simple risk matrix. The corresponding responses for control and opportunity risks will be considered in a later part of this book as the 4As and 4Es respectively. It is important to note that these responses are represented as the dominant or most likely response in each quadrant.

Different and/or additional responses may be appropriate, depending on the circumstances. For example, if high impact/high likelihood risks are embedded within mission-critical activities, they may be unavoidable. In this case, it will not be possible for the organization to terminate those risks.

A difficulty in presenting such a simple risk map showing the 4Ts of risk response is that they meet in the centre. Clearly, it cannot be as simple as suggested, because a small change in the likelihood and impact of a risk could take it from the terminate quadrant into the tolerate quadrant. A slightly modified approach that makes this analysis somewhat more realistic is considered in a later part.

Risk significance

When undertaking a risk assessment, it is quite common to identify a hundred or more risks that could impact the objective, core process or key dependency that is being considered. This is an unmanageable number of risks and so a means is required to reduce the number that will be considered to be priority issues for management.

So that an organization can concentrate on significant risks, a test for risk significance is required. Table 15.1 provides suggestions on the nature of the benchmark tests that could be used to decide whether a risk is significant. For risks that will have a financial or commercial impact, the benchmark test is likely to be based on monetary value. For risks that could disrupt the infrastructure or routine operations of the organization, a benchmark test based on the impact, cost and duration of disruption is appropriate. For reputational risks, the most likely benchmark will be based on the adverse publicity that would result if the risk materializes.

This may vary according to the nature of the risk and whether it is a financial or non-financial one. For large organizations, identifying a financial test for significance can be undertaken in a number of ways. Many organizations will have authorization procedures for spending

Table 15.1 Benchmark tests for risk significance

FIRM risk scorecard	Typical benchmark test for significance
Financial	• Impact on balance sheet of 0.25% • Profit and loss impact of 2.5% annual profit
Infrastructure	• Disruption to normal operations of ½ day • Increased cost of operation exceeds 10% budget
Reputational	• Share price falls by 10% • Event is on national TV, radio or newspapers
Marketplace	• Impact on balance sheet of 0.5% turnover • Profit and loss impact of 1% annual profit

money, and so the test for risk significance should be compatible with the authorization levels that are often set out in a formal document referred to as a 'delegation of authority'.

For a large organization, it may be the case that full board approval is required for expenditure in excess of a particular financial threshold. This is an indication of the sum of money that is considered significant by the organization. Other tests include a percentage of the profit or a percentage of the value of the balance sheet (or reserves) of the organization. Typically, 2.5 per cent of the annual profit or 0.25 per cent of Balance Sheet or 0.5 per cent of annual turnover are appropriate tests for significance.

Financial limits can be used to test whether a risk is significant in relation to financial and marketplace risk segments of the FIRM Risk Scorecard. For infrastructure and reputational segments, identifying a benchmark test for significance may be more difficult. One test of significance for infrastructure risks is to ask whether the risk would disrupt normal operations for more than (say) half a day. For reputational risks, the test for significance may be to determine how the event would be reported. A report on the front page of the local newspaper or in the national press may be an indication that a risk should be considered to be significant.

For an organization, it is possible that the external auditors might indicate that a sum of £1m/$1m would be considered to be a material sum when compiling the accounts of the organization. This would offer a benchmark to the management of the company to use that amount as the benchmark test of significance. Applying this test during a risk assessment workshop could reduce the number of risks for further consideration to about 20. The next stage would be to identify how likely each of the 20 potentially significant risks would be to materialize at or above the financial threshold level. A risk matrix could be used to record and display the results.

Risk capacity

There are several aspects that are important when an organization is deciding how much risk to take. Different approaches will be taken for different types of risks. Hazard risks will give rise to a hazard tolerance, control risks will give rise to a control acceptance and opportunity risks will give rise to an investment appetite. Overall, the organization will have a total risk exposure. This is the sum of the total risk that the organization has taken in these three categories.

Risk exposure is the actual risk that the organization is taking and this may not be the same as the risk appetite that the board believes is appropriate for the organization. There is also another important measure of risk, and that is the risk capacity of the organization. This is a measure of how much risk the organization should take or can afford to take.

In simple terms, the risk appetite of the board should be within the risk capacity of the organization and greater than or equal to the actual risk exposure that the organization faces. A contributing factor to the global financial crisis was that certain financial institutions were exposed to a level of risk beyond the risk-bearing capacity of that organization.

It would be inappropriate for an organization to embark on a project that could exhaust all of the resources of the organization. The capacity of the organization to accept risk will depend on the financial strength of the organization, the robustness of its infrastructure, the strength of its reputation and brands and the competitive nature of the marketplace in which it operates.

The more rapidly the marketplace is changing, the greater capacity for risk the organization is required to have available. For example, if an organization is facing a significant change in technology, the strategic options may be limited. Consider an organization that is involved in the manufacture of CD players when it becomes obvious that MP3 technology is taking over. The organization will be faced with a significant risk related to the change in technology and will need to develop a new business model. It will have to acquire new production equipment, new skills and new distribution patterns. It may be that the transfer to the new technology and the risks that it involves are outside the resources and risk capacity of the organization. If that is the case, the organization may need to explore strategic options, including seeking a joint-venture partner, locating a buyer for the business or simply withdrawing from the marketplace.

The box below provides a real example of the consequences of the global financial crisis. This financial institution discovered that the risk exposure faced by the organization was greater than its risk capacity. Having acknowledged that situation, the financial institution then released a statement to shareholders.

Risk capacity

Risk capacity is the level of risk the bank considers itself capable of absorbing, based on its earnings power, without damage to its dividend paying ability, its strategic plans and, ultimately, its reputation and ongoing business viability. It is based on a combination of budgeted, forecast and historical revenues and costs, adjusted for variable compensation, dividends and related taxes.

Risk exposure is an estimate of potential loss based on current and prospective risk positions across major risk categories – primary risks, operational risk and business risk. It builds as far as possible on the statistical loss measures used in the day-to-day operating controls. Correlations are taken into account when aggregating potential losses from risk positions in various risk categories to obtain an overall estimate of the risk exposure. The risk exposure is assessed against a severe but plausible constellation of events over a one-year time horizon to a 95 per cent confidence level or a 'once in 20 years' event.

Risk appetite is established by the board that set an upper boundary on aggregate risk exposure. A comparison of risk exposure with risk capacity serves as a basis for determining if current or proposed risk limits are appropriate. It is one of the tools available to management to guide decisions on adjustments to the risk profile.

The risk exposure should not normally exceed risk capacity but in the recent extremely difficult market conditions, this relationship has not held. The bank recorded a large net loss, showing that the risk exposures remained greater than its risk capacity. Risk exposure remained high as a result of a lack of liquidity in the markets for securitized assets and due to significantly increased volatility levels in global markets. The reduction in risk exposure that was achieved through sales in addition to the significant writedowns incurred on risk positions was offset by a simultaneous decrease of risk capacity due to downward revisions of earnings expectations as a consequence of the deteriorating economic outlook.

16
Loss control

Risk likelihood

Risk likelihood can also be described as risk frequency. However, using the phrase risk frequency assumes that the risk occurs on a regular basis. The more general term risk likelihood is used throughout this book. Risk likelihood can be determined on an inherent basis for any particular risk, or can be determined at the current level of risk, paying regard to the control measures that are in place.

For hazard risks, previous history may be a good indication of how likely the risk is to occur. For a fleet of motor vehicles, there is certain to be a history of vehicle accidents and breakdowns. Controls will be in place to reduce the likelihood of these events. A road haulage company should assess the likelihood of vehicle breakdowns on an inherent basis and also on the basis of current controls. There are, however, difficulties in assessing the inherent likelihood of vehicle accidents, because certain assumptions would have to be taken about what effect the removal of controls would have on the likelihood of accidents.

Even if an assessment of the breakdown likelihood at the inherent level cannot be undertaken, the company will still need to determine the importance of the vehicle maintenance programme in preventing vehicle breakdowns and whether the maintenance activities provide value for money. In relation to vehicle accidents, the company may have driver training processes in place and, again, the effectiveness of these processes can be determined by evaluating inherent and current levels of risk. Whether levels of risk are evaluated at inherent or at current level, there is no doubt that benchmarking the performance of the fleet against the average performance of the industry will be a useful exercise.

An example of a control measure that has an effect on the magnitude of the risk but may have no effect on its likelihood is the use of seat belts in cars. In simple terms, the driver wears a seat belt to reduce the impact of an accident, because the seat belt has no effect on the likelihood of an accident occurring. The driver wears the seat belt as a control measure for when the accident happens.

A sports club will wish to reduce the chances of a key player being absent. The absence may be caused by inappropriate behaviour by a player, resulting in the need for sanctions against that person. Accordingly, the club may decide to introduce a 'code of behaviour' for senior players, and this would include a commitment by each player to follow an appropriate healthy lifestyle. Failure to comply with the code of behaviour would result in financial and other punishments.

The club may also decide that additional controls were required to reduce player absence, including fitness monitoring and social support for overseas players who had recently moved to the country to join the team. It may also be agreed that an attempt should be made to place contractual limits on the ability of national teams to call on its overseas players. These actions will be taken in addition to other loss-control activities, such as excellent medical facilities to provide immediate medical care and reduce the damage when an injury occurs. Also, the company may purchase insurance to protect itself against the financial losses associated with the absence of a player.

Risk magnitude

Reducing the magnitude of a hazard risk is very important. For hazard risks, magnitude is often referred to as severity of the risk should it materialize. Reduction in hazard risk severity will be achieved by reducing the overall impact or consequences when the adverse event occurs. The seat belt in a car can reduce the consequences of an accident, but has no effect on the likelihood of having an accident.

It is possible for a serious fire to occur that results in a considerable amount of property damage and is considered to be very severe and expensive. However, in reducing the severity of a serious fire, the requirement is to reduce the impact of the fire on the organization. Actions to reduce impact will concentrate on damage limitation at the time of the fire and cost containment after the event.

Damage limitation is also an important feature of reputational risk management. When a serious incident occurs that attracts public attention, an organization will need to be able to protect its reputation by reassuring stakeholders that the organization responded appropriately to the event. It is almost invariably the case that the CEO or chairman of the company will arrive at the scene when there has been a serious train or plane crash.

There have been examples where a serious incident has occurred and the management of the media by the organization has been very poor. In these cases, it is likely that inadequate attention was paid to pre-incident planning, so that the damage to the reputation of the organization was not effectively minimized at the time the incident occurred.

Organizations will also need to be concerned with cost containment. Cost containment following an event is usually based on the business continuity plan (BCP) or disaster recovery plan (DRP) that the organization put in place before the incident occurred. The development of effective BCP and DRP will put the organization in the best position to ensure that the overall cost of the incident is kept as low as possible.

Hazard risks

The range of hazard risks where reducing the magnitude of the adverse event is important will include fraud, health and safety, property protection and efficient operation of IT systems, as well as incidents with the potential to cause damage to reputation. Table 16.1 provides a list of the key dependencies, using the structure of the FIRM risk scorecard, which could give rise to hazard risks. When hazard risks materialize, actions need to be taken to reduce the magnitude of the event, as well as limit the impact.

Table 16.1 Generic key dependencies

FIRM risk scorecard	Example dependencies
Financial	• Availability of funds/finance • Correct allocation of funds/finance • Internal control (fraud) • Liabilities under control (bad debts and pensions)
Infrastructure	• People skills and experience • Premises/plant and equipment • IT hardware and software • Communications and transport
Reputational	• Brand and brand expansion • Public opinion of sector • Regulators enforcement action • Corporate social responsibility
Marketplace	• Regulatory requirements • Health of world or national economy • Product development (technology) • Competitor behaviour

Although the main focus of managing hazard risks will be on loss prevention, successful management of hazard risks must also include consideration of damage limitation and cost containment. There is a developing trend in the insurance market towards settling claims in a more efficient and cost-effective manner. This trend is partly based on encouraging organizations to get back to normal operation as soon as possible. Indeed, some insurance companies refer to initiatives of this type as cost containment.

As mentioned previously, reducing the severity of an incident should be seen as part of an overall attempt to implement loss control in an organization. An integrated approach to loss control is important because it will enable the organization to control both the likelihood and impact when a hazard risk materializes. In fact, loss control should be considered to be loss prevention plus damage limitation plus cost containment.

Although the most important component of loss control is loss prevention, hazard risks can materialize despite the best efforts of organizations. Adequate assessment of hazard risks is vital, so that appropriate pre-planning of post-loss actions can be undertaken. Plans should be in place to ensure that the damage caused by the incident is kept to a minimum and the cost consequences of the event are also tightly controlled and contained.

Loss prevention

Loss prevention is concerned with preventing the losses occurring or, at least, reducing the likelihood of losses occurring. Damage limitation is concerned with reducing the amount of damage that occurs when the hazard event materializes. For example, if a fire occurs the fire doors and fire shutters will reduce the extent of damage. Cost containment is concerned with minimizing the impact of the loss on an organization by ensuring that costs associated with the adverse hazard event are reduced to a minimum.

Techniques for loss prevention will vary according to the type of hazard risk that is being considered. For health and safety risks, loss prevention is related to eliminating the activity completely or ensuring that, for example, hazardous chemicals are not used in processes.

For risks to buildings, loss-prevention techniques involve such controls as the elimination of sources of ignition and the control, containment and segregation of flammable or combustible materials. Loss-prevention techniques will also include restrictions on smoking and other actions taken to reduce hazardous behaviours by persons using the buildings.

For fraud and theft risks, loss-prevention techniques will include separation of responsibilities and security tagging of expensive items. Fraud prevention techniques may also involve pre-employment screening. A more detailed consideration of fraud prevention is set out in a later Part of this book.

Damage limitation

Damage limitation in relation to fire hazards is well established. Although sprinkler systems are often considered to be a loss-prevention measure, they are, in fact, the major control measure for ensuring that only limited damage occurs when a fire breaks out. Other damage-limitation factors related to fire include the use of fire segregation within buildings, the use of fire shutters and well-rehearsed arrangements in place to remove, segregate or otherwise protect valuable items.

Accidents at work still occur, despite the considerable attention paid to health and safety standards and other loss-prevention activities. Provision of adequate first aid arrangements is an obvious damage-limitation activity and suitable first aid facilities are provided by most organizations. For some high-risk factory occupancies, medical facilities are provided on site.

In some cases, these medical facilities will include specialist treatment facilities related to the particular hazards on site. An example is the provision of cyanide antidotes in factories where chromium plating activities take place using cyanide plating solutions. A simpler example is the provision of emergency eye wash bottles in locations where hazardous chemicals are handled.

Cost containment

When a hazard risk materializes, despite the efforts put into loss prevention and the efforts that have been put into damage limitation, there may well still be a need to contain the cost of the event. For example, among the activities for minimizing costs associated with serious fires are detailed arrangements for salvage and arrangements for decontamination of specialist items that have suffered water or smoke damage.

Cost containment in relation to a fire will also include arrangements for specialist recovery services. The actions that will be taken to ensure that post-incident costs are minimized should all be set out in a business continuity plan. The topics of business continuity planning and disaster recovery planning are considered in more detail in another Part of this book.

A further consideration relevant to cost containment after an incident is what insurance companies referred to as 'increased cost of operation'. Most material damage/business interruption insurance policies will allow for payment of increased cost of operation. This may arise when an organization has to sub-contract certain production activities, or has to undertake manufacturing work at another one of its factories, which may be located some distance away.

If a manufacturer discovers that faulty goods have been released into the marketplace, a number of actions become necessary. The organization should have developed plans in

advance of the event occurring for notifying customers of the fact that faulty goods are in the marketplace and how to identify them. The box below considers the importance of product recall in these circumstances.

Product recall risk management

Any company or organization that manufactures, assembles, processes, wholesales, or retails products could be financially impacted by the direct or indirect costs of a product recall. Direct costs can include wages for staff who have to implement the recall plan. Other direct costs include communications and this could entail purchasing air time on radio and television and notices in newspapers or industry publications.

Indirect costs can include lost production time for staff who must focus on the recall process, as well as the hiring of temporary employees to assure continued production. However, the greatest indirect cost is the impact that adverse publicity could have on market share of the market. A product recall should be designed to:

- protect the customer from bodily injury or property damage;
- remove the product from the market and from production;
- comply with specific regulatory requirements;
- protect the assets of the company.

17
Defining the upside of risk

Upside of risk

Defining the upside of risk is one of the greatest challenges for risk management. The overall contribution of risk management is to help deliver compliance, assurance, as well as enhanced decision making and efficiency/effectiveness/efficacy (CADE3). However, there is a desire amongst risk management practitioners to identify a more dynamic range of benefits that can be delivered by successful risk management.

A range of interpretations of the upside of risk is possible and some of these are offered in Table 17.1. There is a belief amongst risk management practitioners that risk management makes a significant contribution to the operation of the organization, and this contribution is often described as the upside of risk. In simple terms, the upside of risk is achieved when the benefits obtained from taking the risk are greater than any benefit that would have resulted from not taking it. In other words, the organization has received an overall benefit from undertaking the activities that resulted in exposure to the risk or set of risks involved.

At its most simplistic, the upside of risk in relation to hazard management is that there is less downside. Good standards of risk management will ensure that there is less potential for disruption to normal, efficient, routine operations. However, it is clearly not sufficient to say that the upside of risk is simply that there would be less downside. A more proactive interpretation of the upside of risk is when an organization realizes that solving a particular risk-based problem has brought a benefit, rather than a cost.

For example, a manufacturing company that produces waste by-products that create a disposal problem may achieve the upside of risk by selling that unwanted by-product or identifying a means of adding value to the waste product and selling it as another product stream. This is an example of identifying a difficulty for the business and, in solving that difficulty, acquiring additional benefits that had not been foreseen and were not otherwise available.

Table 17.1 Upside of risk

- Fewer disruptions to normal operations and greater operational efficiency resulting in less downside of risk
- Ability to seize an opportunity denied to competitors because a better-informed view of the management of risk is taken
- Deliberately identifying events that will be positive during the risk assessment and deciding how to manage those events
- Opportunity management, whereby a detailed evaluation is undertaken of new business opportunities before deciding to take the opportunity
- Achieving a positive outcome from a situation that could have gone wrong without good judgement/risk management
- Achieving compliance/risk assurance in difficult circumstances as an unintended/automatic consequence of good risk management

Another interpretation of the upside of risk is that the risk assessment workshop should also focus on identifying risks that have an upside outcome. The risk assessment workshop would therefore address questions like: 'What events would create a better outcome than expected?' A register of positive outcome risks can then be identified and actions can be taken to make those upside risks more likely to occur or have more beneficial consequences when they do materialize.

A more satisfactory explanation of the upside of risk is that the organization will be able to undertake activities that it would not otherwise have the appetite to undertake. In a commercial sense, this is enabling an organization to seize a business opportunity that a competitor does not have the appetite to take, or considers to be too risky. This may be because of the greater efficiency within the organization, or because a cost-effective means of changing the organization by a development project has been identified that the competitor failed to see. On a strategic level, this upside of risk may arise from the organization identifying a means of targeting the business opportunity, but only the profitable component of that business opportunity.

Another way of looking at the upside of risk is to reflect on a business venture that turned out successfully in circumstances where failure could have been foreseen. This is a somewhat retrospective approach based on the analysis 'that could have gone wrong, but it did not and therefore we have enjoyed the upside of taking that risk.' This approach to the upside of risk depends on the organization being willing to pursue a risky venture, albeit with adequate controls in place, that leads to a positive outcome in circumstances where a competitor may not have been willing to take the risk.

Finally, there is the analysis of the upside of risk that reflects on the benefits of having a robust risk management process. Achieving the CADE3 benefits, especially benefits related

to compliance, may be considered to be a sufficient reason for undertaking a risk management initiative. In these circumstances, certain organizations may consider that achieving compliance is an upside of risk.

Opportunity assessment

Successfully embracing business opportunities is more likely to be achieved if the organization undertakes opportunity assessments. Many consultancy firms undertake a detailed evaluation of each new business prospect. The organization will look at the new business prospect and evaluate the scope for a profitable partnership, opportunities to earn extra income and the reputational benefits that might arise from having that potential client as a customer.

Opportunity assessment can be undertaken in relation to new business ventures, as well as new clients. This opportunity evaluation is designed to identify the additional business opportunities that could arise from winning that client business. The evaluation will also look at the potential disadvantages of successfully acquiring the client prospect. When undertaking such an opportunity assessment, there has to be the possibility that the organization will advise the client prospect that they do not wish to tender for the business.

Consider the options for a theatre that discovers that fewer people are coming to performances and decides to look at the opportunities to take more money from those who continue to attend. The options may include general improvement to the catering facilities within the theatre and the provision of organic produce. Additionally, there is the possibility of selling merchandise themed to the particular performance.

As well as looking at increased revenue during performances, the theatre may also look at sponsorship arrangements and open dialogue with local businesses to discover what type of production would be most likely to gain local support and sponsorship. In future, part of the assessment of any proposed new production could include an evaluation of the level of sponsorship that might be available. As well as generating greater income, this approach could also enable the theatre to stage productions that otherwise would have been considered too risky.

Many organizations already practise opportunity management, although it may not be seen explicitly as a risk management approach. Ideally, opportunity management should be embedded into work processes for developing and implementing strategy and/or taking advantage of business opportunities. Some organizations do not have explicit opportunity management procedures for the evaluation of new business prospects, or for the evaluation of merger/acquisition opportunities.

Riskiness index

The risk profile of an organization can be represented in many ways. The most common method used is to prepare a risk register that contains details of the significant risks faced by the organization. However, a disadvantage of the risk register is that it is usually a qualitative evaluation of individual risks. Organizations need to develop a means of measuring, evaluating and quantifying the total risk exposure of the organization.

One of the features of the enterprise risk management approach is to develop the consolidated view of the risk exposure of the organization. The approach based on calculating the total risk exposure of an organization is similar to the approach taken to the measurement of risk in operational risk management.

This Part introduces the idea of a 'riskiness index'. The idea is to present a semi-quantitative approach that takes a snapshot of the overall level of risk embedded in the organization. The overall level of risk will pay regard to the strategy currently being followed by the organization, the projects that are in progress, and the nature of the routine operations being undertaken.

Table 17.2 presents a set of questions that can be used to develop a riskiness index for an organization. The table uses the structure of the FIRM risk scorecard as a means of categorizing risks. By using the riskiness index, it should be possible for an organization to identify the level of risk faced by its finances, infrastructure, reputation and the level of risk that it faces in the marketplace.

Having completed the riskiness index, the organization can then seek additional controls to reduce the level of risk. The main focus of risk management is then simply to reduce the level of riskiness within the organization without affecting the strategy, project or operations of the organization. The upside of risk then becomes that the organization can follow the desired strategy, projects and operations at the lowest level of risk that is reasonably and cost-effectively achievable.

It will then be for the board of the company to decide whether the level of risk identified by the riskiness index analysis is aligned with the risk appetite of the board and within the risk capacity of the organization. The level of risk identified by the riskiness index represents the risk exposure of the organization. The board can then compare this level of risk exposure with the risk capacity of the organization and the appetite of the board towards risk.

Table 17.2 Riskiness index

Allocate a score of between 0 and 5 to each component of the generic example of the FIRM risk scorecard to determine the level of risk within the organization, project, operation or location being evaluated.

Financial component of the FIRM Risk Scorecard		
Index	Description	Score
1.1	Lack of availability (or unacceptable cost) of adequate funds to fulfil the strategic plans	
1.2	Insufficiently robust procedures for correct allocation of funds for strategic investment	
1.3	Inadequate internal financial control environment to prevent fraud and control credit risks	
1.4	Inadequate funds to meet historical liabilities (including pensions) and meet future anticipated liabilities	
TOTAL for the financial component		

Infrastructure component of the FIRM Risk Scorecard		
Index	Description	Score
2.1	Inadequate senior management structure to support organization and embed 'risk-aware culture'	
2.2	Insufficient people resources, skills and availability, including concerns about intellectual property	
2.3	Inadequate physical assets to support the operational and strategic aims of the organization	
2.4	Information technology (IT) infrastructure has insufficient resilience and/or data protection	
2.5	Business continuity plans are not sufficiently robust to ensure continuation of organization after major loss	
2.6	Product delivery, transport arrangements and/or communications infrastructure unreliable	
TOTAL for the infrastructure component		

Table 17.2 *continued*

Reputational component of the FIRM Risk Scorecard		
Index	Description	Score
3.1	Poor public perception of the industry sector and/or potential for damage to the brands of the organization	
3.2	Insufficient attention to ethics/corporate social responsibility/social environmental and ethical standards	
3.3	Poor governance standards and/or sector is highly regulated with high compliance expectations	
3.4	Concerns over quality of products or services and/or after sales service standards	
TOTAL for the reputational component		

Marketplace component of the FIRM Risk Scorecard		
Index	Description	Score
4.1	Insufficient revenue generation in the marketplace or inadequate return on investment achieved	
4.2	Highly competitive marketplace with aggressive competitors and high customer expectations	
4.3	Lack of economic stability, including exposure to interest rate fluctuations and foreign exchange rates	
4.4	Marketplace requires constant innovation and/or product technology is rapidly developing	
4.5	Supply chain is complex and lacks competition and/or raw materials costs are volatile	
4.6	Organization is exposed to potential for international disruption because of political risks, war, terrorism, crime or pandemic	
TOTAL for the marketplace component		

Table 17.2 *continued*

Score	Description of the level of risk	Score	Description of the level of risk
0	No risk	3	Medium risk
1	Little risk	4	High risk
2	Some risk	5	Extreme risk

Upside in strategy

Organizations will have a mission statement, together with a set of corporate objectives and an understanding of the expectations of the different stakeholders in the organization. The board of the organization then needs to develop an efficacious strategy that will deliver exactly what is expected in terms of the mission, objectives and expectations. In order to make correct strategic decisions, the board of the organization will need access to risk information. A risk assessment of the proposed strategy, together with a risk assessment of any viable alternative strategies, should be undertaken. The availability of this risk assessment information will ensure that the strategic decisions are more likely to be correct.

For opportunity risks, there is probably even less data available on which to predict risk likelihood. An organization may see an opportunity to acquire a new client or develop and market a new product. Accurate risk assessment of the likelihood of positive and negative events will be necessary in order to determine whether the new venture should go ahead. When a new product is launched, the requirement may well be to increase the likelihood of a positive event occurring. If a new product is being launched, then advertising and press coverage will need to be maximized up to the point that it remains cost-effective. Actions should therefore be taken to increase the level of media interest in the launch.

Strategic core processes bring the disciplines of strategic planning and risk management together. Strategic planning is a systematic process for obtaining a consensus at board level on the small number of issues that could have a massive effect on the long-term performance of the organization. Strategic issues are vitally important and failure to implement strategy or the selection of an inappropriate strategy can be amongst the most devastating risks to hit an organization. Implementation of strategy is usually achieved by way of projects and then ultimately delivered by operational core processes.

The box below describes an attitude to risk management that sees a risk as opportunity. This approach to the management of the organization demonstrates the desire to embrace the upside of risk.

Opportunity management

Most managers treat risk as an unwanted by-product of the business – something to be controlled whenever possible. That way of thinking stems from an overly simplistic view of risk. Some risks should be minimized, but others should be embraced in the drive for growth. Indeed, the pursuit of growth requires placing bets on specific products, customer segments, channels, company alliances and so on – all of which entail management of strategic risk. The most successful companies do not try simply to defend against bad risk events; they also define and predict the upside risks that, when well managed, can deliver the maximum rewards.

Upside in projects

It is essential that every organization adopts the correct core processes. A core process may be considered as the collection of activities that deliver a specific stakeholder expectation. This is the meaning of core process that is allocated by business process re-engineering (BPR) practitioners.

There is a difference between a process being efficient and effective. An efficient process means that there is no disruption and no excess cost. However, the process may be the incorrect one for cost-effectively delivering the requirements. Where processes need to be improved, a project will normally be undertaken and change achieved. In circumstances where a series of projects are required, this is often referred to as a programme of work. When a project, or programme of work, is implemented by an organization, the desire will normally be to improve the effectiveness of core processes.

By undertaking adequate risk assessment of the intended change, the organization should be able to ensure that the project is more successfully delivered on time, within budget and to specification. Achieving the upside of risk in the project or programme management requires that projects are adequately managed and that the correct project or priorities have been selected by the organization.

Often, organizations will undertake a post-implementation review to ensure that the benefits expected from the project have been delivered in practice. This review is often undertaken by internal audit and is designed to ensure that the project was delivered successfully, delivered the benefits that were required and was overall worthwhile. During difficult financial times, it is important that the organization selects projects that are not only successful, but represent the best possible allocation of limited resources when compared with alternative projects that have not been selected.

Upside in operations

It is a fundamental requirement for organizations that they have efficient operations. Efficient operations should make best use of the resources of the organization and should operate without unplanned disruption. Undertaking efficient operations that use minimum resources and produce maximum output will deliver the greatest benefit to the organization.

Risk management evaluation of operations can enable the organization to deliver the most efficient activities, operations and processes. By delivering the most efficient operations, a commercial organization can achieve benefits over a competitor and undertake work for a lower cost and still make a profit.

For public services, the delivery of efficient operations is equally important. Most public services have targets for delivery that can be complex and challenging. Failure to anticipate and manage risks appropriately can undermine the delivery of public services. The contribution of risk management will also help achieve sustained improvements in service by bringing flexibility and resilience to the way in which services are delivered. This contribution by risk management may be considered to be part of delivering the upside of risk.

In a competitive marketplace, achieving the upside of risk will often be to the detriment of competitors, suppliers or other third parties. The box below describes a situation whereby a restaurant company was able to take advantage of the market conditions during the global financial crisis.

Embracing opportunities

Consider two simple examples where the global financial crisis has resulted in benefit or upside risk for organizations. An international restaurant brand has discovered that landlords in city centre locations are looking for tenants. This has enabled the restaurant business to relocate into busier parts of a city centre at reduced rents, whilst also increasing trade and profits.

With the reduction in industrial activity resulting from the global financial crisis, an electricity generating company has been able to decommission old, costly generating facilities, and thereby reduce the overall cost per unit of producing electricity. This has increased profit per unit and enabled the company to revise strategic plans for future additional generating capacity to reduce generating costs over the long term.

18
Business continuity planning

Importance of BCP and DRP

There has been considerable interest in the subjects of business continuity planning (BCP) and disaster recovery planning (DRP) in recent times. Several standards have been published around the world. This illustrates the importance of BCP as an integral part of risk management. This increased concern has been reinforced by the potential for major disruption posed by extreme weather events, terrorist attacks, civil emergencies and the fear of a flu pandemic.

In simple terms, BCP is how an organization prepares for future incidents that could jeopardize its existence. The range of incidents that should be covered will include everything from local events like fires through to regional disruption such as earthquakes or national security incidents and extend to international events like terrorism and pandemics.

British Standard BS 31100 defines business continuity planning as a 'holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response to safeguard the interests of its key stakeholders, reputation, brand and value-creating activities'.

In case of a serious incident such as loss of access to premises or failure of a major part of an organization, it is important to have in place a well defined, documented and tested disaster recovery plan. Such plans inevitably focus on recovery of access to IT systems and data, but also commonly cover the provision of alternative premises (if needed) and other facilities, as well as setting out plans for communications with employees and with other stakeholders such as suppliers, customers and the media at a time of crisis.

Business continuity plans build upon this by setting out longer-term plans for restoration of 'business as usual' in the immediate aftermath of a disaster. A business continuity plan is an important part of reducing the impact of a hazard incident. The plan should include

arrangements for reducing the damage caused during the incident and containing the cost of recovery from it.

Disaster recovery plans are a particular component of business continuity planning. If a computer system fails to operate correctly or data has become corrupted, the organization will need emergency procedures to ensure that the data can be recovered and/or ensure that the organization continues in existence.

For a printing firm IT systems are fundamental to the operation of the company, because the computer systems process orders, schedule printing and manage invoicing. For such a company, it may be appropriate to arrange for a mobile emergency computer facility to be available in case of major IT failure. If this decision is taken, a contract should be set up with an outside company for a duplicate computer to be delivered in a trailer to the premises of the company. The duplicate computer would then be connected and the operations would be controlled from the duplicate computer in the trailer. The success of this arrangement will depend on the availability of information from backup disks that should be produced at least once per day and possibly several times per day.

Business continuity standards

The British Standards Institute has published a standard on business continuity management (BCM). This is BS 25999 Part 1 'Code of Practice – Business Continuity Management: 2006' and it provides a widely accepted overview of the key components of business continuity planning. The standard identifies a business continuity planning life cycle that has the following five components:

- understanding the organization;
- determining a BCM strategy;
- developing and implementing a BCM response;
- building and embedding a BCM culture;
- exercising, maintaining and reviewing.

There are many well-established approaches to business continuity planning, in addition to British Standard BS 25999, although most approaches are compatible with the requirements of this standard. Figure 18.1 provides a model for business continuity planning that is consistent with BS 25999.

Table 18.1 provides a checklist of the key activities involved in business continuity planning, which is recognized as a vital buy in most large organizations. Indeed, most governments take an active role in encouraging businesses (especially small businesses) to develop and implement adequate business continuity plans.

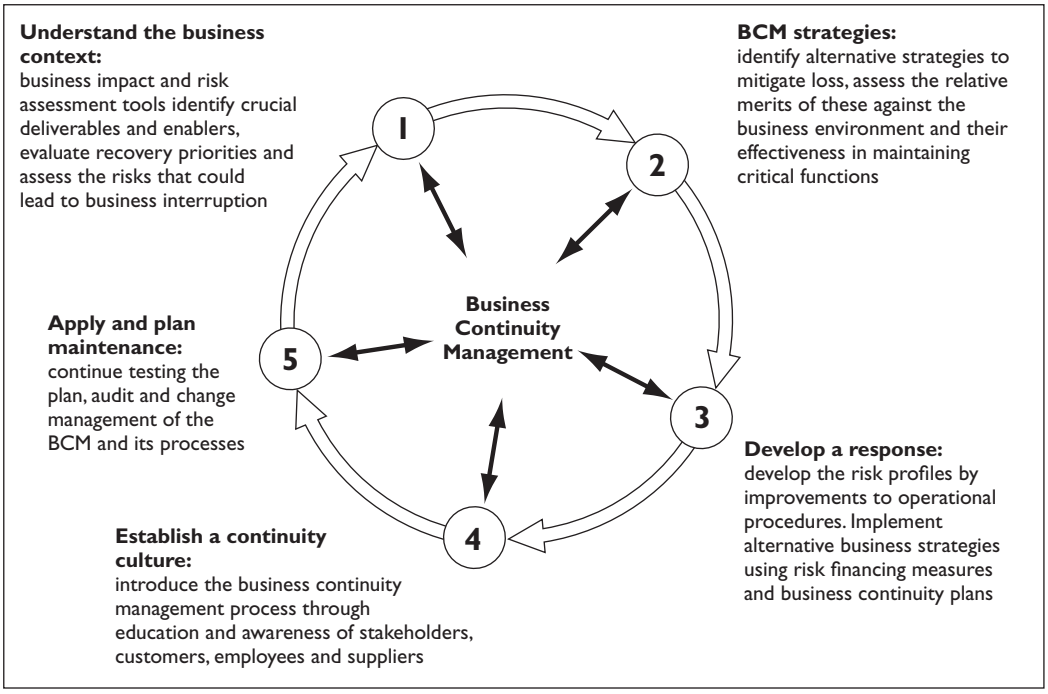


Figure 18.1 Model for business continuity planning

Table 18.1 Key activities in business continuity planning

1. Assess company activities to identify critical staff, materials, procedures and equipment required to keep the business operating
2. Identify suppliers, shippers, resources and other businesses that are contacted on a daily basis
3. Plan what to do if any important buildings, plant or store were to become inaccessible
4. Identify necessary actions to ensure continuity of critical business functions, especially payroll
5. Decide who should participate in compiling and subsequently testing the emergency plans
6. Define crisis management procedures and individual responsibilities for disaster recovery activities
7. Co-ordinate with others, including neighbours, utility suppliers, suppliers, shippers and key customers
8. Review the emergency plans annually and when the business changes and/or new members of staff are recruited

The overriding principles appropriate to successful business continuity planning are that the business continuity plan (BCP) should be:

- comprehensive;
- cost-effective;
- practical;
- effective;
- maintained;
- practised.

It is important that the BCP should cover all the operations and premises of the organization to ensure that the plan can facilitate a complete resumption of normal business operations. It is also important that the plan is cost-effective and proportionate to the risk exposures.

The BCP must be practical and easily understood by staff and others who are involved in the execution of the plan. Overall, the BCP must be effective in that it will recognize the urgency of certain business components or functions and identify responsibilities for ensuring timely resumption of normal work.

In order to guarantee that the BCP will be effective, it needs to be tested, maintained and practised. All members of staff need to be familiar with the intended operation of the plan and training will need to be provided. The lessons learnt during testing and practice of the business recovery plan should be incorporated into the plan so that it becomes more effective.

Testing of business continuity plans is an essential component of ensuring that they will be appropriate and effective. However, testing of plans can be time-consuming and, in some circumstances, disruptive and costly. Even the simple example of a fire evacuation drill from a building illustrates that the testing of procedures is inevitably going to disrupt normal routine operations.

Successful BCP and DRP

The first stage in successful business continuity planning and disaster recovery planning is to gain a thorough understanding of the organization and its interactions, both internal and external. Part of gaining this understanding will be to identify the objectives of the organization and its key dependencies. It is important to understand the critical functions within the organization and identify key resources.

Determining BCP strategy will require the identification of risks to the business and decisions about how likely it is that the risks will materialize. It is also necessary to understand the impact of risks on the business. These assessments should then be used to prioritize treatment of the risks and to agree the likelihood and impact of the risks materializing.

Developing and implementing a BCP and appropriate controls for each of the identified risks will require decisions on the appropriate risk responses. The range of risk responses available have already been discussed as the 4Ts of hazard management. In respect of each of the major risks, the decision will have to be taken whether to tolerate, treat, transfer or terminate the risk.

Building and embedding a business continuity management (BCM) culture will require good communication throughout the organization. All stakeholders will need to be engaged and involved in the process and will need to understand the reasons for the development of the BCP and DRP. The important role of all employees in the avoidance of incidents that could result in major disruption should be emphasized.

When developing the BCP, the mission-critical activities should be identified, together with key roles and responsibilities. These may be produced in the form of clear instructions and checklists. It is important to exercise, maintain and review the BCP by creating a programme to test the plans, review and amend them as necessary, and rehearse staff to improve understanding of the plans. BCP and DRP should be reviewed at least annually, as well as after a test of the plans. Also, if an incident occurs, the lessons learnt should be incorporated into the plans.

The flu pandemic of 2009 provides an example of the importance of business continuity planning. Advice and guidance was produced for companies and individuals in many countries around the world. The box below sets out a summary of the key points provided in that guidance and the practical implications of the flu pandemic for business continuity. In particular, it offers thoughts on 'coming to work sick' and 'staying at home well'.

Flu pandemic

Coming to work sick – People commonly are expected to come to work when they are sick and are often viewed poorly when they stay home with an illness. There are those who take advantage of sick-day policies, particularly when a fixed number of paid sick days is allowed. But when you have a disease where there is a lack of natural immunity, all it takes is one person to infect a department and that department could infect a company. If people don't feel well, they should stay home.

Staying home well – One of the ways to limit the spread of diseases is to avoid forcing a lot of people into the same small space. If a company has an outbreak, the people who weren't at work are likely to survive it and can keep the company running. This would suggest that work-at-home policies may help a company avoid the worst effects of the pandemic.

Business impact analysis (BIA)

A critical part of ensuring that adequate business continuity plans and disaster recovery plans are in place is completion of a business impact analysis (BIA). The BIA will identify the critical nature of each business function by assessment of the impact of interruption to that activity. This information will be required in order to identify appropriate continuity strategies for each function.

The BIA is similar to the risk assessment that is undertaken as part of the overall risk management process. However, the critical difference with business continuity planning is that the emphasis of a BIA is the identification of the relative importance and criticality of each function, rather than identifying the events that could undermine that particular function.

Therefore, the risk assessment and the BIA are related and could well be undertaken together. The risk assessment will help in identifying the risks that might threaten the achievement of the business continuity objectives. Both approaches require a structured and systematic approach.

The business impact analysis has three clear purposes, as follows:

1. Identify mission-critical activities and the required recovery time in the event of disruption. This identification process will establish the timeframe within which the critical functions must be resumed after the disruptive event.
2. Establish the impact potential and the resource requirements for recovery within the agreed timescale. The business requirements for recovery of the critical function must be established.
3. Determine whether the likely impact is within the risk appetite of the organization as the basis for business continuity strategy. The technical requirements for recovery of the critical function also need to be established.

BCP and ERM

There is an obvious link between BCP and enterprise risk management (ERM). ERM is concerned with the risks facing the whole organization and BCP takes an approach that business continuity arrangements should be in place. The BCP approach is to look at the continuity of operations across the whole organization. Ensuring continuity is obviously part of an ERM approach. It should therefore be considered that BCP is part of ERM, but it is not the whole of ERM activity. Nevertheless, there is a strong similarity in approach and the business continuity and disaster recovery activities should take place within the context of a broader ERM initiative, as appropriate.

Enterprise risk management will be explored in more detail in a later Part of this book. The basis of ERM is that the stakeholder expectations and the core processes of the organization that deliver those expectations are the focus of the risk assessment process. The intention of enterprise risk management is to ensure that the core processes are maintained.

Continuation of core business processes is also the basis of business continuity planning. The difference in emphasis is that ERM seeks to identify the risks that could impact the core processes. BCP seeks to identify the critical business functions that need to be maintained in order to achieve continuation of the business. The approaches are complementary and there is a good deal of similarity between BCP and this style of ERM.

Civil emergencies

In many countries, there is an obligation placed on local government to ensure the continuity of local businesses in the event of a major civil emergency. The emergency may be triggered by a natural disaster, such as flooding or earthquake. Alternatively, it could be caused by terrorism, civil unrest or by an epidemic/pandemic.

Several organizations may find that they are required to assist the civil authorities in the event of a civil emergency. This will be the case for organizations that supply products that may be required in such an emergency or have large buildings that could be used as temporary accommodation. The products that may be useful in a civil emergency will include food, bottled water, clothing and blankets.

Many civil authorities publish guidance for businesses to assist them with their business continuity planning. For example, the US government provides valuable information on its website. Also, several trade associations and small business associations offer practical guidance on the business continuity planning, including appropriate actions in the case of civil emergency.

Most local authorities have statutory responsibility for responding to civil emergencies. Factories and warehouses may have equipment and facilities that could be useful in the event of a civil emergency. Likewise, retail shops will have food and other goods that may be required for distribution as emergency supplies. Also, schools and other civic buildings may be required as accommodation in the event of a civil emergency.

Encouraging organizations to make arrangements to ensure business continuity will benefit local authorities in charge of civil emergencies, because there will be fewer problems and issues for them to take into account at the time of the emergency. The box below provides a summary of typical advice provided by a municipal authority to small businesses in the local area.

Secure your business

Thoroughly assessing the disasters that could threaten your firm will give you a clear idea of the business areas that are most important to secure. Usually, these will be the areas on which your business relies the most, and which are exposed to the greatest degree of risk. This is the most important part of your plan. The following check points are essential when writing this stage of your plan. You need to systematically go through each of the following areas and take a practical approach to tackle each of the threats that your business may face, following the process:

- assign ownership;
- identify threats and resources;
- develop contingency plans and policies;
- premises and key equipment.

Clearly, your premises are fundamental to your business – so much so that you probably take them for granted. But you should consider the long-term impact that damage to or destruction of your premises would have on your business. The same applies to business-critical machinery. If a vital piece of equipment is destroyed, damaged or stolen, ask the following questions:

- Would you be able to inform your employees and customers of disruption?
- What would happen to customer orders when your premises were closed?
- Would you be able to make alternative arrangements for regular orders?

Case study

Invensys – risks and uncertainties

Invensys operates globally in varied markets and is affected by a number of risks inherent in its activities, not all of which are within its control. The Risk Committee has accountability for overseeing the risk management processes and procedures, and reports to the Board through the Audit Committee on the key risks facing the business. It also monitors the mitigating actions put in place by the relevant operational managers to address identified risks. Two examples of the principle risk faced by Invensys are set out below.

1. The Group faces intense competition and failure to maintain a competitive and technologically advanced product range could reduce its margins and revenue growth.
2. Invensys operates in highly competitive markets and the Group's products and services are characterized by continually evolving industry standards and rapidly changing technology, driven by the demands of the Group's customers. Failure to keep pace with technological changes and system or application requirements in the industrial sectors may result in loss of market share and lower margins.
3. The Group invests in research and development to develop new technologies and products to sustain or improve its competitive position. However, all new technologies and products involve business risk in terms of possible abortive expenditure, reputation risk and the potential for onerous contracts and customer claims. The Group reviews its portfolio of technologies as part of the strategic planning process. In addition, the businesses control individual development projects through a stage gate review process.
4. The Group may be exposed to liability through the actions of joint-venture partners, co-source partners or its supply chain.

The business activities of the Group are often conducted in conjunction with joint-venture, consortium, co-development or co-source partners whose day-to-day management actions are outside of the control of the Group.

A significant element of the Group's risk profile is the delivery performance of its supply chain. Given the nature of the Group's businesses, a quality or other failure in the supply chain could present a risk to safety and delivery which could have a material adverse effect on the Group's business, financial performance and reputation. Assessment, mitigation and management of these risks are addressed by the businesses in conjunction with the Group's legal, supply chain and risk functions.

Annual Report and Accounts 2009

Part 4

Risk and organizations

Learning outcomes for Part 4

- describe the key features of a corporate governance model and describe the links to risk management in different types of organizations;
- list the different types of stakeholders of a typical organization and explain the influence of these stakeholders on risk management;
- provide a description of a simplified business model and the different types of core processes that need to take place in an organization;
- provide a brief description of the project life cycle and the importance of risk management at each stage, using the 4As approach;
- describe the key features of a project risk management system, such as the project risk analysis and management (PRAM) approach;
- outline the key features of operational risk as practised in financial institutions, such as banks and insurance companies;
- describe the key sources of operational risk in financial institutions and provide examples of how these risks are managed;

- describe the importance of the supply chain and the contribution of supply chain risk management to the success of the organization;
- give examples of the risks associated with outsourcing and how these risks can be successfully managed.

Part 4 Further reading

APM Publishing (2004) Project Risk Analysis and Management Guide, www.apm.org.uk.
Institute of Risk Management (2005) Risk Management Organization and Context, www.theirm.org.
London Stock Exchange (2004) Corporate Governance A Practical Guide, www.londonstockexchange.com.
Reuvid (2008) Managing Business Risk, www.koganpage.com.

19
Corporate governance model

Corporate governance

Corporate governance covers a very wide range of topics, and risk management is an integral part of the successful corporate governance of every organization. Most countries in the world place corporate governance requirements on organizations. These requirements are particularly strong in relation to companies quoted on stock exchanges, organizations that are registered charities and government departments, agencies and authorities. For instance, companies listed on the London Stock Exchange have to be guided by the Combined Code on Corporate Governance published by the Financial Reporting Council.

The purpose of corporate governance is to facilitate accountability and responsibility for efficient and effective performance and ethical behaviour. It should protect executives and employees in undertaking the work they are required to do. Finally, it should ensure stakeholder confidence in the ability of the organization to identify and achieve outcomes that its stakeholders value.

There are two main approaches to the enforcement of corporate governance standards. Some countries treat corporate governance requirements as 'comply or explain'. In other words, the organization should comply with the requirements or explain why it was not appropriate, necessary or feasible to comply. If appropriate, an organization could explain that an alternative approach was taken to achieve the same result. In these countries, the requirements may be regarded as one means of achieving good practice, but equally effective alternative arrangements are also acceptable.

Other countries require full compliance with detailed requirements, although limited alternatives for achieving compliance are sometimes included within these requirements. In these countries detailed compliance is expected and exceptions would not be acceptable.

Corporate governance requirements should be viewed as obligations placed on the board of an organization. These requirements are placed on board members by legislation and by various

codes of practice. Often, these corporate governance requirements are presented as detailed codes of practice. To start the process of enhancing corporate governance standards, an organization may develop a code of ethics for company directors, together with appropriate 'delegation of authority' documents. An annual statement of conflict of interest should be required from directors and training should be provided for the board on corporate governance.

Also, the organization should set up appropriate committees (as listed below) with established terms of reference and membership of each of these committees, which may be established as sub-committees of the board. Reports on corporate governance standards, concerns and activities should be received at every board meeting and these papers will often be presented by the company secretary.

- risk management committee;
- audit committee;
- disclosures committee;
- nominations committee;
- remuneration committee.

OECD principles of corporate governance

A basic definition of corporate governance is 'the system by which organizations are directed and controlled'. Corporate governance is therefore concerned with systems, processes, controls, accountabilities and decision making at the highest level and throughout an organization.

Because corporate governance is concerned with the way that senior management fulfil their responsibilities and authority, there is a large component of risk management contained in the overall corporate governance structure for every organization. Corporate governance is concerned with the need for openness, integrity and accountability in decision making and this is relevant to all organizations regardless of size or whether in the public or private sector.

The Organization for Economic Cooperation and Development (OECD) is an international organization helping governments tackle the economic, social and governance challenges of a globalized economy. The OECD has established a set of principles for corporate governance and these are set out in Table 19.1. These principles focus on the development of an effective corporate governance framework that pays due regard to the rights of stakeholders.

The principles require the equitable treatment of all stakeholders and an influential role for stakeholders in corporate governance. Finally, the principles require disclosure and transparency. All of these principles are delivered by the board of the organization and the principles, therefore, make detailed reference to the responsibilities of the board.

Table 19.1 OECD principles of corporate governance

1. **Effective corporate governance framework**
   Promote transparent and efficient markets, be consistent with the rule of law and clearly articulate the division of responsibilities
2. **Rights of shareholders**
   Protect and facilitate the exercise of the rights of shareholders
3. **Equitable treatment of shareholders**
   Equitable treatment of all shareholders, including minority and foreign shareholders
4. **Role of stakeholders in corporate governance**
   Recognize the rights of stakeholders and encourage active co-operation in creating wealth, jobs and sustainability
5. **Disclosure and transparency**
   Timely and accurate disclosure is made on all material matters, including the financial situation, performance, ownership, and governance
6. **Responsibilities of the board**
   Strategic guidance of the company, effective monitoring of management by the board and accountability of the board to the company and shareholders

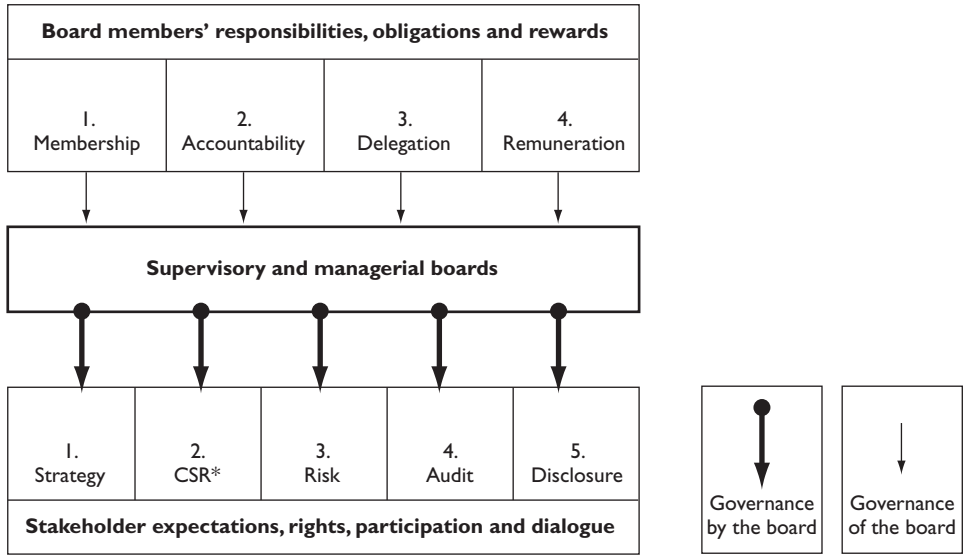
LSE corporate governance framework

The London Stock Exchange (LSE) has produced guidance on corporate governance and the focus of that guidance is on the effectiveness of the board. In the view of LSE, corporate governance is about the effective management of the organization and the appropriate responsibilities and the role of the senior managers and board members within the organization.

Figure 19.1 provides a summary representation of the London Stock Exchange governance framework. Governance activities are centred on the board of the organization and the LSE guidance refers to these boards as supervisory and managerial boards. The corporate governance framework has two main components. These components are: 1) the responsibilities, obligations and rewards of board members, and 2) the fulfilment of stakeholder expectations, rights, participation and dialogue.

The importance of board member responsibilities, obligations and rewards are emphasized and include arrangements for:

- determining membership of the board;
- accountability of board members;



* Corporate social responsibility

Figure 19.1 Corporate governance framework

- delegation of authority from the board;
- remuneration of board members.

The responsibilities of board members must be fulfilled in five important areas, in respect of the fulfilment of stakeholder expectations, rights, participation and dialogue. In summary, these five areas are as follows:

- strategic thinking, planning and implementation;
- corporate social responsibility;
- effective management of risks;
- audit and risk assurance;
- full and accurate disclosure.

The OECD principles and the LSE corporate governance framework provide the overall requirements and framework within which corporate governance must be delivered. However, the processes that are used to deliver each of the five areas of stakeholder expectation will vary.

Risk management activities should be viewed within the wider framework of corporate governance. Although risk management is presented as a separate component of corporate governance in the LSE framework, risk issues also underpin strategy, corporate social responsibility, audit and disclosure.

Corporate governance for a bank

Corporate governance and risk management activities within a financial organization are strictly governed and regulated. Most financial organizations, including banks, produce their own internal corporate governance guidelines. Typically, these guidelines will cover director qualifications, director responsibilities and the responsibilities and delegated authority of board committees. The guidelines should also consider arrangements for the annual performance evaluation of the board and the arrangements for senior management succession.

The corporate governance structure will normally be a set of governing principles for the conduct of the board of directors. These governing principles will include information for board members on dealing with conflicts of interest, confidentiality and compliance with laws, rules and regulations.

A major part of ensuring adequate corporate governance for a financial institution will be adequate training and induction for board members. Typically, the orientation programme for new members of the board will include details of:

- the legal and regulatory framework;
- risk management;
- capital management and group accounting;
- human resources and compensation;
- audit committee, internal audit and external audit;
- communication, including branding.

The global financial crisis has resulted in banks and other financial institutions reviewing their own corporate governance standards. The review in the box below provides an overview of a large national bank and sets out criticisms of that bank in relation to failures of corporate governance.

Operational risk

The bank is the largest financial services institution listed on the national stock exchange and is among the 30 most profitable financial services organizations in the world. In January 2004, the bank disclosed to the public that it had identified substantial losses relating to unauthorized trading in foreign currency options. These losses were classified as operational risk.

Concurrent issues of further substantial losses on home loans called into question the strength of the risk management practices and lack of auditor independence, reinforcing the view that corporate governance had not been given the priority it deserved over a number of years.

Corporate governance for a government agency

For government agencies, robust corporate governance arrangements are usually mandatory. Also, for many government agencies, the main reason for paying attention to risk management is to ensure that adequate corporate governance arrangements are in place. In other words, the main motivation for ensuring good standards of risk management in a typical government agency will be the desire to support the corporate governance arrangements in the agency. Figure 19.2 shows the corporate governance components for a typical government agency.

For commercial organizations, corporate governance and risk management are designed to assist the organization to achieve its objectives, including commercial or marketplace objectives. The motivation for government departments to ensure good standards of corporate governance is narrower and is often focused on accountability.

In government agencies, the driving principles include value for money and avoidance of inappropriate behaviour. Corporate governance is often seen by government agencies as establishing a framework of control that supports innovation, integrity and accountability and encourages good management throughout the organization.

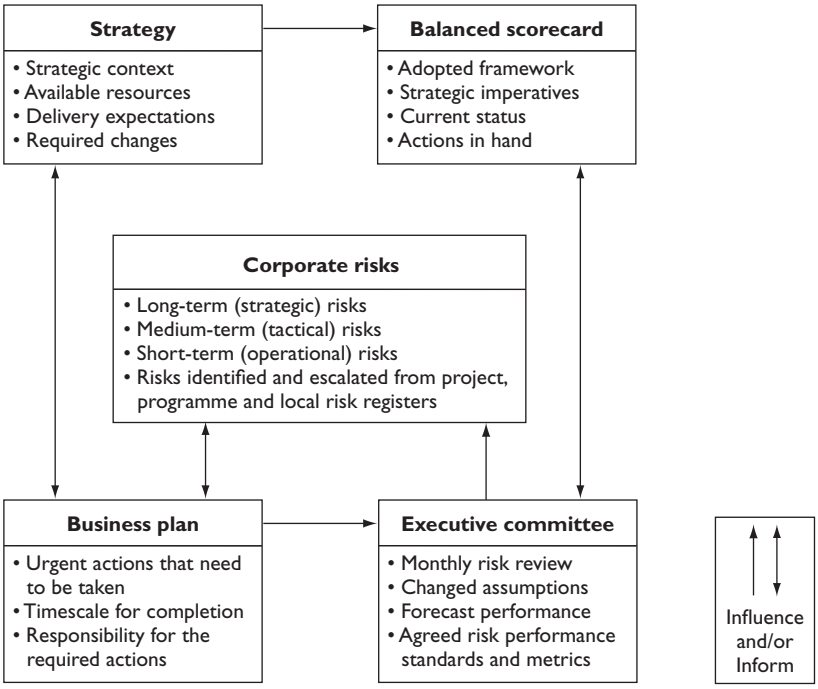


Figure 19.2 Corporate governance in a government agency

Within the corporate governance framework, responsibilities of individual members of staff are frequently specified. The reporting structure for risk issues is also outlined. Linking risk management efforts to corporate governance can also enable specific areas of risk to be identified for particular attention. Typically, these will include value for money, business continuity, fraud prevention and IT security assurance. Underpinning corporate governance activities within a government department, agency or authority will be the principles of public life, often referred to as the Nolan principles. These are set out in Table 19.2

Table 19.2 Nolan principles of public life

1. **Selflessness**

   Holders of public office should act solely in terms of the public interest and should not seek benefits for themselves, their family or friends

2. **Integrity**

   Holders of public office should not place themselves under any financial or other obligation to outside individuals or organizations

3. **Objectivity**

   In carrying out public business, the holders of public office should make choices on merit

4. **Accountability**

   Holders of public office are accountable for their decisions and actions to the public and must submit themselves to appropriate scrutiny

5. **Openness**

   Holders of public office should be as open as possible about all the decisions and actions that they take and give reasons for their decisions

6. **Honesty**

   Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts

7. **Leadership**

   Holders of public office should promote and support these principles by leadership and example

The box below provides an example of the importance of corporate governance arrangements within a government agency. The important contribution of risk management and corporate governance arrangements and management practices is highlighted in this example.

Welsh Assembly Government – Risk management policy

The risk policy of the Welsh Assembly Government (WAG) sets out policy on the identification and management of risks that it faces in the delivery of its objectives. Its aims are to ensure that risk is taken into account at all stages in the development and delivery of WAG activities, including risk analysis, the development of actions to manage risks, and to monitor, review and evaluate such activity.

The Accounting Officer and Strategic Delivery & Performance Board of the Welsh Assembly Government have adopted the following risk management policy to create the environment and structures for the implementation of the WAG Plans, to:

- ensure that the objectives of the Welsh Assembly Government are not adversely affected by significant risks that have not been anticipated;
- ensure achievement of outputs and outcomes and having reliable contingency arrangements to deal with the unexpected that might put service delivery at risk;
- promote a more innovative, less risk-averse culture in which the taking of appropriate risks in pursuit of opportunities to benefit the WAG is encouraged;
- provide a sound basis for integrating risk management into decision making;
- form a component of excellent corporate governance and management practices.

Risk Improvement Manager
Corporate Governance and Assurance
Welsh Assembly Government

February 2008

Evaluation of board performance

Evaluation of board performance is a critically important part of the corporate governance arrangements for any organization. Table 19.3 provides a checklist of issues that should be included in the evaluation of the effectiveness of a board. The areas for evaluation are as follows:

- membership and structure;
- purpose and intent;
- involvement and accountability;
- monitoring and review;
- performance and impact.

The checklist set out in Table 19.3 focuses on corporate governance effort and on the level of performance of the board. When deciding issues related to strategy, projects and operations, the board will need to ensure that adequate processes are in place for reaching decisions. These decisions will result in a course of action and the implementation of that course of action needs to be monitored.

Table 19.3 Evaluating the effectiveness of the board

Membership and structure
• Does the board have the necessary range of knowledge, skills and experience? • Is there appropriate turnover of board membership to ensure new ideas? • Are the sub-committees of the board effective with appropriate delegated authority? • Are board decision-making processes satisfactory with adequate information available? • Do communication processes exist between board members outside board meetings?
Purpose and intent
• Do all board members understand and share the vision and mission? • Do members of the board understand the objectives and position statements? • Is there sufficient knowledge and understanding of the significant risks? • Are board members sufficiently involved with the development of strategy? • Have measurable budget and performance targets been put in place?
Involvement and accountability
• Does the board have shared ethical values, including openness and honesty? • Are the established policies unambiguous and consistent with the ethics? • Do board members understand their duties, responsibilities and obligations? • Is there a feeling of mutual trust and respect at board meetings? • Are there adequate delegation and authorization procedures in place?

Table 19.3 *continued*

Monitoring and review
• Is there sufficient monitoring of performance using appropriate measurements? • Does the board challenge planning assumptions when and where appropriate? • Does the board demonstrate the ability to respond rapidly to changes? • Is there a mentality that demands continuous improvement in performance? • Does the board assess financial and other controls and seek assurance on compliance?
Performance and impact
• Is there a satisfactory level of attendance at board, committee and other meetings? • Are board decisions and actions fully recorded and actions tracked and confirmed? • Are the established targets and agreed performance indicators evaluated and assessed? • Is the impact of board decisions and actions evaluated in a timely manner? • Is there an emphasis on accuracy, honesty and open reporting to external agencies?

The course of action will result in some outputs, and these need to be evaluated in terms of the impact that is achieved. When evaluating the effectiveness of the board, the impact of its decisions is the ultimate test. The level of impact can then be evaluated against the vision, mission and objectives of the organization.

20
Stakeholder expectations

Range of stakeholders

Organizations will have a wide range of stakeholders, some of whom may indeed be unwanted as far as the organization is concerned. For example, if a distribution company wishes to build an extension to its depot, local residents may want to object to it. The local residents are stakeholders in the operation of the company, even though the owner of the company may not wish to acknowledge that fact. ISO Guide 73 defines a stakeholder as a 'person or group concerned with, affected by, or perceiving themselves to be affected by an organization'.

There will be a wide range of stakeholders in a typical sports club and these will include the following:

- supporters;
- players;
- staff;
- financiers;
- sponsors;
- suppliers.

Stakeholders may have contradictory expectations of the organization. For example, staff will seek pay that is as high as possible. This would be in opposition to the requirements of financiers, who want the club to be as profitable as possible. It is part of the role of management to balance the conflicting interests of different stakeholders and implement actions that provide the best balance between conflicting stakeholder expectations.

For organizations in different sectors, the range of stakeholders will be different. For government agencies, the general public will be a major stakeholder. Specific groups within the general public will be stakeholders in different agencies, depending on the purpose of each

particular agency. For organizations that have significant environmental interests or exposures, a different range of stakeholders would need to be considered. For some energy companies, environmental pressure groups are often unwelcome stakeholders. There may be a substantial conflict between a mining company that wishes to extract minerals and the local population who do not want heavy industrial activities taking place in the area.

Depending on the nature of the stakeholder, questions should be asked about the risk awareness of the organization, the activities that are designed to achieve risk improvement and risk governance arrangements within the organization. Relevant stakeholders are entitled to receive information on the risk profile of the organization. They are also entitled to information on the arrangements for risk improvement and the metrics that are in place to monitor risk performance. Finally, stakeholders are entitled to information on the risk appetite of the organization and the arrangements for incorporating risk into the development of strategy.

The box below provides an example of how stakeholders will have different expectations of an organization. Sometimes, these expectations will be contradictory. Even if they are not contradictory, it is helpful for one group of stakeholders to have an understanding of the expectations of the other groups.

Stakeholders in a theatre

Assume that a theatre is seeking to involve all stakeholders in its activities. This will extend to consideration of the objectives of performers at the theatre, including artistes and actors. There needs to be a distinction between the objectives of the performer and the requirements of the audience. For example, an established musician may wish to promote a new album, but the audience will want to hear the established favourites from previous ones.

The performer will have the best chance of presenting a successful show if the starting point is an evaluation of audience expectations, followed by an evaluation of the expectations of the theatre. The performer can then plan the specific content of the show to be consistent with those expectations as well as taking account of his or her professional and personal objectives. The theatre may encourage this approach and recognize the performer as a stakeholder, but encourage the performer to consider other stakeholders and their expectations.

Stakeholder dialogue

Dialogue with stakeholders should be based on a mutual understanding of the objectives of the organization. The board is responsible for ensuring that the dialogue is satisfactory.

Although specific members of the organization may have the day-to-day responsibility for communications with particular groups of stakeholders, the board will retain overall responsibility. Table 20.1 provides a summary of the information that should be provided to shareholders of a company. This information will focus on the provision of accurate financial data.

The level and nature of dialogue with stakeholders will depend on the particular interests of the stakeholder in the operations of the organization. The supporters of a sports club will require different information than the banks that are providing the necessary financial support for the club.

To obtain the fullest picture of the risks facing an organization, analysis of stakeholders and their expectations is necessary. The identification of stakeholder expectations is one output from the external evaluation stage of the business cycle. Different stakeholders may have expectations that are contradictory or even mutually exclusive in terms of the demands placed on the organization.

Table 20.1 Data for shareholders

General
• A clear statement of strategy and vision • Corporate profile and principal markets
Financial data
• Annual report and financial statements • Archived financial information for the past three years
Corporate governance and CSR
• Information related to compliance with Combined Code • Information on the company CSR policies
Shareholder information
• Shareholder analysis by size and constituent • Information on directors' share dealings
Relevant news
• Access to all news releases and presentations • Developments that might affect the share value

Stakeholders and core processes

Core processes deliver stakeholder expectations and they are related to the internal and external context of the organization. Therefore, a risk can be defined as an event with the potential to impact the fulfilment of a stakeholder expectation. This approach has the advantage that both internal and external stakeholders can be identified, together with their short-term, medium-term and long-term expectations. Figure 20.1 provides a graphical illustration of the relationship between stakeholder expectations and the core processes of the organization. The figure illustrates that the core processes of an organization can be strategic, tactical and operational. This classification of core processes as strategic, tactical and operational is acknowledged in British standard BS 31100 when it discusses risk management perspectives. Strategic perspectives set the future direction of the business; tactical perspectives are concerned with turning strategy into action by achieving change; and operational perspectives are related to the day-to-day operations of the organization, including people, information security, health and safety and business continuity.

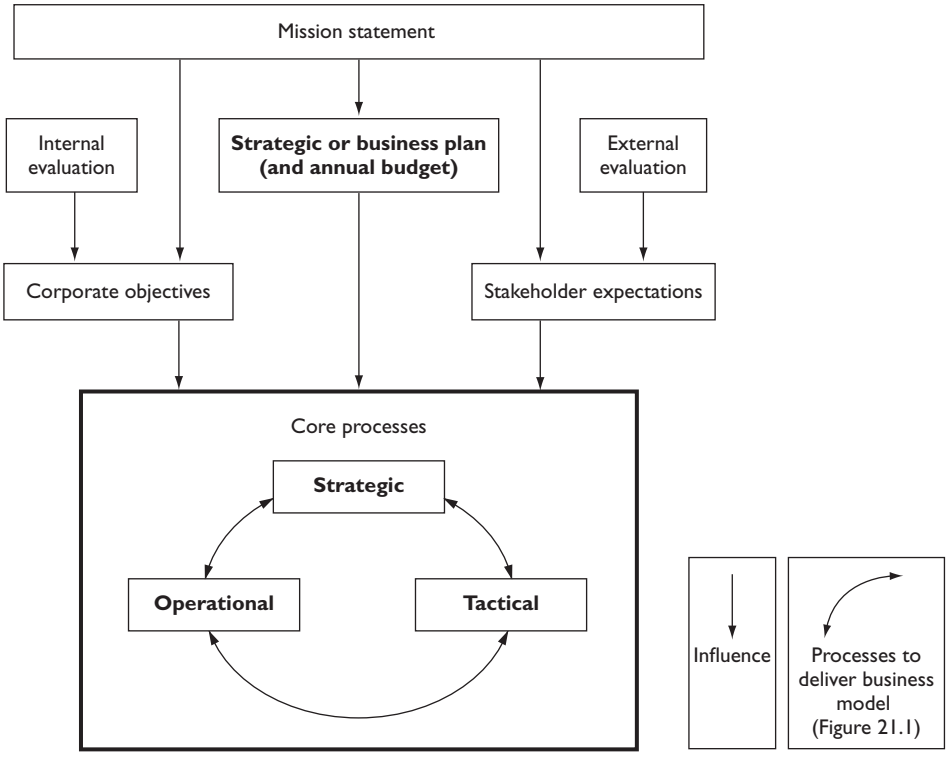


Figure 20.1 Importance of core processes

An approach based on stakeholder expectations has many advantages. It facilitates a full and thorough validation of the core processes of the organization in relation to the expectations that each stakeholder places on each core process. An important aspect of managing an organization is balancing the various stakeholder expectations. There are dangers inherent in achieving this balance, and a risk identification process based on analysis of stakeholder expectations is the most robust way of ensuring that these dangers are recognized, analysed and minimized.

The analysis of stakeholder expectations is also one of the fundamental requirements of the business process re-engineering (BPR) approach. The stakeholders in the current and future activities of the organization can be identified. The expectations of each stakeholder in relation to each stated objective and the corporate mission can then be evaluated. Shared expectations will emerge and the core processes of the organization can then be defined (or refined) specifically in terms of the delivery of these shared expectations.

Although the analysis of stakeholder expectations can be one of the most robust ways of identifying risks, there are implications in terms of the time and effort required for this approach to be successful. BPR can be a very time-consuming exercise, when undertaken thoroughly.

Stakeholders and strategy

It has been clearly established and demonstrated by research that incorrect risk management decisions related to strategy can destroy more value for an organization than incorrect risk management decisions associated with the operations or projects undertaken by the organization.

Strategic processes, therefore, need to be the most robust processes in the organization, and indeed this will be required by major stakeholder groups. Such stakeholders include financiers and other shareholders who are interested in the long-term success of the organization.

Strategic core processes for a sports club may include the building of a new stadium. This would be a significant investment that will require substantial support from financiers. In order to secure support, the club will need to be aware of the expectations of the financiers and ensure that the plans for the new stadium and the financial arrangements that will be put in place fulfil the necessary stakeholder expectations. The construction phase of acquiring a new stadium will be a significant project for the club, with a different range of stakeholders to consider.

Stakeholders and tactics

Tactical stakeholders of an organization may be very different from those who are concerned with the organization's operations.

If the tactics of an organization involve improvements to products, investment in new production techniques, response to technological changes or other developments that require a project, then finance is likely to be required. This means that financial bodies are likely to be key stakeholders in projects and similar tactical changes. Other stakeholders in projects may include building contractors and providers of other specialist professional support, such as architects.

The importance of employees in the implementation of tactics should not be underestimated. Staff will also have an interest in operational issues and be major stakeholders in the organization's operations. If changes to work practices or product features are to be successfully incorporated into the operations of the organization, then the support of staff is vitally important and good communication with them is essential.

Stakeholders and operations

There may be many stakeholder groups involved in the operational activities of an organization. To continue with the example of a sports club, fans will be major stakeholders in a large number of different aspects of the club's activities. One of the primary concerns of fans will be good results on the pitch. They will also be interested in other operational aspects, including the arrangements for buying tickets, transport and access arrangements, as well as the facilities provided within the stadium.

Pharmaceutical companies are generally large organizations with a very diverse range of stakeholders. In particular, a pharmaceutical company producing a critical medication has an obligation to ensure a constant availability of that medication for all its patients. Patients should be viewed by the pharmaceutical company as important stakeholders who have expectations regarding the availability and effectiveness/efficacy of the medication that has been prescribed.

The stakeholder groups that have an interest in the operational activities of an organization are likely to be customers, suppliers and others that may be affected by disruption to the normal efficient operation of the organization. For example, customers are likely to be affected if a hazard risk were to materialize. Likewise, suppliers are stakeholders in the organization and they will suffer if the organization is disrupted to the extent that their supplies/produce/components/service are no longer required.

Other stakeholder groups that are likely to be affected by hazard risks will also have an interest in the continuity of the activities of the organization. For financial organizations such as banks, customers would be immediately affected if critical IT systems fail.

Corporate governance models require the involvement of stakeholders and adequate stakeholder dialogue. In several countries, employees are recognized as stakeholders in

the organization to the extent that employee representation on the board may be mandatory. The box below considers the position in some European countries.

Employee representation on the board

Board-level employee representation involves employee representatives who sit on the supervisory board, board of directors or similar structures in companies. These employee representatives are directly elected by the workforce, or appointed in some other way, and may be employees of the companies, officials of organizations representing those employees, or individuals considered to represent the employees' interests in some way.

Board-level representation also differs from other types of indirect participation such as works councils in that it attempts to provide employee input into overall company strategic decision making rather than focusing on information and consultation on day-to-day operational matters at the workplace.

In most cases in western Europe, employee representatives are in the minority, and board-level participation is associated with the obtaining of information and understanding and the expression and exchange of opinions, views and arguments about an enterprise's strategy and direction. In a few cases, however, when employee representatives are equal in number to those of shareholders or other parties, issues of control, veto and real influence over company strategy – sometimes known as 'co-determination' – come into play.

21
Analysis of the business model

Simplified business model

In order to place risk management within the context of business operations, it is necessary to consider a simplified business model. Figure 21.1 sets out the basic elements of a business model in simple terms. The first stage for an organization is to decide the strategy that it is seeking to deliver. The strategic aims will be determined by considering the mission statement of the organization, the corporate objectives and the stakeholder expectations. The organization should establish a strategy that is capable of delivering the mission statement of the organization. In other words, the strategy of the organization needs to be efficacious.

Having established the overall strategy, the processes that will deliver it need to be identified. For many organizations, the processes that are already in existence will be sufficient. However, if the strategy requires changes to processes or the introduction of new processes, then projects or programmes of work will be required. The processes introduced by the organization should be effective in that they are the correct processes to deliver the desired outcomes in the most cost-effective manner.

The operations of the organization will need to be efficient in that they deliver the required and anticipated outputs at the lowest cost with least disruption. The operations of the organization are the day-to-day operations that build into the processes that deliver the overall strategy for the organization. In relation to operations, the desired state of the organization is the continuity of normal efficient operations with no unplanned disruption.

Figure 21.1 sets out the stages that are described above. The strategy can be seen as 'where the organization wants to be'. Review of the operations of the organization will collect information on 'where the organization is now' and the tactics define 'how the organization will get there'. This is a three-stage business model that has events at its centre. In many circumstances, these events will represent risks that could materialize. The other component of this simple business model is the reporting of the results of operations.

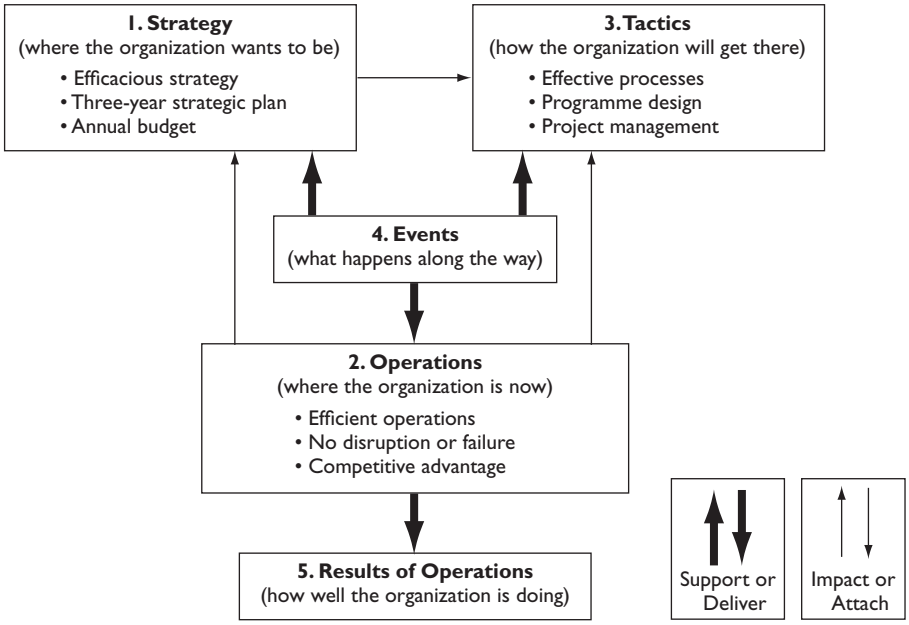


Figure 21.1 Simplified business model

Actions and events can be good, bad or routine, and enable the organization to monitor what progress is being made against the business strategy, projects and operations. These actions and events impact the organization and its ability to sustain efficacious, effective, efficient and compliant business operations and core processes.

Identification of strategy will require an approach based on opportunity management. Delivery of tactics, often by way of projects, will require attention to uncertainties and management of control risks will be important. Delivery of effective and efficient operations will require particular attention to the successful management of hazard risks.

Core business processes

A core process is one that is fundamental to the continued success (or even existence) of the organization. Core processes ensure that the organization is able to achieve the mission and corporate objectives and fulfil stakeholder expectations. Each core process creates value and is designed to deliver one or more of the stakeholder expectations.

There are three basic types of core process as set out in Figure 20.1 (page 188). These are processes designed, implemented and managed to ensure the following:

- development and delivery of strategy;

- management of tactics, projects and enhancements;
- continuity and monitoring of routine operations.

An activity is an individual job or task that builds into the processes that deliver stakeholder expectations. The processes themselves are designed and intended to add value to the organization.

Having identified stakeholder expectations, core processes can then be put in place to ensure that these expectations are delivered to the level that the organization has decided is appropriate. No organization will be in a position to fully deliver all expectations to the level desired by all stakeholders. Often, this is because different stakeholder expectations are contradictory.

Weaknesses or gaps in the core processes of the organization are likely to be present, as follows:

- There may be weaknesses related to the development and delivery of strategy. These weaknesses will result in the organization failing to retain its position as market leader. They give rise to a leadership gap.
- There may be weaknesses related to the management of projects and product or service enhancements. These weaknesses will result in the organization failing to keep up with competitors. They give rise to a competition gap.
- There may be weaknesses related to failure to ensure continuity and monitoring of routine operations. These weaknesses will result in the organization failing to maintain efficient operations. They give rise to an efficiency gap.

Efficacious strategy

Business strategy is the statement of what the organization intends to achieve and how it plans to achieve it, and is based on the strategic decisions about the future of the organization. Establishing a detailed business strategy enables the organization to deliver its mission, objectives, strategy and plans. The overall objective of risk management input into strategy is to ensure efficacious strategy and strategic decisions that will deliver the desired outcomes.

The main risk management input into business strategy is likely to be risk assessment. This is a critical component for the formation of efficacious strategy. Risk assessment of the existing strategy and any proposed new strategy should be undertaken. If clear strategic options are present, then a risk assessment of each of the viable options should be undertaken individually.

Some organizations exist in a very competitive marketplace that is undergoing significant technological changes. In these circumstances, there are significant risks associated with the business and huge strategic decisions have to be taken. Often, these decisions are related to developments in technology that challenge the way in which the organization delivers cus-

tomer solutions. Changes in technology can require huge and speculative investment decisions. The investment decisions may be speculative because of untested new technology or because there are alternative technologies available.

A risk assessment of strategic options needs to be undertaken, including an analysis of stakeholder expectations, existing customer requirements and existing staff skills, as well as a strengths, weaknesses, opportunities and threats (SWOT) analysis. The strategic options available to the company might include joint ventures, outsourcing the work, sub-contracting or investing in new technologies.

Detailed risk assessment of strategic options will ensure that the board has the best available information in order to make correct strategic decisions. Events and other circumstances that could reduce the successful delivery of efficacious strategy should be identified during the risk assessment. The organization will then be able to decide the controls that should be put in place to optimize the likely impact if any of these risks materialize.

Effective processes

Business processes are the means by which the organization will deliver the business strategy. Processes need to be correctly selected, implemented and controlled to ensure the effectiveness and efficiency of operations. Processes should also deliver reliability of financial reporting and compliance with applicable laws and regulations. The intended outcome is effective, efficient and compliant business processes.

Changes to processes are delivered by projects, and the importance of risk management in projects will be discussed in a later chapter of this book. When undertaking a project, the organization needs to be concerned about the risks within the project that could stop it being delivered on time, within budget and to specification.

However, there is a further consideration related to projects and that is the effectiveness of enhancements to processes that the project is designed to deliver. There is little benefit in having a project delivered on time, within budget and to specification if the required increase in process effectiveness is not achieved. For example, the installation of a new business software system may be undertaken by a successful project, but if the new software system is inadequate, or does not deliver all of the additional benefits anticipated, then the improvement in business processes may not have been achieved.

The main risk management inputs into processes and projects will be risk assessment, risk response enhancement and the review and monitoring activities. The purpose in undertaking a risk assessment of a project is to identify necessary controls. When these controls have been implemented, the effectiveness and efficiency of the controls will need to be reviewed. Overall, the intention is to ensure that processes and projects are themselves effective and efficient.

Efficient operations

The overall objective of risk management input into operations is to achieve operational efficiency that is protected from unplanned disruption. Disruption of operations is likely to be caused by a hazard risk materializing. The design of efficient processes that are free from disruption will provide the organization with significant competitive advantage or place the organization in a better position to deliver value for money.

Risk management can have a major impact on the operations of an organization. All stages of the risk management process are relevant to the continuity of uninterrupted efficient business processes. Risk recognition and rating (risk assessment), responding to significant risks, resourcing controls, reaction planning, reporting on risk and review and monitoring are all critical inputs. In summary, risk management input into operations needs to be comprehensive if operations are to be efficient and uninterrupted.

Internal audit also has an important role to play in the delivery of efficient operations. Internal auditors frequently refer to the added value that internal audit activities bring. This added value relates to the evaluation of control activities, especially in relation to operations. Not only should the operations be effective and efficient, but the controls that are in place should also be effective and efficient. Internal audit activities have a significant role to play in providing the appropriate risk assurance and providing confirmation of compliance, where relevant.

Reporting performance

Operational reports indicate how well the strategy is being delivered. Data need to be available on an ongoing basis, so that management can respond and modify the business processes, as necessary.

Operational reports also provide information that can be used to prepare reports to stakeholders on the performance of the organization. However, the organization needs to decide what will be reported and disclosed to stakeholders and the format that will be used for those reports. To ensure accurate reporting and disclosure, appropriate control activities need to be applied. In the United States, the Sarbanes–Oxley Act (SOX) sets out duties that are primarily concerned with the accuracy of financial reports to shareholders.

The main risk management input into reporting of performance is the risk assessment of the reporting lines and the data-handling procedures. The SOX duties have increased the attention paid to the control of reporting procedures. Section 404 of SOX requires that financial reports and the financial reporting procedures are attested by external auditors to confirm that they are accurate.

Aspects of the business model can also be applied to personal objectives and the achievement of personal success. Many books have been published on the personal traits of highly successful people, and the box below indicates some of the key characteristics exhibited by these high flyers.

Personal success

In a recent survey, respondents indicated that the top two drivers for success were: 1) having a strategic vision; and 2) having written goals. Most people indicated that their definition of success was 'work that is both challenging and rewarding'. Here are some key characteristics exhibited by successful people:

- clearly identified core values/mission/vision;
- personal definition of success;
- clearly defined, written goals;
- competency in negotiation;
- embracing risk taking;*
- continuous learning.

* People who are comfortable taking risks typically experience increased autonomy, heightened self-esteem, a more positive attitude towards life and an increased sense of personal power. Most successful people recognize that taking risks typically involves personal growth. Those with an aversion to risk often link risk with failure.

22
Project risk management

Introduction to project risk management

Projects will be undertaken by organizations for a number of reasons. When alterations to strategy are being planned, a project or series of projects (programme of work) will often be necessary in order to implement the revised strategy. Also, improvements to operational processes will require changes that will be implemented by undertaking a project.

Project risk management should be seen as an extension of conventional project planning. The main requirements for any project are that it is delivered on time, within budget and to specification or performance. Risk is often defined in terms of uncertainty or deviation from expected/required outcomes. It is in relation to project risk management that the definition of risk being represented by uncertainty is most relevant. Within project management, variability of outcomes is very undesirable. Therefore, the focus of risk management is often on the reduction in the variability of outcomes and the management of control risks.

There will be uncertainties within any project related to events, conditions and circumstances. The requirements of project risk management are to identify the events that could give rise to uncertainty and respond to the event appropriately. The style of risk management most relevant to project risk management is control management.

As well as managing the risks and uncertainties in a project, the project manager should also be looking for opportunities that may arise when certain developments within the project are more favourable than expected. Project risk management should take account of these positive developments and ensure that the structure for managing risks in projects is sufficiently flexible for the opportunities to be recognized and benefits obtained.

For example, consider a project of building a new road where one of the bridges can be completed well ahead of schedule because of favourable ground conditions. There may be an opportunity to build the benefit of this early completion into the future project plan, so that this gain is not lost in the overall timescale for delivery of the final completed project.

Development of project risk management

Project risk management is a type of control management. Projects relate to the delivery of a finite, specific or tactical product such as new:

- construction;
- products;
- IT systems;
- technology;
- markets.

Projects and enhancements are fundamentally important to organizations. Most projects are undertaken either to keep ahead of competitors or to catch up with them. In the context of risk management, the project itself may be considered to be a risk reduction exercise that is designed to achieve specific management objectives. The only purpose in spending money on business enhancement projects is to achieve a business or value-for-money advantage.

Project risk management is a well-developed discipline, with risk control and (especially) event management as the risk management activities that are most important. Project risk management is one of the more sophisticated and successful areas for the application of risk management tools and techniques.

The requirement for all projects is that they are delivered within the defined cost, time and quality parameters. Quality is the relationship between specification and performance. Some projects require that the outcomes comply with a certain specification, such as a new floor in a restaurant that has to be constructed from specified materials. Other projects may require a desired level of performance, such as specifying the level of slip resistance of the floor. Sometimes, both a specification and a performance will be required.

Because of the nature of projects, historical loss data will not usually be available. Accordingly, project risk management needs to be forward looking in order to anticipate problems before they arise.

Hazard, control and opportunity risks need to be considered as part of the successful management of any project. There are risks to the project that can prevent it being delivered on time and within budget (hazard risks). There are risks to the project concerning the specification, performance and quality of the final outcome (control risks). Finally, there are risks to the project whereby the full range of benefits or enhancements are not achieved (opportunity risks).

Uncertainty in projects

In order to manage uncertainty in projects, organizations have a range of possible actions they can take. An organization can decide to adopt one of the following:

- Accept the risk or uncertainty.
- Adapt processes and procedures.
- Adopt contingency plans and responses.
- Avoid the risk or uncertainty.

For low-exposure/low-uncertainty risks, the organization (or project) will usually accept uncertainty attached to each risk. For high-risk-exposure/low-uncertainty risks, the organization will adapt process procedures and introduce controls, including (when appropriate) insurance. For low-risk/high-uncertainty risks, the organization will adopt appropriate contingency plans and for high-exposure/high-uncertainty risks, the organization will wish to avoid the uncertainty attached to the risk.

This analysis (the 4As of control (or project) risk management) can also be applied to the management of uncertainty in general. The 4As of uncertainty management can be compared to the 4Ts of hazard management and represent a broadly similar approach. Management of control risks and uncertainty is considered in more detail in Chapter 27 and is illustrated in Figure 27.1 (page 246).

Project life cycle

Project risk management has become one of the best-developed and respected branches of risk management. This is not surprising given the dynamic and pressured environment in which many projects are undertaken. Projects can range from the implementation of a new software package on a computer system through to the building and commissioning of a substantial new sports stadium or delivering the Olympic Games in London (2012).

Whatever the size of the project, a number of specific stages will always be present. Figure 22.1 illustrates the key stages in the project life cycle. An important additional feature of project risk assessment is that the requirements of the client should always be of the utmost importance. The client may be external to the organization, but is sometimes part of the same organization.

Figure 22.1 sets out the project life cycle as having four stages. These are project inception, project planning, project execution and project closure. The activities within each of these four stages are listed in the figure. It is important to understand the stages in the project life cycle, so that the risk management inputs into each stage can be planned, executed and the required benefits obtained.

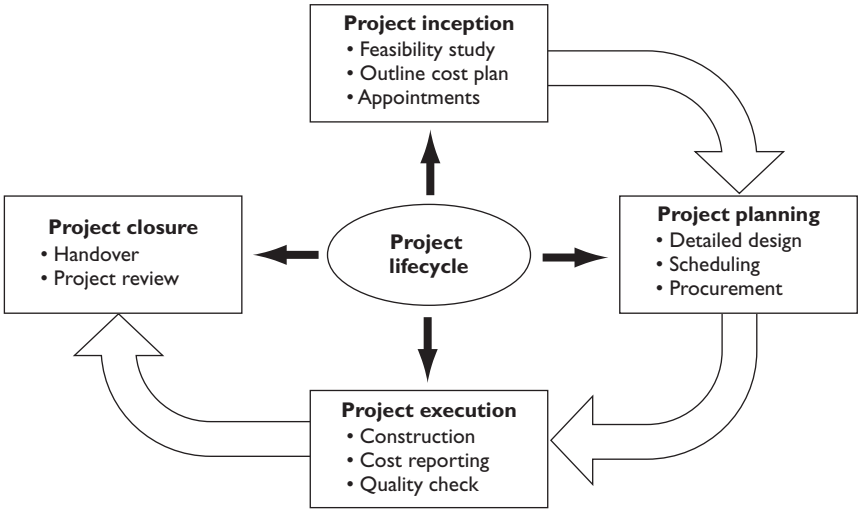


Figure 22.1 Project life cycle
Reproduced with permission from Feasible.

The risk management process as applied to project management is similar to the standard risk management process illustrated in Figure 4.1. However, the framework that supports the risk management process in each case may be quite different, because of the dynamic nature of the projects.

Each stage of the project life cycle will have significant risk and uncertainty issues embedded within it. The uncertainty embedded in each stage of the project will include such issues as defining the project precisely, agreeing the timescale and budget and confirming the performance/specification. There will also need to be arrangements for changes and developments within the project specification, as well as arrangements for any deviation from expected circumstances.

Take the example of refurbishing a block of flats. There will be a large number of interested parties, including architects and the principal contractor. External agencies will also need to be involved, including planning, building regulations requirements, health and safety, environmental protection and the utilities. Successful management of a project of this type will require the following:

- Make risk management part of the project.
- Identify risks early in the project.
- Communicate about risks.
- Consider both threats and opportunities.
- Clarify ownership issues.

- Prioritize risks.
- Analyse risks.
- Plan and implement risk responses.
- Register project risks.
- Track risks and associated tasks.

Opportunity in projects

Projects are undertaken because they represent an opportunity to be embraced or a challenge that needs to be overcome. Often a number of projects will need to be undertaken at the same time. A collection of projects of this sort is referred to as a programme.

Good project planning requires arrangements to overcome unexpected events or circumstances. This is often referred to as contingency in the budget or timescale. Contingency may be for additional time to complete a task, or additional costs that may arise to ensure that the final project deliverable operates to the required specification. As the project develops, any perceived difficulties will need to be addressed and opportunities to reduce the impact these difficulties explored.

Very frequently, the specification of a project will change during the course of the work. A well risk-managed project will take the opportunity of change to specifications to provide a greater level of customer satisfaction, as well as a greater level of income for the organization delivering the project.

Project risk analysis and management

The Association for Project Management (APM) developed the Project Risk Analysis and Management (PRAM) Guide in the mid-1990s. The key considerations that underpin the PRAM approach are set out in Table 22.1. Perhaps one of the most important points made is that there is often no historical experience specific to the project that will enable accurate prediction of the impact of risk-based events. The PRAM Guide provides steps to project risk management that are broadly consistent with the steps outlined above.

Table 22.1 PRAM model for project RM

Project Risk Analysis and Management is a process that enables the analysis and management of the risks associated with a project
• Properly undertaken it will increase the likelihood of successful completion of a project to cost, time and performance objectives • Risks for which there is ample data can be assessed statistically • However, no two projects are the same • Often things go wrong for reasons unique to a particular project, industry or working environment • Dealing with risks in projects is therefore different from situations where there is sufficient data to adopt an actuarial approach • Because projects involve a technical, engineering, innovative or strategic content, a systematic process is preferable to an intuitive approach • Project Risk Analysis and Management (PRAM) has been developed to meet this requirement

The PRAM approach represents a continuous process that can be started at almost any stage in the life cycle of a project. There are five points in a project where particular benefit can be achieved from using the PRAM model:

- Feasibility – at this stage the project is most flexible, enabling changes to be made that can reduce the risks at a relatively low cost.
- Sanction – the client can view the risk exposure associated with the project and check that all steps to reduce/manage the risks have been taken.
- Tendering – the contractor can ensure that all risks have been identified and that risk contingency or risk exposure limits have been set.
- Post-tender – the client can ensure that all risks have been identified by the contractor and assess the likelihood of programmes being achieved.
- During implementation – the likelihood of completing the project to cost and timescale will increase if all risks are identified and correctly managed.

The box below provides further commentary and advice on the importance of risk management in projects. Some important characteristics of risk management in projects, as well as some of the means of achieving success are discussed.

Risk management and projects

Embedding risk management within project management leads some to consider that it is just another project management technique or that its use is optional and appropriate only for large, complex or innovative projects. These attitudes often result in risk management being applied without full commitment or attention, and are often responsible for the failure of risk management to deliver the benefits.

To be fully effective, risk management must be closely integrated into the overall project management process. It must not be seen as optional, or applied sporadically only on particular projects. Risk management must be built in to project management and not seen as a bolt-on.

Built-in risk management has two key characteristics:

- First, project management decisions are made with an understanding of the risks involved. This understanding includes the full range of project management activities, including scope definition, pricing/budgeting, value management, scheduling, resourcing, cost estimating, quality management, change control and post-project review.
- Second, the risk management process must be integrated with other project management processes. Not only must these processes use risk data, but there should also be a seamless interface across process boundaries. This has implications for the project toolset and infrastructure, as well as for project procedures.

23
Operational risk management

Operational risk

The importance of managing operational risk has been well established for some time. Operational risk may be considered to be the type of risk that will disrupt normal everyday activities. In many ways, operational risk is closely related to infrastructure risks described in the FIRM risk scorecard classification system.

Operational risks are usually hazard risks, and historically this has been an area of strong application of risk transfer by way of insurance. However, operational risk now has a more extensive application and a more specific definition, especially in financial institutions. Whilst addressing the same types of risks, operational risk in financial institutions is differentiated by the fact that there is a need to quantify these risks in terms of potential financial loss.

Financial institutions are required to have sufficient capital reserves available to meet the actual and potential financial losses and obligations faced by the organization. This is a key requirement of the regulatory framework set out for banks in the Basel II Accord and under emerging regulation for European insurance companies through the Solvency II European Directive. Therefore, financial institutions need to measure the level of operational risk that they face. A major contributing factor to the global financial crisis was that banks adopted high-risk strategies that resulted in the banks having insufficient capital when the risks materialized.

The capital adequacy regulations that are based on Basel II require that banks take their operational risk exposure into account in determining their capital requirements. This operational risk management framework should include identification, measurement and monitoring, reporting, control and mitigation frameworks for operational risk. This assessment of capital requirements is often called economic capital.

In addition, the regulations require that banks must follow one of three specific quantitative methods to provide another measure of capital requirement. This is the so-called regulatory

capital. Two of the methods are based on incomes of the financial institution. The third method requires assessment of all material operational risk exposures to a high degree of statistical quality. Under Solvency II Directive, insurance companies in the EU will have to adopt a similar approach.

Basel II is the second of the Basel Accords that set out recommendations on banking laws and regulations, as issued by the Basel Committee on Banking Supervision. The purpose of Basel II (2004) is to create an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks they face.

Definition of operational risk

Operational risks faced by banks and other financial institutions represent essentially the same types of disruptive hazard risks that are faced by other organizations, although the definition may be broader. The specific point in the case of operational risk for financial institutions is that the level of operational risk needs to be quantified, because the level of risk has to be covered by available capital within the institution. This leads to an imperative for the bank to reduce the level of operational risk to the lowest level that is cost-effective.

Banks have long been concerned with market risk and credit risk (and insurance companies with underwriting risk as well), but the advent of Basel II and Solvency II requires financial institutions to consider broader operational risk exposures. Operational risk was initially defined as being any form of risk that was not market risk or credit risk. This imprecise definition was replaced by Basel II with a definition of operational risk as: 'the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events'.

The Basel II definition includes legal risk, but excludes strategic and reputational risk. The types of risks associated with the Basel II definition include the following:

- internal fraud, including misappropriation of assets, tax evasion and bribery;
- external fraud including theft, hacking and forgery;
- employment practices and workplace safety;
- clients, projects and business practices;
- damage to physical assets;
- business interruption and systems failures;
- execution, delivery and process management.

However, there is also recognition that operational risk is a term that has a variety of meanings and that certain financial institutions use a different term or a broader definition. The Basel II

definition identifies four types of risk categories: people, process, system and external risks. People risks include failure to comply with procedures and lack of segregation of duties. Process risks include process failures and inadequate controls. System risks include failure of applications systems to meet user requirements and the absence of built-in control measures. Finally, external risks include action by regulators (change of regulation, but excluding enforcement or disciplinary action), unsatisfactory performance by service providers and fraud, both internal and external. Finally, external risks also include legal action by customers of financial institutions in relation to negligence or fraud committed by staff.

The definitions of market risk and credit risk are also worth considering in relation to financial institutions. Market risk is the risk that the value of investments may decline over a period, simply because of economic changes or other events that impact large portions of the market. Credit risk is the risk that there will be a failure by customer/client to repay the principal and/or interest on a loan or other outstanding debt in a timely manner, or at all. Underwriting risk is also important for insurance companies; it is the exposure to the risks of the client through insurance policies.

Basel II

The 10 principles of 'Sound Practices' on operational risk put forward by the Basel II committee are set out in Table 23.1. One of the key requirements as set out in Principle 5 is that processes necessary for assessing operational risk should be established. The intention of Basel II is to help protect the international financial system from the types of problems that might arise should a major bank or a series of banks collapse.

Basel II attempts to protect the international financial system by setting up rigorous risk and capital management requirements designed to ensure that a bank holds capital reserves appropriate to the risk the bank exposes itself to through its lending and investment practices. These rules mean that the greater risk to which the bank is exposed, the greater the amount of capital it needs to hold to safeguard its solvency and overall economic stability. Basel II aims to ensure that capital allocation is more risk sensitive, that operational risk is separated from credit risk (both of which should be quantified) and that a global regulatory regime is in place.

The Basel II Accord describes a comprehensive minimum standard for capital adequacy that national supervisory authorities are working to implement. In addition, Basel II is intended to promote a more forward-looking approach to capital supervision that encourages banks to identify the risks they face and improve their ability to manage those risks. As a result, it is intended to be more flexible and better able to evolve with advances in markets and risk management practices.

There has been considerable debate about the effectiveness of the Basel II Accord (2004) in achieving its stated objectives. The effectiveness of the accord should be assessed against the

Table 23.1 ORM principles (Basel II)

The 10 principles on 'Sound Practices' of the Basel II committee are as follows:

1. The board is responsible for establishing the operational risk strategy.
2. Senior management is responsible for implementing the operational risk strategy.
3. Information, communication and escalation flows must be established.
4. Operational risks inherent in activities, processes, systems and products should be identified.
5. Processes necessary for assessing operational risk should be established.
6. Systems should be implemented to monitor operational risk exposures and loss events.
7. Policies, processes and procedures to control or mitigate operational risks should be in place.
8. Supervisors should require banks to have an effective system to identify, measure, monitor and control operational risk.
9. Supervisors should conduct regular independent evaluations of these principles.
10. Sufficient public disclosure should be made to allow stakeholders to assess the operational risk exposure and the quality of operational risk management.

failure of the banking system in 2008. The role of that failure in the global financial crisis has been the topic of much detailed evaluation.

Measurement of operational risk

Operational risk has become a specific issue in financial institutions, because of the requirement to measure/quantify the level of operational risk that they face. The measurement of operational risk can involve a number of methods and these are normally based on historical information, simulated information or a combination of these. Table 23.2 sets out examples of operational risks faced by a bank or financial institution.

Basel II offers three alternative approaches to measuring operational risk for regulatory capital purposes, as set out below. The first two methods are a proxy for operational risk management exposure; whilst research work was undertaken to validate these methods, individual firms could vary substantially from the assessments these two methods would provide:

Table 23.2 Operational risk for a bank

Event category	Definition	Description	Examples
Internal fraud	Losses due to fraud, misappropriation or circumvention of regulations by internal party	Unauthorized activity, theft and fraud	• Unreported transactions • Unauthorized transactions • Theft and fraud • Tax non-compliance • Insider trading
External fraud	Losses due to fraud, misappropriation or circumvention of the regulations by third party	Systems security, theft and fraud	• Theft/robbery • Forgery • Hacking/theft of information
Employees	Losses arising from injury or non-compliance with the employment legislation	In a safe environment, damaged employee relations and discrimination	• Compensation claim • Discrimination allegation
Clients	Losses arising from failure to meet professional obligations to clients	Disclosure and fiduciary	• Fiduciary breaches • Disclosure violations • Misuse of confidential information
Physical assets	Losses arising from loss or damage to physical assets	Disasters and other events	• Natural disaster losses • Terrorism/vandalism
Systems	Losses arising from disruption of business or system failures	Systems	• Hardware or software failure • Telecommunications • Utility disruption
Processes	Losses from failed transaction processing or process management	Transaction capture, execution, documentation and maintenance	• Data entry, or loading error • Missed deadline or responsibility • Failed reporting obligation • Incorrect records

- *Basic indicator approach*: calculates the value of operational risk capital using a single indicator for the overall risk exposure.
- *Standardized approach*: calculates the value for operational risk, using a broad financial indicator, multiplied by operational loss experience.
- *Advanced approach*: uses the internal loss data and a combination of qualitative and quantitative methods to calculate the operational risk capital.

In order to measure operational risk, the financial institution needs to adopt a structured approach. Even after the identification of the risks, quantification is only possible if the amount of damage and risk probabilities are determined. Operational risks are hard to quantify since loss histories are usually not available and some risks cannot easily be quantified.

Many banks have undertaken detailed evaluation and quantification of their operational risks. In general, it has been discovered that the size of the bank (measured in terms of number of employees) influences the size of losses that will be suffered. This appears to indicate that larger banks tend to have larger clients. The other general trend being identified is that the number of losses is strongly correlated to the number of customers that used the bank.

Difficulties of measurement

The development of interest in operational risk has been based on the need to quantify operational risk in financial institutions. The challenges of quantifying operational risk have been considerable. Expected levels of loss can only be estimated, even if the probability of loss is fairly accurately known. Although statistical approaches have been adopted and developed, a universally accepted approach is still not available.

The expected losses can have a direct and indirect cost. Indirect costs are often larger, and include the loss of a customer. This loss can be represented by the present value of that customer and all future gains from that relationship. Actions that should be taken will include internal control measures as well as evaluation by internal audit. Internal audit within a financial institution has the familiar, but vitally important, responsibility of checking whether procedures are followed in practice and whether the procedures themselves are likely to be effective in reducing the level of operational risk.

Table 23.3 illustrates the different natures of operational risk faced by financial and industrial companies. The table provides a comparison of the nature and impact of human error in a financial institution, compared with an industrial undertaking. It is clear that the control of staff behaviour and actions is much more difficult in financial institutions than in manufacturing facilities.

Table 23.3 Operational risk in financial and industrial companies

Financial	Industrial
• Errors mostly arise when people reach their mental limits.	• Errors are mostly due to people reaching their physical limits.
• Systems are highly complex and widely distributed and the environment is only partly manageable.	• People are working in relatively simple relationships and the environment is highly manageable.
• Loss prevention is concerned with security of value and assets.	• Loss prevention is mainly concerned with physical safety, equipment protection and avoiding accidents.
• Loss prevention is aimed at avoiding financial loss.	• Loss prevention is aimed at avoiding physical harm to people or equipment and/or the manufacture of faulty goods (scrap).
• The main incentive for committing mistakes is personal financial gain or self-interest.	• The main incentive for making deliberate mistakes is reducing effort or (possibly) sabotage.
• Risk management is a key skill in financial services and has central importance to the organization.	• Risk management is not central to operations, although the aim is to avoid disruption to manufacturing processes.

It is worth noting that operational risk quantification is possible for non-financial institutions, and a transport company (for example) could investigate the operational risks associated with its activities. The risks associated with the operations include the price of fuel, tax obligations and the financial consequences of delivery mistakes. Operational risks can arise from road traffic accidents or other delivery delays and changes by the customers that have not been correctly incorporated into the delivery schedule.

It is likely that the most important operational risks faced by a transport company would be incorrect customer deliveries and road traffic accidents. The quantification of risk exposures associated with the various categories of operational risk will help a transport company focus on those risks with the greatest potential to cause disruption to normal efficient routine operations – and then take the appropriate control actions to reduce these operational risk exposures.

Developments in operational risk

It is generally accepted that operational risk concerns need to be integral to the management of a financial institution. It is often the case that management trainees within financial institutions spend some time in the risk management function, as they progress with their career in the general management side of the business. It is the intention that this involvement with risk management will create greater awareness before the individual progresses into other roles.

The measurement of operational risk in financial institutions is still proving to be a challenge, especially during the global financial crisis, which has showed that the extent of operational risk exposure was greater than most banks believed. Certain financial institutions are seeking to adopt risk management standards, such as the IRM standard and the COSO framework. Basel II does not prescribe or require any particular framework for use with operational risk management, except that the adopted framework is conceptually sound and pays high regard to integrity issues.

There are other tensions that exist with the development of operational risk within financial institutions. In many cases, the quantification of operational risk is seen as a compliance requirement rather than a business opportunity. Given that the quantification of operational risk can be quite technical, there may be a tendency for management within an organization to feel that it is the role of the operational risk manager to take responsibility for this work.

The responsibility for the management of risk and the implementation of controls usually rests with the line managers. If this responsibility is not accepted, there is a danger that operational risk management will not be fully integrated into management of the financial institution, with disastrous consequences.

Calculation of operational risk exposure is a requirement of Basel II and financial institutions, therefore, have to undertake this work. Financial institutions are driven by increasing regulatory demands and other corporate governance pressures. Raising the level of operational risk awareness by quantifying the level of risk and explaining the full significance of risk management to relevant members of staff should be to the benefit of the organization. This increased awareness will enable the organization to identify the sources of operational risk and take appropriate cost-effective actions to optimize the level of operational risk exposure.

The Risk and Insurance Managers Society (RIMS) has undertaken an evaluation of the causes of the global financial crisis. This evaluation considered the contribution that could have been made by enterprise risk management and the reasons for the failure in the application of ERM tools and techniques. The conclusions reached by RIMS are set out in the box below.

Failure of financial models

There are many ways to implement an ERM programme. The degree of success will be indicated by the competence of the risk management practices in the organization and the degree to which risk management behaviours are embedded into culture and decision making. The global financial crisis is not a failure of ERM; it was caused by the following failures:

- There was an over-reliance on the use of financial models, with the mistaken assumption that the 'risk quantifications' (used as predictions) based solely on financial modelling were both reliable and sufficient tools to justify decisions to take risk in the pursuit of profit.
- There was an over-reliance on compliance and controls to protect assets, with the mistaken assumption that historic controls and monitoring a few key metrics are enough to change human behaviour.
- There was a failure to properly understand, define, articulate, communicate and monitor risk tolerances, with the mistaken assumption that everyone understands how much risk the organization is willing to take.
- There was a failure to embed enterprise risk management best practices from the top all the way down to the trading floor, with the mistaken assumption that there is only one way to view a particular risk.

24
Supply chain management

Importance of the supply chain

Many organizations outsource major parts of their operations and support services. This can range from the use of contract cleaners through to transport, communications and manufacturing outsourcing. Many leading suppliers of fashion goods design the products and supply the finished items through franchised retail stores. All manufacturing and distribution activities are frequently outsourced to third-party providers in different parts of the world.

Because of these developments, supply chain management has become vitally important. Managing the supply chain in an increasingly globalized and competitive world can be very challenging. Uncertainties in supply and demand, globalization of marketplaces, shorter product lifecycles and rapid changes in technology have led to a higher exposure to risks in the supply chain.

All kinds of uncertainties can cause problems in the supply chain and this has increased the importance of risk management. It is impossible to eliminate risk entirely, but adequate attention to risk management matters can reduce the likelihood and magnitude of any disruption to supply. As the trend towards obtaining components and finished goods continues to lead to greater use of manufacturing facilities overseas, the corporate social responsibility issues also tend to increase.

Take the example of a sports club that has decided to outsource the procurement of merchandise sold to fans of the club. The expectation of fans is that merchandise will be desirable, available, distinctive and of appropriate quality and will represent value for money. The club itself will require that merchandise is of an appropriate quality and high availability, desirable, profitable and ethically sourced. The risks associated with the supply chain and the risks of managing conflicting stakeholder expectations need to be assessed.

The conflicting stakeholder requirements of value for money and profitability have led the club to take the decision that merchandise will have to be procured from a low-cost

manufacturer, probably based in a country with lower employment costs. However, the club may have also decided that it will not procure directly from a manufacturer, but will use a third-party procurement agency. The requirements then placed on the procurement agency will include the goods being of appropriate quality and obtained at the lowest cost available from an ethical supplier.

There are many risks associated with the course of action that the club has decided to take. There may be quality and availability issues that could cause dissatisfaction amongst fans and result in reduced sales. There are also questions of corporate social responsibility that need to be addressed. It is likely that the decision to use a third-party importer will reduce these problems, because the importer should be in a better position to establish and monitor corporate social responsibility standards.

Scope of the supply chain

Because of the increased use of outsourcing, there is an increasing interest in the risks associated with reliance on third parties. Outsourcing of operations is normally undertaken because it is assumed that costs can be reduced and risks transferred. A careful evaluation of the balance between risk and reward should be undertaken before any supply chain outsourcing decisions are taken.

The organization should be aware of the fact that outsourcing means that the organization will not only have to focus on its own risks but should also look at the risks associated with other links in the supply chain. Supply chain management and risk management are interrelated. Supply chain considerations are becoming more common, as well as much more complex.

Outsourcing of the various components of the infrastructure of an organization is only part of supply chain management. Successful management of the supply chain will rely on strategic partnerships and may also extend to joint-venture arrangements. Supply chain issues also extend to simple outsourcing decisions, such as the appointment of cleaners and caterers. There was a strong trend in the 1980s to the outsourcing of many types of facilities management within buildings.

In summary, the scope of the supply chain can extend to strategic partnerships, joint ventures, support services and outsourcing of facilities' management activities. Many organizations also choose to outsource the transportation component of their business. It is not unusual for chains of retail stores to outsource warehousing arrangements and the delivery of goods to the individual shops.

The box below is a summary of the supply chain considerations that affected Nike in the mid-2000s. The company took actions to address the ethical sourcing issues that had been raised. In order to protect its reputation, NIKE took rapid and decisive action in response to critical reports.

Nike supply chain

Nike has said that it has been facing a lot of problems with manufacturing in China with suppliers giving falsified documents, underage workers and unpaid wages topping the list. The sneakers and sportswear manufacturer, in what is believed to be its first country-specific supply chain report, has said that the company has been trying to get the Chinese suppliers to follow its code of conduct and Chinese law.

It is reported that the company's difficulties are a reflection of the depth of some of the problems faced by manufacturing businesses in China, which reportedly is Nike's largest single sourcing country, with around 180 manufacturers and about 210,000 employees, at a time when prices are rising and the legal environment is stiffening.

The report, which was posted on Nike's website, said: 'As China continues to develop we see progress and best practices emerging. But like our partners in any other country, the factories we contract with in China continue to face challenges as well.' According to the report, the company faced several labour-related problems, which included falsification of payroll records (entry of age in particular), hiring practices and the absence of a proper grievance system for workers.

Strategic partnerships

When setting up arrangements to outsource part of its operations, an organization will need to consider very carefully the selection of each strategic partner. For example, the production of an in-house magazine will be outsourced by many organizations. Depending on the importance placed on this magazine, an organization may wish to set up a strategic partnership with the publisher.

Supply chain considerations become even more important when production activities are involved. When a supermarket sets up an arrangement for the supply of manufactured goods, there are many considerations. The ability of the supply chain partner to deliver the required goods on time and within the agreed cost on a sustainable basis will be key considerations.

In order to secure exclusive supply, the supermarket may wish to enter into strategic partnerships with its suppliers. These strategic partnerships will result in the supermarket receiving priority treatment in the event of potential disruption to supply. The benefit to the supermarket of this arrangement is that continuity of supply is guaranteed and costs will be reduced. For the supplier, the benefits will be a secure market for their goods and a long-term contract. The disadvantage for the supplier is that the price may be fixed, even though the supplier could obtain a better price on the open market from time to time. There is a further disadvantage that the supplier may be dependent on orders from only one customer.

With increased focus on cost and use of 'just in time' delivery, single supplier arrangements may increase the risk of business interruption. Although organizations will wish to limit potential losses by purchasing insurance, it is unlikely that traditional insurance will adequately protect the reputation and market share of the organization in these circumstances. Therefore, organizations will need to look at business continuity strategies and developing strategic partnerships.

Joint ventures

Securing priority status from suppliers may be part of the arrangements for an organization to secure its supply chain. However, for very critical components or support operations, priority status may be insufficient. Many organizations, therefore, explore the possibility of setting up joint ventures with their suppliers in order to ensure priority supply status.

Setting up joint ventures also allows the organization to have some management control over the operation of that supplier and eliminate the possibility that the supplier will deliver goods to a competitor in difficult market conditions. Joint-venture arrangements may also be an appropriate way of responding to competitor activities by denying the competitor access to the products produced by the joint-venture partner. Joint ventures may also be a successful way of responding to technology changes in the marketplace, because the organization will not need to find all of the funding required to embrace the new technology.

These sorts of changes in the supply chain may be very significant. In fact, it may be beyond the resources of existing organizations operating in the marketplace to respond to these changes. Joint-venture operations can ensure continuity of supply chain and also, if correctly executed, deliver competitive advantage.

Outsourcing of operations

Outsourcing of non-core operations can also give rise to supply chain exposures. Table 24.1 sets out a list of considerations when setting up a contract for the supply of outsourced support. It is important that organizations consider the scope of the outsource arrangements and the range of services to be supplied. Various other features of the outsourced agreement will need to be addressed.

In many countries, there is legislation covering the protection of employees when an operation is outsourced. For example, if an organization decides to transfer the catering or the cleaning services to an outsourced company, the employment rights of staff previously employed by the organization may be protected. This can be a significant obstacle to the outsourcing of certain facilities' management and other activities and obtaining the cost reduction that would result.

Table 24.1 Risks associated with outsourcing

As a minimum, the agreement between the organization and the out-sourced service provider must address the following issues:

- scope of the arrangement
- duration of the agreement
- services to be supplied
- pricing and fee structure
- service levels and performance requirements
- transfer/implementation arrangements
- audit and monitoring procedures
- business continuity management
- confidentiality, privacy and security of information
- default arrangements and termination provisions
- dispute resolution arrangements
- liability and indemnity
- restrictions on sub-contracting
- insurance requirements

The box below considers some of the benefits of outsourcing. Outsourcing is often undertaken to save costs, but it may also be undertaken so that the work is fulfilled by a specialist company. For example, a mortgage lender may outsource property surveys to a company with great resource and more expertise.

Benefits of outsourcing

Most businesses outsource certain functions, but this is a major decision and the benefits can be difficult to define. Outsourcing can cut costs by reducing overheads and having a professional perform the operation. Although this benefit is attainable, it should not be the only reason a company decides to outsource.

The benefits of outsourcing can be divided into two types. First, there are the direct benefits of having a specialist company undertaking the outsourced activities. Then, there are the indirect benefits of giving greater focus to the core activities that remain in-house. The direct benefits of outsourcing are reduced costs, decreased cycle times and improved customer perception and satisfaction, including:

- focus on core competency;
- reduction in the cost of manufacturing and logistics services;

- reduction in head count of hourly workers and management;
- improved accuracy;
- flexibility and wider range of services;
- access to global networks and superior technology;
- improved service and quality;
- reduced capital investment and increased cash flow.

Risk and contracts

Risk management is clearly an important component when setting up supply chain contracts or deciding to outsource certain activities. The need for a detailed contract between the organization and the suppliers of the outsourced service will depend on at least the following factors:

- level of the risk associated with the contracted service;
- value of the contract for supply of goods or services;
- duration and scope of the contract;
- level of skill required in the delivery of the contracted services;
- critical nature of the goods or services that are being contracted.

The desire to achieve greater value for money and reduce costs has resulted in complex supply chains that are far more fragmented than was previously the case. Many organizations will contract out key parts of their activities, so that money can be saved and a greater level of specialist expertise is available from the outsourced company. Outsourcing also enables organizations to focus on their own core operations and competencies.

However, this has resulted in complex global supply chains that are more vulnerable to potential disruption through external sources such as terrorism, pandemics and natural disasters. Organizations need to undertake a thorough risk assessment of their supply chain and outsourcing arrangements to ensure that the risks associated with these contracted services are adequately managed. Remember that contracting out the supply of goods or services does not transfer all of the risks.

Outsourcing arrangements should be introduced only when it is the cost-effective and efficient way of running the business. Outsourcing decisions based on a belief that risks are being completely transferred to a third party may prove to be incorrect. Damage to reputation may still be suffered if the outsourced manufacturing activity produces substandard goods.

For example, an organization that decides to have manufacturing undertaken in a lower-cost territory may discover that the goods produced do not comply fully with safety requirements. There have been examples of toys manufactured in one part of the world that were illegal in the country where the toys were to be sold because of the use of lead-based paint.

It is possible that the cost of supply will be reduced, but the risks may actually be increased. When contracting out services and supply, the organization needs to be satisfied that the risks associated with this transfer are within the risk appetite of the organization, and also within its risk capacity. Finally, evaluation should be undertaken to determine the actual risk exposures that are associated with increasingly complex supply chain arrangements.

Case study

Hercules Incorporated – outsourcing logistics

Odyssey Logistics & Technology Corporation, a provider of outsourced logistics management services to process manufacturers, today announced that Hercules Incorporated, a $1.7 billion chemical manufacturer and marketer, has signed a five-year, multimillion-dollar contract to outsource its North American import and export transportation and logistics operations to Odyssey.

As Hercules' contract transportation arm, Odyssey will provide all necessary services to ship product from Hercules' manufacturing plants and other shipping facilities to its global customers. Hercules' four divisions are focused on providing chemicals and other materials for industrial manufacturers in markets such as pulp and paper, personal care products, paints, carpets and adhesives.

In 2002, Hercules forged a renewed focus on its core business units and decided to outsource its transportation functions for three compelling business reasons: to achieve more insight into its global supply chain costs; to reduce its transportation costs by gaining increased leverage in negotiating rates with its multimodal carrier network; and to deploy its own expertise in the business of manufacturing chemical products and meeting its clients' needs.

Prior to outsourcing to Odyssey, Hercules worked with a variety of third-party logistics providers who were focused on one or two modes of transportation. Unlike Odyssey, they were not connected to one another and could not provide Hercules with a holistic view of its multimillion dollar transportation spend.

Odyssey's transportation management solution interfaces directly with Hercules' enterprise resource planning application, incorporating the order management system directly into its freight planning solution. The technology integration provides the critical link to allow Hercules senior executives to have one view of the transportation supply chain.

Odyssey is a full-service third-party logistics provider with capabilities in all transportation modes – truck, rail, ocean and air. The company has significant experience supporting the requirements of the chemical industry where the movement of liquids and dry bulk are often an important part of the product mix.

Odyssey Logistics & Technology Corporation 2008

Part 5

Risk response

Learning outcomes for Part 5

- provide alternative definitions of enterprise risk management (ERM) and identify the key features of an enterprise-wide approach;
- describe the 10 steps in the implementation of a successful ERM initiative, as set out in more detail in Appendix B;
- outline the importance of risk appetite as a planning tool in the implementation of a risk management initiative;
- describe the relationship between risk appetite, risk exposure and risk capacity and the interface with operations, projects and strategy;
- describe the risk response options in terms of tolerate, treat, transfer and terminate, and explain how these can be shown on a risk matrix;
- describe the types of controls that are available, in terms of preventive, corrective, directive and detective (PCDD) controls;
- explain how to determine whether controls are cost-effective, how controls change loss expectancy and how to learn from controls;

- provide practical examples of the control of selected hazard risks, including risks to finances, infrastructure, reputation and marketplace;
- describe the importance of insurance and the circumstances in which insurance is purchased, including the involvement of a captive insurance company;
- explain the importance to the insurance purchasing process of cost, coverage, capacity, capabilities, claims and compliance.

Part 5 Further reading

Association of Insurance and Risk Managers (2006) Insurance Buyers Guide, www.airmic.com.
COSO Enterprise Risk Management – Integrated Framework (2004) Executive Summary, www.coso.org.
HM Treasury (2004) Orange Book: Management of Risk – Principles and concepts, www.hm-treasury.gov.uk.
Vance and Makomaski (2007) Enterprise Risk Management for Dummies, Wiley Publishing, www.wiley.com.

25
Enterprise risk management

Enterprise-wide approach

In the past few years, there have been important developments in the practice of risk management. Firstly, there has been the development of specialist branches of risk management, including project, energy, finance, operational risk and clinical risk management. Secondly, organizations have embraced the desire to take a broader approach to the practice of risk management.

Various terms have been used to describe this broader approach, including holistic, integrated, strategic and enterprise-wide risk management. It is the term enterprise or enterprise-wide risk management (ERM) that is now the most widely used and generally accepted terminology for this broader approach. The fundamental idea behind the ERM approach is to move away from the practice of risk management as the separate management of individual risks.

ERM takes a unifying, broader and more integrated approach. The ERM approach means that an organization looks at all the risks that it faces across all of the operations that it undertakes. ERM is concerned with the management of the risks that can impact the objectives, key dependencies or core processes of the organization. Also, ERM is concerned with the management of opportunities, as well as the management of control and hazard risks.

There has also been consideration of the fact that many risks are interrelated and that traditional risk management fails to address the relationship between risks. With the ERM approach, the relationship between risks is identified by the fact that two or more risks can have an impact on the same activity or objective. The ERM approach is based on looking at the objective, key dependency or core process and evaluating all of the risks that could impact the item being evaluated.

An example of the ERM approach is to consider a sports club where the core process is to maximize attendance at games. This process is made up of several activities, including marketing, advertising, allocation and sale of tickets as well as logistical arrangements to ensure that

the experience at the game is as good as possible. Part of maximizing attendance at games will be to ensure there are adequate parking and transport arrangements, together with suitable catering and other welfare arrangements in the ground.

By identifying the key activities that deliver the selected core process, the club is able to identify the risks that could impact both these activities and the core process. Targets can then be set for increased attendance at future games and responsibility for the success of this core process has been allocated to the Commercial Director of the club. A consideration of the opportunities for increasing attendance at games can also be included in this broader approach.

Definitions of ERM

Table 25.1 presents a number of suggested definitions of enterprise risk management. There are three components that are required in a comprehensive definition of ERM. These are: 1) the description of the process that underpins enterprise risk management; 2) identification of the outputs of that process; and 3) the impact (or benefit) that arises from those outputs.

Table 25.1 Definitions of enterprise risk management

Organization	Definition of enterprise risk management
BS 31100	Enterprise risk management is the approach to managing all of an organization's key business risks and opportunities with the intention of maximizing stakeholder value.
ACT (Association of Corporate Treasurers)	Enterprise risk management is designed to enhance corporate decision-making with tools being developed and implemented to support actions ranging from optimization of the insurance programme to analysis of overseas expansion plans, business mix or capital allocation.
COSO ICAEW (Institute of Chartered Accountants in England and Wales)	Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, manage risk to be within its risk appetite and to provide reasonable assurance regarding the achievement of entity objectives.
IIA (Institute of Internal Auditors)	A rigorous and co-ordinated approach to assessing and responding to all risks that affect the achievement of an organization's strategic and financial objectives.
HM Treasury	All the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them and monitoring and reviewing progress.

Many of the definitions concentrate on the process by describing the activities that make up the ERM approach. This is a good starting point, but the outputs from that process are more important than the process itself. Some of the definitions do include reference to the outputs from the process, such as being able to manage risks within the risk appetite of the organization and provide reasonable assurance regarding the achievement of objectives.

To be comprehensive, however, the definition must also consider the intended impact of those outputs. In summary, the intended outputs from ERM are that better decisions will be taken, correct processes will be identified and introduced, possibly by way of projects, and operations will be efficient and free from unplanned disruption. This list of outputs can be described as compliance, assurance, decisions and efficiency/effectiveness/efficacy (CADE3).

The following is offered by way of a comprehensive definition of ERM:

- ERM involves the identification and evaluation of significant risks, assignment of ownership, completion and monitoring of mitigating actions to manage these risks within the risk appetite of the organization.
- The outputs are the provision of information to management to improve business decisions, reduce uncertainty and provide reasonable assurance regarding the achievement of the objectives of the organization.
- The impact of ERM is to improve efficiency and the delivery of services, improve allocation of resources (capital) to business improvement, create shareholder value and enhance risk reporting to stakeholders.

ERM in practice

The developing role of the risk manager has been discussed in Chapter 9. It was mentioned that the seniority of the risk manager should be proportionate to the risks that the organization faces. For many organizations, including those in finance and energy, a board-level risk manager is often appropriate.

Where it is appropriate and proportionate, the risk manager at board level is often referred to as a chief risk officer (CRO). To date, these appointments have been almost exclusively in the energy and finance sectors, although this may change as ERM becomes more clearly established in a wider range of organizations.

The seniority of the CRO is just one example of how ERM should be achieved in practice. The principles of risk management set out as PACED are fully applicable to the practice of enterprise risk management. The principles of risk management are that it should be proportionate, aligned, comprehensive, embedded and dynamic (PACED).

By taking a comprehensive approach to enterprise risk management, a wide range of benefits can be delivered and these are set out in Table 25.2. It is for each organization to decide how the enterprise risk management initiative will be structured and how these benefits will be achieved.

The key feature of ERM is that the full range of significant risks facing the organization is evaluated. The interrelationship between risks should be identified, so that the total risk exposure of the organization may be compiled. Having measured the total risk exposure of the organization, that level of risk exposure can then be compared with the risk appetite of the board and the risk capacity of the organization itself.

Table 25.2 Benefits of enterprise risk management

FIRM risk scorecard	Benefits
Financial	• Reduced cost of funding and capital • Better control of CapEx approvals • Increased profitability for organization • Accurate financial risk reporting • Enhanced corporate governance
Infrastructure	• Efficiency and competitive advantage • Achievement of the state of no disruption • Improved supplier and staff morale • Targeted risk and cost reduction • Reduced operating costs
Reputational	• Regulators satisfied • Improved utilization of company brand • Enhanced shareholder value • Good reputation and publicity • Improved perception of organization
Marketplace	• Commercial opportunities maximized • Better marketplace presence • Increased customer spend (and satisfaction) • Higher ratio of business successes • Lower ratio of business disasters

ERM and business continuity

There is an important relationship between enterprise risk management (ERM) and business continuity management (BCM). The risk assessment that is required as part of the risk management process and the business impact analysis that is the basis of business continuity planning (BCP) are closely related.

The normal approach to risk management is to evaluate objectives and identify the individual risks that could impact these objectives. The output from a business impact analysis is the identification of the critical activities that must be maintained for the organization to continue to function.

Based on the definition of enterprise risk management set out above and the fact that enterprise risk management should be applied to the evaluation of core processes, it can be seen that the ERM approach and the business impact analysis approach are very similar, because both approaches are based on the identification of the key dependencies and functions that must be in place for the continuity and success of the business.

The next stage in the process differs between ERM and BCP, because the former is concerned with the management of the risks that could impact processes, whereas business continuity is concerned with actions that should be taken to maintain the continuity of individual activities. The business continuity approach, therefore, has the very specific function of identifying actions that should be taken after the risk has materialized in order to minimize its impact. Business continuity planning relates to the damage-limitation and cost-containment components of the loss control, as described earlier.

ERM in energy and finance

Risk management in the energy and finance sectors has become a well-developed specialist branch of the discipline. In the finance sector, the objective of an ERM initiative is to enhance shareholder value by:

- improving capital and efficiency by providing an objective basis for allocating resources and exploiting natural hedges and portfolio effects;
- supporting financial decision making by considering areas of high potential adverse impact and by exploiting areas of risk-based advantage;
- building investor confidence by stabilizing results and protecting them from disturbances and thus demonstrating proactive risk stewardship.

ERM in the energy sector is often dependent on the treasury function and the specialist expertise of hedging against the price of a barrel of oil. This area of financial risk management has

become well established, with very large departments being set up in many energy companies. However, the practice of ERM in energy companies still remains very closely related to the management of treasury risks.

One of the drivers for risk management in the finance sector is the regulatory environment. Banks have been subjected to Basel II for some time, and the insurance sector in Europe is about to be subjected to similar requirements set out in the Solvency II Directive. This gives rise to the obligation on financial institutions to measure their exposure to operational risk.

The output of operational risk management (ORM) activities in financial institutions is the ability to calculate the capital that should be held in reserve to cover the consequences of the identified risks materializing. The impact of these ORM activities is that risks will be better identified and managed, so that the capital required to meet the consequences of the risks materializing is lowered. ORM within financial institutions can be seen as a particular application of the ERM approach.

The failure of the world banking system called into question the effectiveness of risk management activities in banks and, in particular, the effectiveness of operational risk management. One of the consequences of the world financial crisis is that the news reports now routinely state that: 1) risk is bad; and 2) risk management has failed. In fact, taking risk is essential for the success of organizations.

The statement that risk management has failed in banks is more difficult to contradict. However, the reality is that it was not the failure of risk management principles that caused the banking crisis. It was the failure to correctly apply those principles. Many banks made two simultaneous mistakes:

- An accurate risk and reward analysis was not undertaken, so that banks made decisions on the basis of the rewards available, rather than taking a more balanced view of the risks involved in seeking those higher rewards.
- Quantification of the level of risk involved was not accurate, because the banks were taking such a risk-aggressive approach that certain events were considered to be so unlikely that they could be ignored.

Detailed analysis of the banking crisis in 2008 is outside the scope of this text. However, it appears that the crisis was caused by the failure of two different sets of risk analysis models. Firstly, the banks had assumed that re-packaged debts, including sub-prime mortgages, would continue to be tradable commodities in the market, but this proved not to be the case.

Secondly, the banks assumed that short-term borrowing on the wholesale money markets would continue to be available. This short-term money is used by banks so that they can continue to lend money on a long-term basis, at a more profitable rate. The collapse of the wholesale money markets was not anticipated by the credit models used by most banks.

Future development of ERM

The COSO ERM cube represents a framework for undertaking enterprise risk management, although there is insufficient description in the COSO model of the risk management process itself. However, the COSO approach is becoming more widespread because the COSO Internal Control framework (1992) is the preferred approach for compliance with the requirements of the Sarbanes–Oxley Act. US companies that have subsidiaries around the world frequently require that their subsidiaries adopt the COSO approach.

Other important developments in risk management are the publication in 2008 of British Standard BS 31100 and the publication in 2009 of the ISO risk management standard, ISO 31000. ISO 31000 was adopted by Standards Australia to replace the previously available and well-established Australian Standard AS 4360 (2004) that was first published in 1995. The approach in ISO 31000 is very similar to the approach described in British Standard BS 31100.

Future developments in the practice of ERM are likely to be focused on two key areas: firstly, ensuring risk management activities are fully embedded in the business processes of the organization; and secondly, demonstrating measurable financial benefits associated with the implementation of an enterprise risk management initiative. The embedding of ERM in the organization is achieved by leadership, involvement, learning, accountability and communication (LILAC). Developments in the practice of operational risk management are probably leading the way in the measurement of the total risk exposure of an organization.

In summary, the discipline of enterprise risk management has become established and is here to stay, but it has to be able to demonstrate significant and measurable financial benefits. These financial benefits need to be demonstrated in the form of increased profit in private sector organizations and in the form of the enhanced efficiency and/or value for money delivery of services in the public sector. The box below suggests the keys to success in ERM.

Successful ERM initiatives

How leading organizations develop an ERM programme; define a governance model and support structure; collect, analyse, and share ERM information; and gauge success. The following were the keys to success:

- Maturity of ERM capabilities enables partner organizations to be more agile and flexible in responding to business needs.
- ERM is not a stand-alone or discrete activity, but a part of everyday life – a performance improvement effort.
- Effective ERM is conducted at the corporate level in order to communicate policy and provide support to the entire organization.

- ERM is successful when championed at the enterprise level and owned by the CEO and board of directors.
- Formal ERM is provided in ERM, so that risk management is part of the strategic planning process and everybody becomes a risk manager.
- Mature ERM practices leverage technology to automate data capture and report risk measures.
- Measurement frameworks provide a comprehensive understanding of the value of ERM.

26
Importance of risk appetite

Risk capacity

Many commercial organizations make adequate profits, but take too much risk or make inappropriate use of the risk capacity of the organization. Risk capacity, or the capability of the organization to take risk, is not the same as the cumulative total of all of the individual values at risk associated with the risks facing the organization. This cumulative total is the risk exposure of the organization.

By contrast risk appetite is the total value of the corporate resources that the board of the organization is willing to put at risk. Most organizations have not determined the value they should risk (risk appetite), nor calculated how much value is actually at risk (risk exposure), nor the capability of the organization to take risk (risk capacity).

An organization should be able to decide how much it wishes to put at risk. Agreeing the risk appetite will ensure that the organization does not put too much (or too little) value at risk. The risk capacity of the organization needs to be fully utilized to ensure that risk taking is at the optimal level and delivers maximum benefit. Similarly, the organization should not put more value at risk than is appropriate, given the sector in which it operates and prevailing market conditions.

Figure 26.1 represents the relationship between risk and uncertainty. It illustrates the typical range of outcomes for hazard risks, control risks and opportunity risks. By including all three types of risk in a single figure, it is possible to demonstrate that the three types of risk are related, interdependent and form a continuum. The sum of all of the hazard tolerances, control acceptances and opportunity investments will represent the total risk appetite of the organization.

The curved lines in Figure 26.1 represent the range of possible outcomes for each risk position, to within a 95 per cent certainty. An organization may decide that it has a risk appetite such that it is willing to tolerate a hazard risk shown at point A. Risk appetite point A represents the

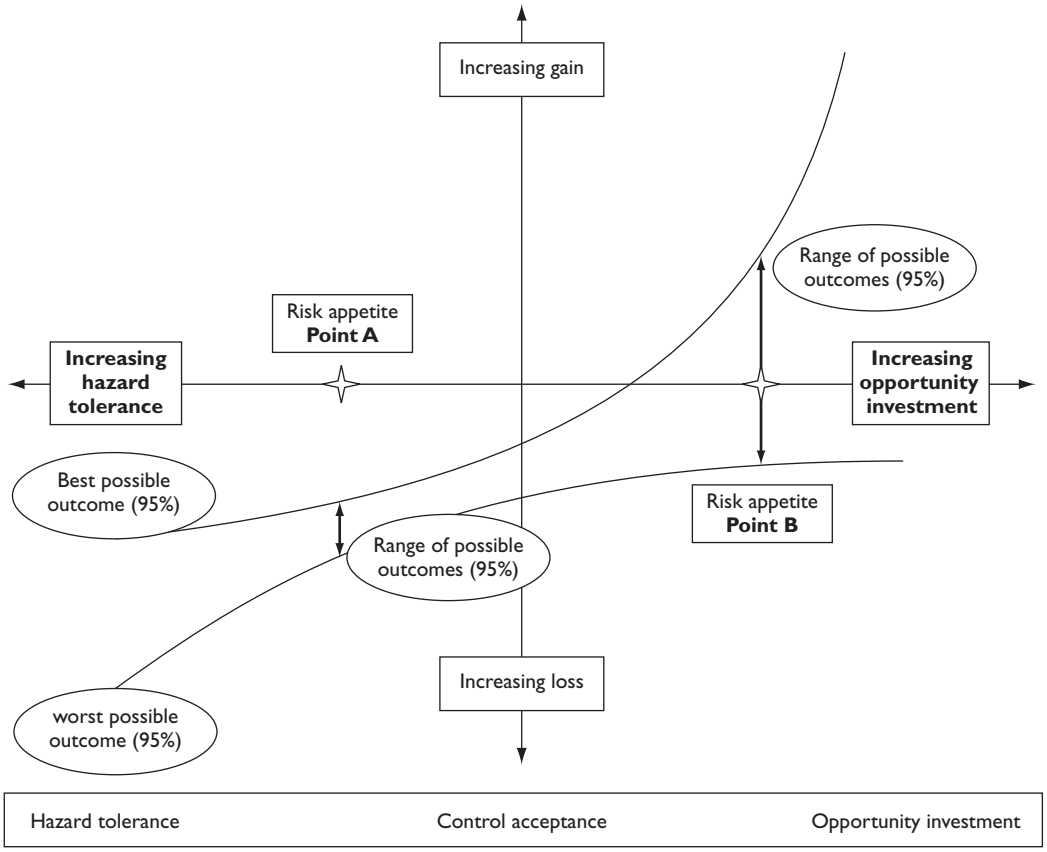


Figure 26.1 Risk and uncertainty

risk appetite for that type of hazard risk. In setting a risk appetite, the organization will realize that a range of outcomes for that risk appetite is possible. That range of outcomes is shown as the 95 per cent certainty lines.

Likewise, in pursuit of an opportunity, the organization will have an appetite presented by point B. Again, there will be a range of possible outcomes for this opportunity investment. The intended outcome is a positive return, but a loss may be suffered if the investment is not successful. The range of possible outcomes is demonstrated by the 95 per cent certainty lines. Figure 26.1 is used to demonstrate that a range of outcomes is possible when a value is put at risk. This figure also provides the basis for demonstrating the contribution of risk management (discussed below and shown in Figure 26.5) that plots risk management and uncertainty.

Risk exposure

Total cost of risk (TCR) calculations were commonplace in the 1980s. These calculations were usually undertaken by organizations or their insurance brokers. They enabled an organization to determine the total cost of hazard risks to the organization. The calculation had three main components: insurance premium; money spent on loss-control actions, and cost of claims not covered by insurance.

Tables were published on total cost of risk in various organizations and it was possible to benchmark the performance of an organization against other companies in the same sector. This sort of total cost of risk calculation was useful and was often used as a justification for setting up an in-house or captive insurance company, as discussed in Chapter 30.

The difficulty with this type of calculation was that it depended substantially on historical information. Historical loss data is not necessarily a good guide to future loss performance. This approach was intended to encourage organizations to seek the lowest overall cost for the management of hazard risks. Unfortunately, this lowest-cost approach often proved to be a mistake when a major incident occurred.

Organizations should be aware that the TCR calculation could represent the lowest cost for the management of hazard risks, but that might be achieved at a high overall risk position. It is worth noting that the purchase of too much insurance could represent a position for the organization that is the lowest risk position but achieved at a high overall cost.

The type of total cost of risk calculation undertaken by organizations is now somewhat different. Organizations often use the concept of risk appetite to undertake calculations that identify the level of risk that the organization is willing to accept. The risk appetite of the board can then be compared with the actual risk exposure that the organization faces. The actual risk exposure in this calculation is an updated version of the total cost of risk calculation, but should include all types of risks – not just those that can be insured.

Generally speaking, as the marketplace becomes more volatile, the organization will be forced to increase its risk exposure. This requires a discussion in the boardroom leading to an agreement to increase the total value that the organization is willing to put at risk and/or to find mechanisms to reduce the total risk exposure. As a consequence, risk management becomes more important in times of rapid change and increased marketplace volatility.

Risk exposure will also increase when an organization decides whether to embark on a merger or acquisition. Organizations need to undertake an opportunity analysis of all acquisition opportunities and this analysis should include consideration of at least the following features of the acquisition opportunity:

- financial strength and reputation of the proposed acquisition;
- potential for developing further revenue/profit from the acquisition;

- risks associated with suggested purchase contract terms and conditions;
- anticipated profitability and sustainability of the proposed acquisition;
- investment required to deliver the anticipated future plans for the acquisition;
- impact on existing investment and business development plans.

Risk exposure is the actual cumulative total at risk, but it is often calculated on a risk-by-risk basis, without consideration of whether the risks are correlated. An organization will need to allow for correlation of risks and thereby take account of the likelihood of the risks materializing. When calculating the total actual risk exposure of the organization, it is important that the cumulative total of the values at risk is adjusted to take account of whether risks are correlated.

Nature of risk appetite

Organizations face a number of risks that can cause disruption. These are the hazard risks that have been discussed throughout this book and give rise to the organization having a hazard tolerance. In other words, the organization will be willing to accept exposure to certain hazard risks as part of its normal operations. British Standard BS 31100 defines risk appetite as the 'amount and type of risk that an organization is prepared to seek, accept or tolerate'.

There will be a cost associated with hazard risks, both in terms of the cost of incidents that do occur and also in terms of the cost of loss-prevention, damage-limitation and cost-containment activities, including insurance costs. For each hazard risk, there will be a range of possible outcomes, all of them negative and this is illustrated in Figure 26.1.

The organization will need to quantify the possible hazard risks and costs associated with those risks. It should be able to decide how much hazard risk it will tolerate and this is part of the total risk appetite. Although the organization may decide how much hazard risk it will tolerate, the actual exposure to hazard risks may be greater than the anticipated.

Also, all organizations face uncertainties and the control risks that give rise to these uncertainties. These are risks linked to events that, if they materialize, will have uncertain outcomes. As an example of control risks, if all fraud controls in an organization were removed, there would be a net saving represented by the cost of the controls. However, fraudulent behaviour might result and substantial losses might be suffered, but there would be uncertainty about how much fraud would actually result from the removal of all controls.

There will be control risks embedded within the projects that the organization is currently undertaking. The cost of necessary controls may be part of the overall budget for a project. When planning a large project, it would be unwise not to include the cost of necessary controls

in the budget for the project. The cost of the controls within the project budget represents the control acceptance of the organization.

The portion of risk appetite that is associated with opportunities can be considered to be the opportunity investment that the organization is willing to embrace. Organizations will be willing to invest resources in opportunities that the organization believes will produce a positive gain. However, the organization should recognize that value put at risk in this way may not produce a positive gain. Implementation of strategic decisions may result in losses. In fact, more value can be destroyed by incorrect strategic decisions than by hazard or control risks.

Figure 26.1 illustrates the range of outcomes for different risk exposures. In relation to opportunity investment, a range of outcomes are possible from complete loss of the invested resources to a substantial gain. Sometimes, the losses may exceed the initial investment, if the total negative risk exposure associated with the investment was not correctly calculated.

The organization may have an appetite for investing a sum of money in an opportunity, but it needs to be sure that it has the capacity to endure any loss that may result. It also needs to be sure that the total amount invested, or value at risk, is not beyond the capacity of the organization. Careful calculation of the actual risk exposure associated with the opportunity should be undertaken.

Figure 26.2 illustrates the concepts of risk appetite, risk exposure and risk capacity. Risk appetite is illustrated by way of shaded squares on the risk matrix and the overall risk exposure of the organization is shown as a curved line. This illustration represents risk appetite, exposure and capacity for a risk-averse organization.

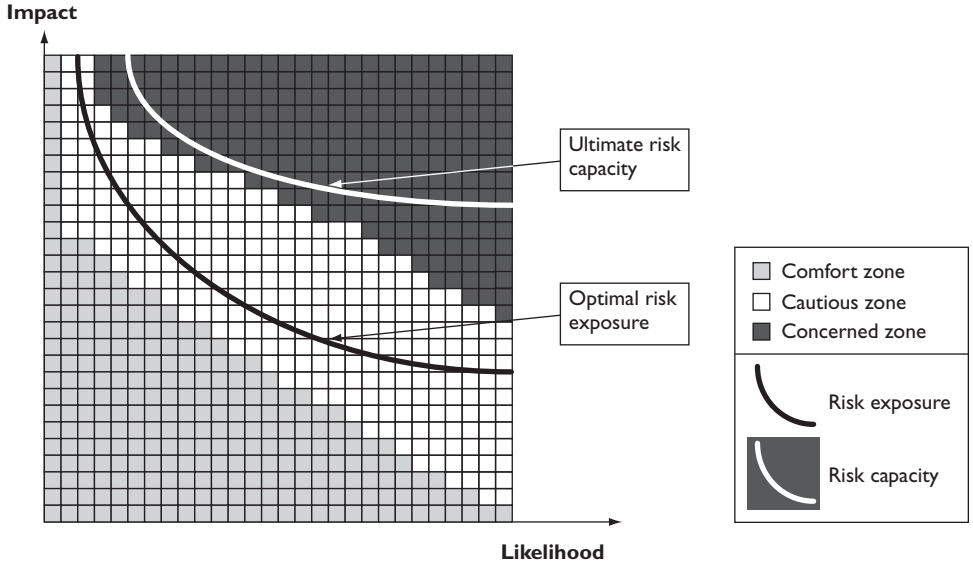


Figure 26.2 Risk appetite, exposure and capacity (optimal)

The lighter area represents a situation where the organization is comfortable with taking the risk. The medium-shaded area represents a cautious zone, where management judgement is required before the risk is accepted. Accepting risks in the darker area will cause the organization concern, and these risks will only be accepted when there is a business imperative.

The curved lines in Figure 26.2 represent the overall risk exposure of the organization and this is the optimal position, where the overall exposure cuts through the lighter section. The risk capacity of the organization is shown as higher than both the risk appetite and the risk exposure and is embedded well in the darker area. This represents an optimal state of affairs. This ensures that the organization is taking risks that are within the appetite of the board and not exceeding the ultimate risk capacity of the organization.

Figure 26.3 represents a risk-aggressive organization with a much larger comfort zone for accepting risk. The lighter-shaded or cautious zone is smaller and the darker zone is an even smaller part of the overall figure. This situation can be described as representing an approach to risk that has a very limited universe of risk. The universe of risk for the organization is represented by the darker squares and it is only in this area that the board of the organization will consider that the risks are significant.

In Figure 26.3, the ultimate risk-bearing capacity of the organization is shown as within the medium-shaded zone. This represents a situation where the organization may be taking risks that are beyond the ultimate risk capacity of the organization. To make circumstances worse, the actual risk exposure of the organization is shown as well within the darker area. This makes the organization vulnerable to risk, because its actual risk exposure is shown to be well beyond its ultimate risk-bearing capacity.

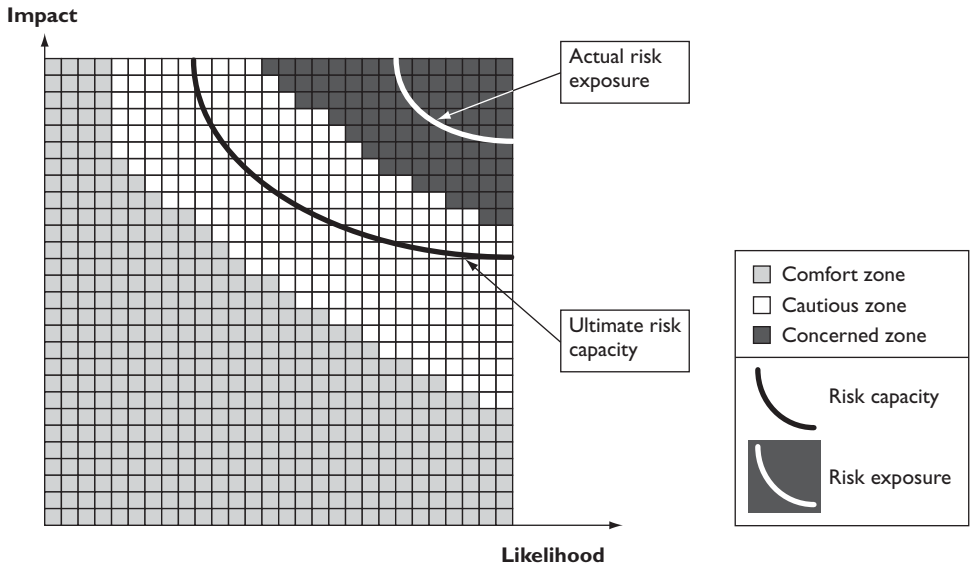


Figure 26.3 Risk appetite, exposure and capacity (vulnerable)

The identification of the risk appetite for the organization requires judgement, and this judgement can be exercised at different levels within the organization. Consideration of risk appetite will be a strategic driver at board level. Risk appetite is likely to be an operational constraint at line-manager level because line managers will be expected to operate within the risk appetite policy that has been established by the board.

At the individual level, it is likely that consideration of risk appetite will be a behaviour regulator. This is because individual members of staff should only operate within the risk appetite framework that has been developed at board level and is implemented by line managers.

Cost of risk controls

The inherent level of a risk is the level of the risk with no control measures in place. This is sometimes referred to as the gross level of the risk. The current level of risk is the level that takes account of the control measures currently in place. This is sometimes referred to as the net level of risk or the residual risk. Throughout this book, 'current level' has been used instead of 'residual level', because this implies a much more dynamic approach to risk management.

Figure 26.4 provides an illustration of the control effect or control vector when controls are put in place. When considering the current and target risk levels, the organization should be aware of the cost involved in implementing the controls that have been identified. The cost of the control measures should be considered to be part of the total cost of risk for the organization. The organization can then evaluate whether the controls in place are cost-effective.

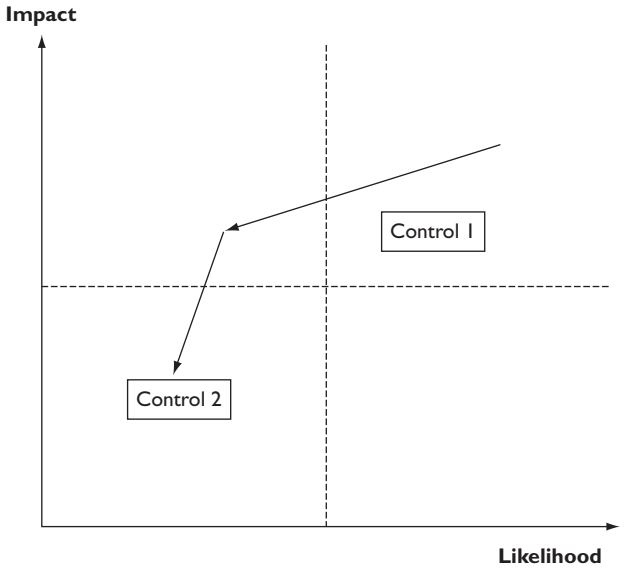


Figure 26.4 Illustration of control effect

As can be seen in Figure 26.4, a line can be drawn to represent the effect of each individual risk control measure. It is obvious that the longer the line, the greater the effect of the control. It will also be the case that the longer the line, the greater control effort is required, in terms of management time, effort and money.

A simple diagram like Figure 26.4 provides an illustration of the distance between the inherent and current level of the risk. If a target level of risk is established, additional control effort would be required in moving the level of risk from the current to the target level. This simple illustration of control effort is important, and demonstrates that there is value in undertaking a risk assessment at the inherent level of risk (if this is possible) so that the required control effort can be clearly identified and illustrated.

If a calculation is undertaken of the risk exposure at the original level and a further calculation is undertaken of the risk exposure at the new level, the overall benefit of each control can be measured. Consideration of the cost of each control can then be undertaken, so that a cost–benefit analysis of individual controls may be completed. This will be an important exercise for the organization to undertake, so that cost-effective risk control priorities may be established.

Risk management and uncertainty

Reducing uncertainty is at the heart of risk management. In fact, British Standard BS 31100 defines risk as the 'effect of uncertainty on objectives'. Although management of uncertainty should only be considered to be a part of the risk management approach, it is vitally important. A component of reducing uncertainty in an organization is to manage and reduce the level of inconsistency in the way risks are managed.

For an organization that is highly regulated, detailed systems and procedures will be produced and these will be monitored by the regulator. These rules and procedures represent the controls that must be in place. Part of successful risk management is to ensure that these controls are always implemented and a high level of consistency is achieved in relation to staff behaviour.

The overall approach of risk managers is to facilitate the identification of the significant risks faced by the organization. Risk managers tend to take the approach that risk assessment is complete when existing controls have been identified and the need for any additional controls has been documented. However, different controls have different levels of effectiveness and efficiency.

An alternative, but complementary, approach to the management of significant risks is to use risk assessment as a tool that ultimately leads to the identification of the critical controls for the organization. The critical controls are the most important controls in relation to the management of the significant risks.

Figure 26.5 illustrates the effect of risk management on the uncertainty. In effect, this figure demonstrates the value of critical controls in changing the range of possible outcomes at a particular level of risk exposure. The identification of critical controls is important, because staff and managers may be more concerned about the implementation of the critical controls than the details of the risk assessment that identified those controls.

Figure 26.5 illustrates the contribution of different control mechanisms and the effect that those mechanisms have on the range of possible outcomes. The impact of loss control and insurance on hazard risks is shown. The contribution of opportunity management and hedging or joint ventures on opportunity risks is also shown.

The approach based on the identification and evaluation of critical controls is closely aligned to the activities of the internal audit. It is worth remembering that internal auditors prefer to

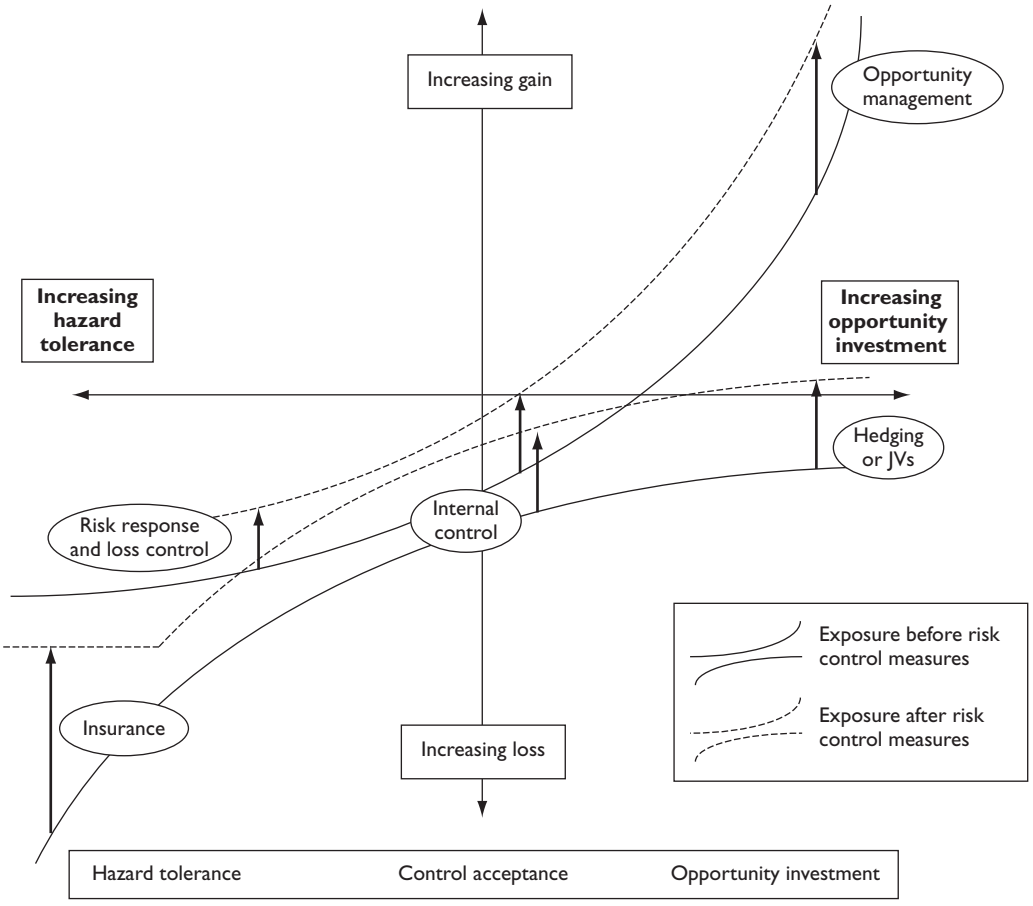


Figure 26.5 Risk management and uncertainty

undertake a risk assessment of the inherent level of risk, assuming that there are no controls in place. This is a valuable approach, because it identifies critical controls. The difficulty is that it is sometimes impossible to identify the inherent level of risk, or it is sometimes the case that such an approach is not helpful because it becomes too theoretical.

Risk appetite and lifestyle decisions

There is a relationship between personal risk appetite and lifestyle decisions. Decisions will be taken about, for example, long-term health issues, depending on family history and personal lifestyle. Decisions will also be taken on medium-term health issues, based on medical treatment, dieting and weight gain. Short-term decisions will also need to be taken on health issues, including those related to exercise, alcohol and recent illness or accident.

Individuals will need to take lifestyle decisions based on risk appetite, risk exposure and risk capacity. In relation to health issues, decisions will need to be taken on the level of exercise that the individual is willing to take in the short term to maintain weight within a healthy range.

There may be a certain appetite for risk issues associated with health and well-being, but the exposure that an individual actually suffers may be greater than the appetite for such risks. For example, people are willing to smoke cigarettes, but also wish to develop a healthier lifestyle. This is an example where the appetite for risk may be less than the actual risk exposure.

There is a tendency for people to take a course of action when the outcome is immediate, positive and certain. Therefore, a smoker will want a cigarette because the nicotine effect will be immediate, positive and certain. In contrast, giving up smoking will probably result in long-term benefit, but that benefit will be delayed and uncertain and there will also be negative feelings of being without nicotine.

The box below describes attitudes of individuals to the risks associated with lifestyle decisions. This demonstrates that the attitude of people to risk taking will vary considerably depending on the type of risk that is being considered. For example, individuals may be very risk averse in the way they drive their cars, but accept significant risk factors in relation to their health.

Health risk factors

The number of Canadians who are overweight or obese has increased dramatically over the past 25 years. Obesity is a risk factor in a number of chronic diseases. Achieving and maintaining a healthy weight is important to reduce the risk of those diseases and improve overall health.

Although smoking remains the greatest threat to public health in Canada, poor eating habits, physical inactivity and their contribution to obesity are also critical public health challenges. Statistics Canada reports that two out of every three adults in Canada are overweight or obese.

Many factors have contributed to the increasing rates of overweight and obesity. Changes in society, work and leisure have affected activity and eating patterns, leading to a rise in excessive weight and obesity. There has been a shift towards less physically demanding work, as well as an increased use of automated transport and passive leisure activities, such as television viewing and playing video games.

27
Tolerate, treat, transfer and terminate

The 4Ts of hazard response

Priority significant risks facing an organization are those that have:

- high or very high impact in relation to the benchmark test for significance;
- high or very high likelihood of materializing at or above the benchmark level;
- high or very high scope for cost-effective improvement in control.

Generally speaking, it is only priority significant risks that require attention at the most senior level of the organization. However, it is appropriate that regulatory risks also receive boardroom attention. In practice, the board will expect these regulatory risks to be properly managed and the board will only receive routine/annual reports describing risk performance, or a special report if a specific issue has arisen.

The benchmark test for significance should be set at a level that represents a significant impact for the organization. Having identified the priority significant risks, the organization then needs to review the controls in place and decide whether further actions are required. For hazard risks, the range of responses available is often described as the 4Ts.

There is a broad range of terminology available to describe risk response options. In fact, both British Standard BS 31100 and ISO 31000 use the term risk treatment as the more generic description. For example, the British Standard defines risk treatment as the 'process of developing, selecting and implementing controls'. Likewise, ISO 31000 defines risk treatment as 'development and implementation of measures to modify risk'.

The terminology used in the Orange Book has been adopted for this text for the risk response stage of the risk management process. The options for responding to risk can then be identified as the 4Ts. Appendix A contains information on the alternative definitions that are used by different publications.

More information and a brief description of each of the 4Ts is provided in Table 27.1. The 4Ts of hazard risk management can be summarized as:

- Tolerate;
- Treat;
- Transfer;
- Terminate.

Figure 27.1 suggests that there is a dominant response in relation to each of the 4Ts, according to the position of the risk on a risk matrix. For risks that are low likelihood/low impact, the main response is tolerate. For risks that are high likelihood/low impact, the main response is treat. For risks that are low likelihood/high impact, the main response is transfer, and for risks that are high likelihood/high impact, the main response is terminate.

Table 27.1 Description of the 4Ts of hazard response

1.	***Tolerate*** **Accept/retain**	The exposure may be tolerable without any further action being taken. Even if it is not tolerable, the ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained.
2.	***Treat*** **Control/reduce**	By far the greater number of risks will be addressed in this way. The purpose of treatment is that, whilst continuing within the organization with the activity giving rise to the risk, action (control) is taken to constrain the risk to an acceptable level.
3.	***Transfer*** **Insurance/contract**	For some risks the best response may be to transfer them. This might be done by conventional insurance, or it might be done by paying a third party to take the risk in another way. This option is particularly good for mitigating financial risks or risks to assets.
4.	***Terminate*** **Avoid/eliminate**	Some risks will only be treatable, or containable to acceptable levels, by terminating the activity. It should be noted that the option of termination of activities may be severely limited in government when compared to the private sector.

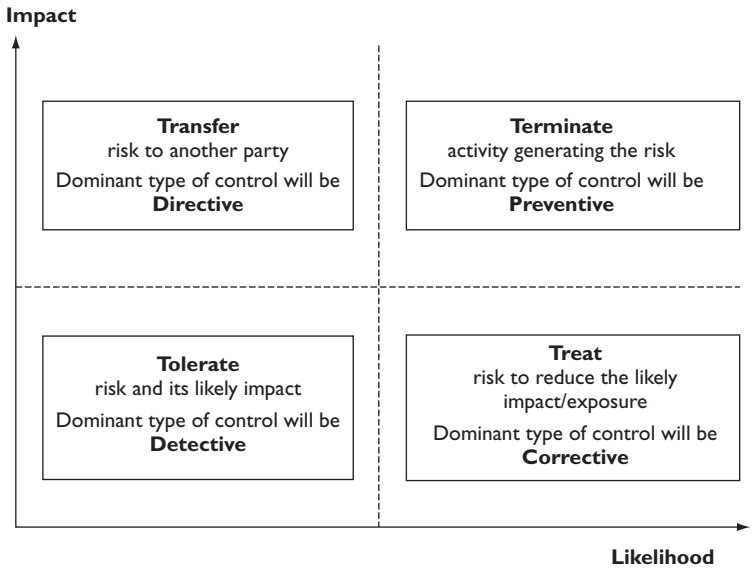


Figure 27.1 Types of controls for hazard risks

In order to give some context to the range of risks that is being considered, Table 27.2 provides examples of the range of potentially significant risks associated with the headings of the FIRM risk scorecard. Assessment of each of the risks will enable the organization to place the risk on a risk matrix. The position of the risk on the risk matrix will then indicate the most unlikely response to that risk. If the risk assessment is undertaken at the current level of risk, the effect of the existing controls will already have been evaluated as part of the risk assessment exercise.

Consider the case of a theatre that needs to respond to the increasing use of agents who require payment at the time of the booking, rather than after the performance. Also, a recent failure of an actor to arrive on the night of the performance caused the theatre considerable financial loss. This has resulted in the theatre reviewing the booking and appearance arrangements for actors and decided that responses are appropriate in relation to all 4Ts.

The theatre might decide that it has to tolerate the new booking fee arrangements. It has also decided that in order to treat/reduce the risk, it will only deal with established agents in future and terminate existing arrangements with an agency that has proved unreliable in the past. The theatre might also investigate the possibility of buying insurance, so that the theatre can transfer the cost of a performance cancelled because the actor fails to arrive on the night.

Table 27.2 Key dependencies and significant risks

FIRM risk scorecard	Example dependencies	Example of a significant risk
Financial	Availability of funds	Insufficient funds available from parent company
	Correct allocation of funds	Inadequate profit because of incorrect capital expenditure decisions
	Internal control	Fraud occurs because of inadequate internal controls
	Liabilities under control	Higher than expected liabilities arise in the pension fund
Infrastructure	People	Failure to achieve/maintain health and safety standards
	Premises/plant and equipment	Damage to key location caused by insurance peril
	IT	IT systems not available because of virus or hacker activity
	Communications and transport	Transport networks closed because of severe weather conditions
Reputational	Brand	Product recall causes damage to product image and brand
	Public opinion	Lost sales or revenue because of change in public tastes
	Regulators	Regulator enforcement action causes loss of public confidence
	CSR	Allegations of unethical product-sourcing causes loss of sales
Marketplace	Regulatory environment	Change in tax regime results in unbudgeted tax demands
	Economic health	Decline in world or national economy reduces consumer spending
	Product development	Changes in technology reduce product appeal and sales
	Competitor behaviour	Competitor substantially reduces prices to win market share

Risk tolerance

Risk tolerance is defined in British Standard BS 31100 as the 'organization's readiness to bear the risk after risk treatments in order to achieve its objectives'. An organization may have to tolerate risks that have a current level beyond its comfort zone and its risk appetite. On occasions, an organization may even have to tolerate risks that are beyond its actual risk capacity. However, this situation would not be sustainable and the organization would be vulnerable during this period.

When the hazard risk is considered to be within the risk appetite of the organization, the organization will tolerate that risk. Risk tolerance is shown as the approach that will be adopted in relation to low-likelihood risks with low impact. However, an organization may decide to tolerate risk levels that are high because they are associated with a potentially profitable activity or relate to a process that is fundamental to the nature of the organization.

It is unusual for a hazard risk to be accepted or tolerated before any risk control measures have been applied. Generally speaking, a risk only becomes tolerable when all cost-effective control measures have been put in place, so that the organization is accepting or tolerating the risk at its current level. Certain control measures may have been applied because the inherent level of the risk may have been unacceptable. Control effort seeks to move the risk to the low-likelihood/low-impact quadrant of the risk matrix, as illustrated in Figure 27.1.

Sometimes risks are only accepted as part of an arrangement whereby one risk is balanced against another. This is a simple description of neutralizing or hedging risks, but on a business level this may represent a fundamentally important strategic decision. For example, an electricity company operating independently in the northern states of the United States may have to accept the impact of variation in temperature on electricity sales.

By merging (or setting up a joint venture) with an electricity company in the southern states, the north/south combined operation will be able to smooth the temperature-related variation in electricity sales. The combined operation will then sell more electricity in the northern states during cold weather, when demand in the southern states is low. Conversely, the combined operation will sell more electricity for air-conditioning units in the southern states in the summer, when demand for electricity in the northern states may be lower.

Risk treatment

When the level of risk exposure (likelihood) associated with a particular hazard is high but the potential loss (impact) associated with it is low, the organization will wish to treat the risk. Risk treatment will often be undertaken with the risk at the inherent and/or current level, so that when the risk has been treated, the new current level or target level may become tolerable.

Actions to improve the standard of risk control will always be under constant review in an organization. On a personal level, wearing a seat belt when driving a car or fitting an intruder alarm in a house are examples of risk reduction actions. Improvements to standards of risk control in relation to physical (insurable) risks are well known. Fitting sprinklers to buildings, providing enhanced building security arrangements and employee security vetting are all examples of risk improvement actions designed to better manage hazard risks.

When identifying suitable risk treatment options, the organization will need to look at the effect of the treatment on the likelihood of the risk materializing as well as looking at the impact of the risk should it materialize. Cost-effective risk treatments will need to be selected and the effect of different control measures can be shown on a risk matrix, as in Figure 27.1.

Risk transfer

When the likelihood of a risk materializing is low but the potential is high, the organization will wish to transfer that risk. Insurance is a well-established mechanism for transferring the financial consequences of losses arising from hazard risks and (to a lesser extent) control risks. The issues associated with the use of insurance as a risk transfer mechanism are considered in more detail in Chapter 30.

In some cases, risk transfer is closely related to the desire to eliminate or terminate the risk. However, many risks cannot be transferred to the insurance market, either because of prohibitively high insurance premiums or because the risks under consideration have (traditionally) not been insurable.

Risk transfer can be achieved by conventional insurance and also by contractual agreement. It may also be possible to find a joint-venture partner, or some other means of sharing the risk. Risk hedging or neutralization may therefore be considered to be a risk transfer option, as well as a risk treatment option.

The cost of risk transfer is a component of risk financing. Once again, there is variation in the definitions used. In relation to risk financing, both BS 31100 and ISO 31000 agree that risk financing involves the cost of contingent arrangements for the provision of funds to meet the financial consequences of a risk materializing. Such arrangements are usually provided by insurance, and insurance is, therefore, finance that is contingent upon certain insured events taking place.

The difference in definition between BS 31100 and ISO 31000 is that ISO 31000 also considers that the cost of risk financing should include the provision of funds to meet the cost of risk treatment. In this text, resourcing of controls is considered to be a separate step in the risk management process. This is another example that illustrates that there is no universally agreed or common language of risk.

Risk termination

When a risk is both of high likelihood and high potential impact, the organization will wish to terminate or eliminate the risk. It may be that the risks of trading in a certain part of the world or the environmental risks associated with continuing to use certain chemicals are unacceptable to the organization and/or its stakeholders. In these circumstances, appropriate responses would be elimination of the risk by stopping the process or activity, substituting an alternative process or outsourcing the activity that is associated with the risk.

An organization may wish to terminate a risk, but it could be the case that the activity that gives rise to it is fundamental to the ongoing operation of the organization. In such circumstances, the organization may not be able to terminate or eliminate the risk entirely and thus will need to implement alternative control measures.

This is a particular issue for public services. There may be certain risks that are high likelihood and high impact, but the organization is unable to terminate the activities giving rise to them. This may be because the activity is a statutory requirement placed on a government agency or public authority. The public service imperative may restrict the ability to cease the activity, so the organization will need to introduce control measures, to the greatest extent that is cost-effective.

It is likely that such control measures will be a combination of risk treatment and risk transfer. As these control measures are applied, the level of risk will move to a level where the organization will be able to tolerate the risk. Because of the variable nature of risks, it may not be possible to get all risks to a level that is within the risk appetite of the organization. The organization may find that it has to tolerate risks beyond its empirical risk appetite in order to continue to undertake a certain activity.

Project and strategic risk response

The overall approach to the management of control and opportunity risks is similar to the approach adopted for the management of hazard risks. However, there are sufficient differences in the range of options available for these to be presented separately.

Figure 27.1 illustrates the 4Ts of hazard risk management and the type of controls that are most likely to be associated with each type of hazard risk response. The types of controls are considered below. This chapter has been concerned almost exclusively with responding to hazard risks. However, there is a similar range of responses available for control risks and for opportunity risks.

Figure 27.2 shows the range of responses that are available when managing uncertainty in projects. The similarities with the 4Ts of hazard risk management are obvious. However, the

emphasis in project risk management is to achieve progress in accordance with a project plan with as little variation from the plan as possible. Project risk management is mainly concerned with the management of uncertainty and is closely aligned to control management.

Chapter 22 considered project risk management in more detail and Figure 27.2 should be viewed in the context of the information set out in that chapter. Low-uncertainty and low-exposure risks in a project will be accepted. For low-uncertainty but high-exposure risks, the project manager will introduce relevant controls and adapt appropriate procedures.

For low-exposure but high-uncertainty risks, the project manager will wish to transfer these risks to a third party. However, the transfer risks embedded in a project will tend to be achieved by contractual arrangements. Also, the project manager will wish to adopt appropriate contingency plans in order to manage the high-risk-exposure but high-uncertainty risks. High-exposure and high-uncertainty risks will be avoided within the project, whenever this is feasible.

Figure 27.3 suggests that there are a range of responses available for the management of opportunity risks. Developing and implementing efficacious strategy will require the evaluation of the level of risk associated with each available strategy and the level of reward that the strategy will deliver.

The 4Es of opportunity management are set out as exist, explore, exploit and exit. There is a close relationship between the 4Es and the status of the organization, as illustrated in Figure 27.3. A start-up operation will face a higher level of risk and low potential rewards.

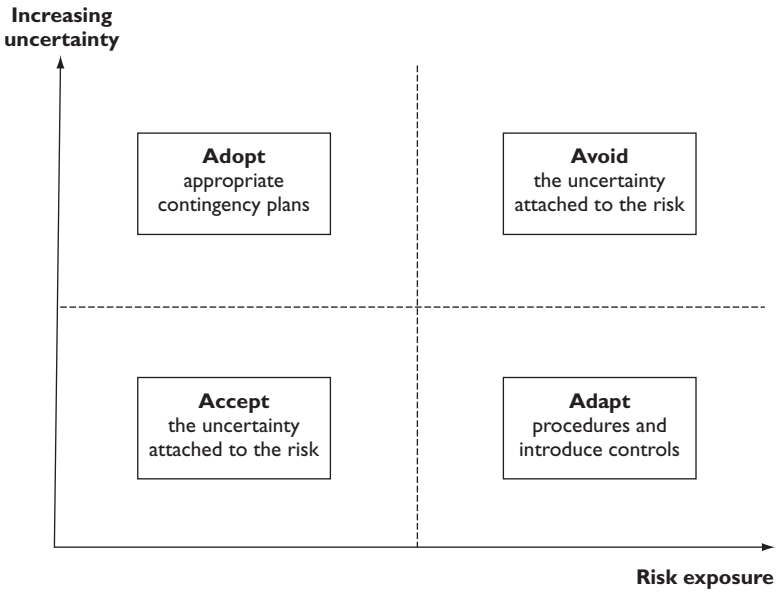


Figure 27.2 Risk versus uncertainty in projects

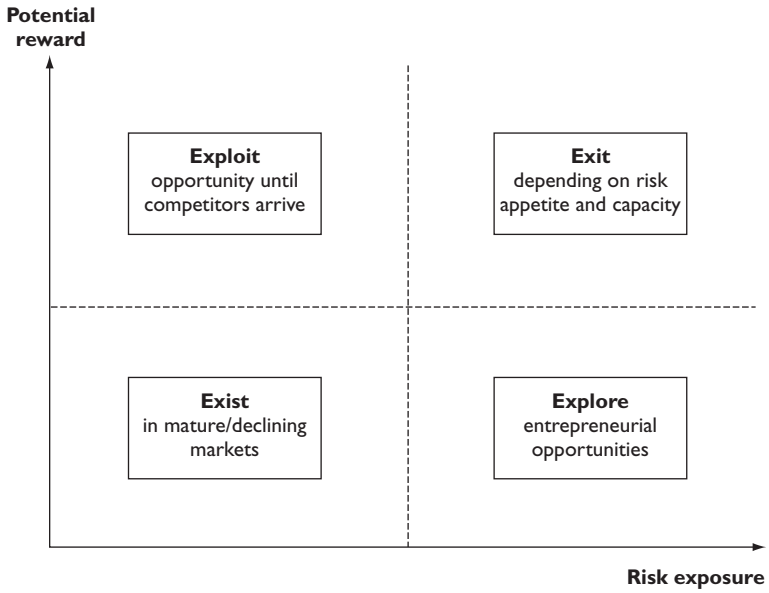


Figure 27.3 Risk versus reward in strategy

Entrepreneurial opportunities will be explored at this time. As the organization grows, potential rewards will increase while the level of risk will remain high. The organization will seek to achieve growth, but may feel that growth is too slow or the level of risk remains too high, and if so it will exit from those operations.

After a period of growth, the organization should be achieving a high reward for a reduced risk. This represents the phase where the organization will exploit opportunities until competitors arrive. This is a mature operation. All mature operations are exposed to the possibility of decline, although many organizations choose to exist in a mature, declining market, where risk exposure is low and so are potential rewards.

28
Risk control techniques

Hazard risk zones

Although the 4Ts of hazard response can be illustrated on a simple risk matrix, such as Figure 27.1 (page 246), the options are not that clear cut. It can be seen that the tolerate and terminate options meet at the centre of the risk matrix. It is not sensible to suggest that a small increase in risk likelihood and potential impact would completely change the approach of the organization to that particular risk.

Figure 28.1 provides a slightly more realistic analysis by providing a diagram that builds on Figure 13.1, the application of risk appetite matrix (page 128), as well as Figure 26.2, which illustrates risk appetite, exposure and capacity (page 237). Figure 28.1 illustrates that there are three zones on the risk matrix. The comfort zone is predominantly for low-likelihood and low-potential-impact events. As can be seen, there is a level of potential impact that will always be within the comfort zone. Likewise, there is a level of risk likelihood that is always considered to be so low that it will not happen.

However, as risk likelihood and potential impact increase, a point is reached, where judgement is required as to whether the risk should be tolerated. Judgement is required within the cautious zone and actions will usually be taken to treat and/or transfer the risks within that zone.

As the risk likelihood and potential impact further increases, a critical line is reached. When the risk gets above the critical line, the organization will be concerned about tolerating those risks and will wish to terminate exposure to them. In certain circumstances, the organization will not be able to terminate these risks, either because they may represent a business imperative, or because they are associated with a high-risk–high-reward strategy that the board has adopted.

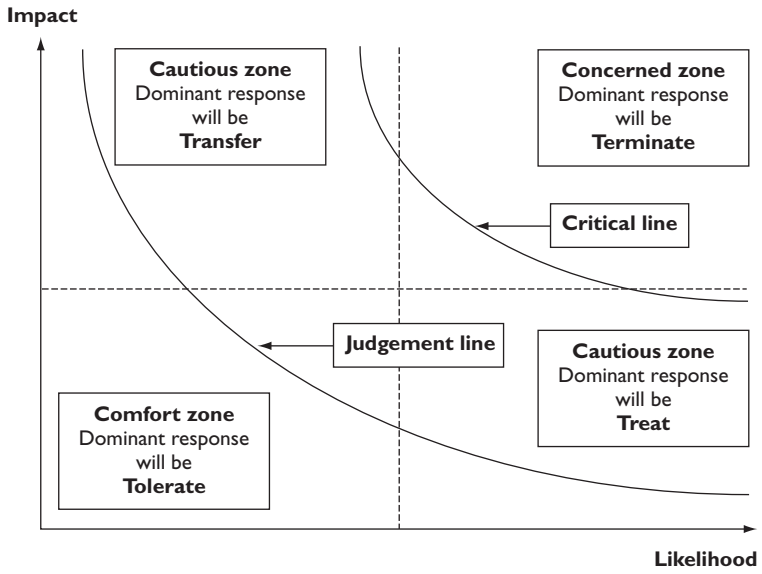


Figure 28.1 Hazard risk zones

Types of controls

There are a range of controls that can be applied to hazard risks. The most convenient classification system is to describe these controls as preventive, corrective, directive and detective. This is the risk classification system suggested in the 'Orange Book'. Table 28.1 provides a more detailed description of each of these four types of hazard controls.

In relation to hazard risks, the control options of preventive, corrective, directive and detective represent a clear hierarchy of controls. The relationship between these four types of controls and the dominant risk of response for different levels of risks is illustrated on the risk map shown in Figure 27.1 (page 246). Table 28.2 gives examples of these four types of controls in relation to health and safety risks.

Preventive controls are designed to limit the possibility of an undesirable hazard event occurring. The majority of controls implemented in organizations in response to hazard risks are preventive controls. For health and safety risks, preventive controls will include substituting a less hazardous material in the process or enclosing the process so that employee exposure to dust or fumes is eliminated. Examples of preventive controls for fraud risks are shown in Table 28.2.

Corrective controls are designed to correct undesirable circumstances and reduce unacceptable risk exposures. Such controls provide a key means whereby the risk is treated so that it becomes less likely to occur and/or the impact is much reduced. In general terms, corrective controls are designed to correct the situation. For example, machinery guards are corrective controls.

Table 28.1 Description of types of hazard controls

1.	**Preventive (terminate)**	These controls are designed to limit the possibility of an undesirable outcome being realized. The more important it is to stop an undesirable outcome, then the more important it is to implement appropriate preventive controls.
2.	**Corrective (treat)**	These controls are designed to limit the scope for loss and reduce any undesirable outcomes that have been realized. They may also provide a route of recourse to achieve some recovery against loss or damage.
3.	**Directive (transfer)**	These controls are designed to ensure that a particular outcome is achieved. They are based on giving directions to people on how to ensure that losses do not occur. They are important, but depend on people following established safe systems of work.
4.	**Detective (tolerate)**	These controls are designed to identify occasions of undesirable outcomes having been realized. Their effect is, by definition, 'after the event' so they are only appropriate when it is possible to accept that the loss or damage has ocurred.

Table 28.2 Examples of the hierarchy of hazard controls

Generic control category	Hierarchy of controls for health and safety risks	Hierarchy of controls for fraud risks
Preventive	• Elimination or removal of the source of the hazard • Substitution of the hazard with something less risky	• Limits of authorization and separation of duties • Pre-employment screening of potential staff
Corrective	• Engineering containment using barriers or guards • Exposure reduction by job rotation or limitation on hours worked	• Passwords or other access controls • Staff rotation and regular change of supervisors
Directive	• Training and supervision to enforce procedures • Personal protective equipment and improved welfare facilities	• Accessible, detailed written systems and procedures • Training to ensure understanding of procedures
Detective	• Health monitoring to enquire about potential symptoms • Health surveillance to seek early symptoms	• Reconciliation, audit and review by internal audit • Whistle-blowing policy to report (alleged) fraud

Directive controls are designed to ensure that a particular outcome is achieved. In health and safety terms, directive controls would include instructions/directions given to employees to use, for example, in the use of personal protective equipment. Training in how to respond to a particular risk event and detailed instructions and procedures are directive controls. Directive controls are also associated with actions that must be taken in the event of a loss to limit the damage and contain the costs.

Detective controls are designed to identify occasions when an undesirable outcome has occurred. The control is intended to detect when these undesirable events have happened, to ensure that the circumstances do not deteriorate further. An example of detective controls in a project is undertaking a post-incident review.

There is a clear hierarchy of effectiveness of controls that is represented by the order preventive, corrective, directive and finally detective. Preventive controls are clearly the most effective, followed by controls that correct adverse circumstances. Providing training and direction to staff is a weaker level of control and detective controls only confirm that an adverse event has occurred.

The importance of disaster recovery planning (DRP) and business continuity planning (BCP) should not be underestimated. DRP and BCP are methods of cost containment designed to ensure minimum disruption after a hazard risk has materialized, so they are aligned with detective controls. However, DRP and BCP do not conveniently fit into the PCDD classification system for controls, because they are post-loss procedures. Some control classification systems include BCP and DRP as a fifth category of control.

The example in the box below illustrates that an organization will use all four types of control in order to build a robust set of risk responses. The road transport company will make use of all four types of controls in order to reduce road traffic accidents.

Application of the 4Ts

Take the example of the road transport company and the desire to reduce the number of road traffic accidents per million miles driven and the options for reducing this number. The company can look at the preventive, corrective, directive and detective control hierarchy and decide the following:

- The scope for introducing preventive controls includes review of vehicle routing and realistic estimates on delivery schedules so that drivers do not need to drive dangerously to arrive on time.
- The types of corrective controls that will be introduced include enhanced maintenance procedures and improved arrangements for drivers to report vehicle defects.

- Enhanced directive controls will be based on defensive driver training and the provision of a vehicle driver handbook with practical advice that is easy to understand and follow.
- Although some detective controls are already in place through the use of tachographs in the vehicles, the company may decide to also introduce a routine review of drivers' licences to check for penalty points.

Other controls that might be evaluated by the transport company include routine inspections of vehicles to discover and report damage, and a review of fuel consumption to identify drivers with an aggressive driving style. The company is then in a position to introduce structured and measurable loss-control programmes to reduce the overall cost of running the fleet of vehicles.

Preventive controls

Table 28.1 provides a brief description of the nature of preventive controls. These are the most important type of risk controls, and all organizations will use preventive controls to treat certain types of risks. Prevention or elimination of all risks is not possible on a cost-effective basis, nor may it be desirable for the future of the organization and the continuation of certain activities.

Examples of preventive controls include the separation of duty, whereby no person has authority to act without the consent of another when paying an invoice. Also, expenditure systems should prevent the same person from ordering goods and then authorizing the payment for those goods. In health and safety terms, preventive controls include the elimination or removal of the hazard and the substitution of the hazard with something less risky. For example, a hazardous chemical used in a cleaning operation may be substituted with a less harmful alternative.

The advantage of preventive controls is that they eliminate the hazard, so that no further consideration of it is required. In reality, this may not be a cost-effective option and may not be possible for operational reasons. The disadvantages of preventive controls are that beneficial activities may be eliminated and either outsourced or replaced with something less effective and efficient.

Health and safety practitioners refer to the elimination of hazardous activities 'so far as is reasonably practicable'. Achieving something so far as is reasonably practicable involves the balance between cost in terms of time, trouble and money against the benefit in terms of the reduction in the level of hazard that is achieved. For example, eliminating the risk of collapse can be achieved in underground mines by the provision of the support beams and props.

However, the extent to which this is reasonably practicable will need to take into account the cost of providing these props against the level of risk reduction that would be achieved in that particular mine.

Corrective controls

Table 28.1 provides a brief description of the nature of corrective controls. Corrective controls are the next option after it has been decided that preventive controls are not technically feasible, operationally desirable or cost-effective. Corrective controls are capable of producing an entirely satisfactory result, whereby the current level of risk is reduced to within the risk appetite of the organization.

Examples of corrective controls can be found in the management of health and safety at work. Engineering containment by way of barriers or guards is a very well-established type of corrective control. In relation to fraud exposures, use of passwords or other access controls can be considered to be corrective controls. Staff rotation and regular change of supervisors also fit into this category of controls.

The advantage of many corrective controls is that they can be simple and cost-effective. Also, they do not require that existing practices and procedures are eliminated or replaced with alternative methods of work. The controls can be implemented within the framework of existing activities. The disadvantage of some corrective controls is that the marginal benefits that are achieved may be difficult to quantify or confirm as cost-effective.

Sometimes, corrective controls are over-engineered and their cost is disproportionate to the benefit that is achieved. It is for risk management practitioners and internal auditors, as well as employees themselves, to identify where expensive and/or ineffective corrective controls have been implemented. Very often, corrective controls are put in place because of regulatory requirements. This may be unsatisfactory from the point of view of the organization and introduce additional costs and/or inefficiency. However, it is for the organization to ensure that the appropriate level of corrective control is achieved in order to comply with the minimum requirements of legislation.

Directive controls

Table 28.1 provides a brief description of the nature of directive controls. Organizations will be familiar with the directive controls, because staff will need to be advised of the correct way of undertaking specific tasks. Where tasks involve a level of risk, documented procedures – together with information, training and instruction – can be seen as directive controls.

An example of directive controls is the requirement to wear personal protective equipment when undertaking potentially dangerous activities. Staff will need to be trained in the correct use of the equipment and a level of supervision will be required in order to ensure that it is used correctly.

The advantage of directive controls is that the risk control requirements can be explained during a normal training and instruction session provided for staff. However, directive controls, especially in relation to health and safety risks, represent a low level of control that may require constant supervision in order to ensure that the correct procedures are being followed.

Although directive controls on their own represent an insecure and unreliable method of risk control, they will always be a component in the overall approach to risk control adopted by any organization. Developing systems, procedures and protocols are important for any organization. However, there is a danger that if the developed procedures are not implemented in practice, the organization will be more exposed to allegations of poor risk control. Developing detailed risk control procedures is an indication by the organization that risks exist and need to be managed. However, failing to implement the identified procedures will leave the organization unable to defend itself by claiming that it was not aware of the risks.

Detective controls

Table 28.1 provides a brief description of the nature of detective controls. As suggested in the title, detective controls are those procedures that identify when the hazard has materialized. Detecting that a hazard has materialized some time after the event is not entirely satisfactory, but can be justified in certain circumstances. Sometimes, other controls may be unable to completely eliminate the chances of a risk materializing.

Examples of detective controls include stock or asset checks to ensure that stock or assets have not been removed without authorization. Bank reconciliation exercises can detect unauthorized transactions. Also, post-implementation reviews can detect the lessons learnt from projects that can be applied in future. Detective controls are closely related to review and monitoring exercises undertaken as part of the risk management process.

The advantage of detective controls is that they are often simple to administer. In any case, they are essential in many circumstances where the organization will require early warning that other risk control measures have broken down. The disadvantage of the detective controls is that the risk will already have materialized before it has been detected. It could be argued, of course, that the fact that detective controls are in place will deter certain individuals from attempting to circumvent other risk controls.

Detection of fraud is often only possible after the fraud has taken place. However, there are considerable advantages in the detection of fraud early, so that the nature and scale of the fraud may be reduced and the scope for future similar fraudulent activities is eliminated. Even in health and safety arrangements, there is scope for the use of detective controls. Certain work processes have hazards associated with them that can lead to permanent and serious health issues. By having detective controls to identify the early symptoms of these occupational ill health conditions, employees will be diagnosed early and further exposure can be eliminated. Examples of these types of controls in health and safety include early detection of lung disease from dust exposure, skin conditions such as dermatitis and finally deafness caused by exposure to occupational noise.

29
Control of selected hazard risks

Risk control

Risk treatment is sometimes referred to as risk control and it includes the selection and implementation of actions to reduce risk likelihood and risk impact. The types of controls described in Chapter 28 should be considered in turn when deciding the nature and extent of risk control activities that should be implemented. When reasonably practicable, it is obvious that preventive controls should be introduced as the first option. If prevention is not possible, then corrective controls should be introduced to minimize the likelihood and impact of an adverse event.

When risks have been prevented and corrected to the greatest extent that is cost-effective, the organization should then consider directive controls that are designed to direct the actions of people involved in the management of that particular risk. Finally, and in addition to the three other types of controls, the implementation of detective controls may be appropriate. Detective controls are used in a wide range of applications, including health and safety.

The examples in the sections below cover the main hazard risks that are likely to be of concern to an organization, as outlined in Table 27.2 (page 247). In each case, the section sets out to describe what can go wrong in relation to the hazard, and the considerations and the issues that need to be evaluated. The control options that are available in relation to that particular risk are considered, followed by consideration of the controls that are necessary and appropriate.

Table 28.2 (page 255) provides examples of the four types of controls described in Chapter 28 as applied to two types of hazard risks. The examples of fraud and health and safety are selected, so that the application of different types of controls to these two hazards can be illustrated. For other hazard risks not listed below, a similar generic approach can be taken and the types of controls that are possible can be listed, using the format of preventive, corrective, directive and detective controls.

When selecting and implementing controls, it is important to ensure that cost-effective controls are selected. Figure 29.1 provides an analysis of the balance between the cost of controls and a reduction in the potential loss that implementing these controls would achieve. This figure illustrates that there is an optimum level of control that represents the lowest total cost as a balance between cost of control and the level of potential losses.

It can be seen in Figure 29.1 that a significant reduction in potential loss is achieved with the introduction of low-cost controls. This section of the diagram is labelled 'Cost-effective controls'. The centre section of the diagram illustrates that spending more on controls achieves a reduction in the net cost of risk up to a certain point. In this segment, judgement is required on whether to spend the additional sum on controls. On the right-hand side of the diagram, spending more on controls achieves only a marginal reduction in potential loss. In this segment, further controls are not cost-effective.

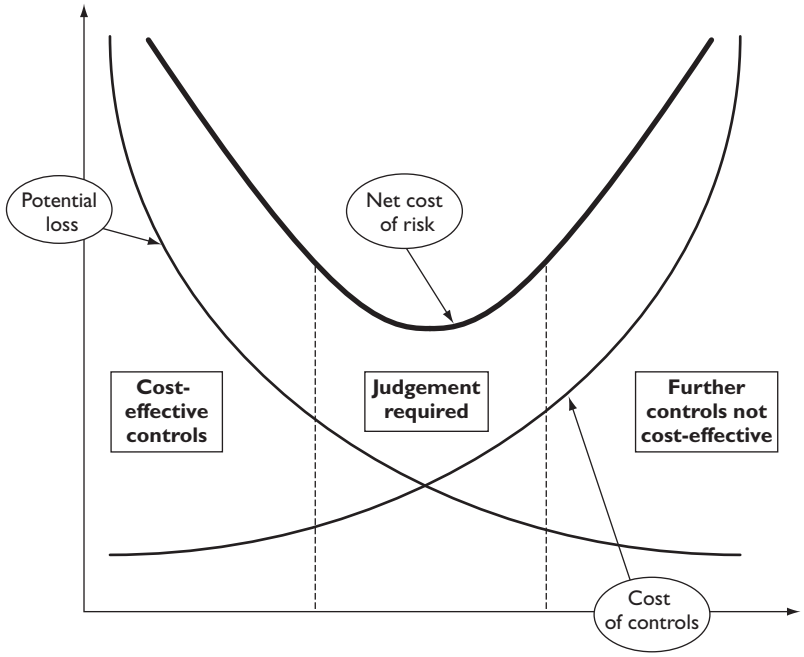


Figure 29.1 Cost-effective controls

Control of financial risks

Fraud

One of the key areas of financial risk faced by all organizations is fraud, which can be committed by employees, customers or suppliers. Also, fraud may be committed by the organization

itself by falsely reporting the results of operations. The Sarbanes–Oxley Act requirements are primarily aimed at the avoidance of fraudulent reporting by organizations.

Fraud occurs when there is the motive for undertaking it, the organization has assets that are worth stealing, there is an opportunity to undertake the theft or fraud and there is a lack of adequate control. Concerns about fraud should also extend to measures that are designed to reduce theft. These will include the provision of security fences and gates, as well as the provision of security guards, improved lighting and secure building access.

Organizations need to undertake an analysis of the effectiveness of their fraud controls. This is an area where internal audit is often involved. This analysis should check for losses in terms of money or goods, as well as evaluating areas where controls are insufficient. The analysis should be a proactive review that should include an analysis of vulnerable assets, who is responsible, how fraud might be undertaken and the effectiveness of the existing controls.

As well as undertaking an analysis of the effectiveness of existing controls, organizations should make an annual review of circumstances where fraud has been detected. These reports should be supplied to the audit committee.

In order to prevent fraud, the organization should introduce a corporate fraud policy that sets out the attitude of the organization towards fraud, the methods for controlling and investigating it, responsibilities for fraud control and details of the resources that are allocated to fraud detection. The arrangements for whistle-blowing and a policy for dealing with persons suspected of committing fraud should also be established.

Risk control actions related to fraud can be divided into the categories listed above as preventive, corrective, directive and detective. The following methods are available to organizations for minimizing fraud:

- improve recruitment processes;
- reduce the motive for fraud;
- reduce the number of assets worth stealing;
- minimize the opportunity to steal;
- increase the level of supervision;
- improve financial controls and management systems;
- improve detection of fraud;
- improve record keeping.

Historical liabilities

One of the most difficult financial risk areas for organizations is related to their exposure to historical liabilities. These liabilities arise from previous activities of an organization, or acquired parts of the organization that were purchased together with their historical liabilities.

An area that is very difficult to quantify for industrial organizations is the previous exposure to agents that may give rise to delayed industrial diseases. The most obvious example is exposure to asbestos and the potential for the development of mesothelioma, a malignant cancer of the pleura or lining of the lungs. For many organizations, claims related to mesothelioma arise 30 or 40 years after the alleged exposure. Exposure will have occurred at a time when insurance arrangements may be difficult to confirm and the evidence of the exact working conditions will no longer be available.

Another area of exposure to historical liabilities relates to pension funds. Previously, many pension funds offered pension arrangements related to the final salary that the employee was earning. These are often referred to as defined benefit pension plans. Risks associated with the value of the pension fund and the level of pension that the available fund will purchase rest entirely with the employer in a defined benefits pension plan.

There has been a strong recent trend towards pension arrangements that build up a sum of money that is available to the employees to purchase a pension at the time of retirement. The member of staff is required to contribute money to his or her pension fund, and this arrangement is usually referred to as defined contribution pension plan. In this arrangement, the risks attached to the value of the fund have been much reduced and the risk associated with the value of pension that the fund will purchase has been transferred to the employee.

The particular risk control issue of concern to employers is related to the defined benefit pension plan and the liability to persons who are no longer employed by the company but have pension entitlements within the defined benefit pension plan. These are often referred to as deferred benefits. The organization will need to look at the risk control options for dealing with these deferred benefits. Options available include encouraging former staff members with deferred benefits to opt out of the scheme by paying them a sum of money, transferring the deferred benefits arrangements to an insurance company on payment of an annuity premium or seeking to transfer the deferred benefits into a captive insurance company.

Historical liabilities of this type are, by definition, more of an issue for organizations that have been in existence for some time. This means that the organization will have a long history and third parties will be able to pursue liabilities that arose some considerable time ago. These historical liabilities may be more severe if the organization has changed in nature over time, especially if it is a much smaller organization than it had been previously. Also, organizations that have undergone a good deal of acquisition and merger activity will be more at risk.

Control of infrastructure risks

Health and safety at work

One of the major areas of concern in relation to infrastructure risks for organizations is health and safety at work. This is a highly regulated topic that should be a priority concern for all organizations. This is a well-established discipline within risk management, although it is often managed as an independent function.

The health and safety risks faced by an organization include prosecution by a regulatory authority, being sued by an injured employee and disruption caused by accidents and dangerous occurrences. Many health and safety tools and techniques are applied in broader risk management activities and there is no doubt that the full co-operation of health and safety specialists is vital to the success of any risk management initiative.

Undertaking risk assessments in relation to health and safety has been established for a long time. These risk assessments can be generic when the risks are relatively low. For high-risk activities, specific written detailed risk assessment will usually be required.

The features of a risk assessment include identification of the hazard, identification of who might be injured by the hazard and analysis of how serious it would be if an injury occurred. Details of the controls and precautions in place, together with the information on further actions that are required should also be included as part of the risk assessment. The only purpose in undertaking a risk assessment is to ensure that controls are adequate and that people are not inappropriately at risk.

There is a hierarchy of controls that is well-established in relation to health and safety risks and this hierarchy is set out in Table 28.2 (page 255). The overall generic control categories of preventive, corrective, directive and detective controls also apply to fraud risks, and Table 28.2 shows the equivalent categories of fraud control in comparison with the well-established terminology for the hierarchy of health and safety at work controls.

Having undertaken a risk assessment of the health and safety risks, organizations need to introduce controls that will include strategies for minimizing the risks (preventive controls), strategies for controlling the hazard (corrective controls), together with strategies for controlling staff and exposure (directive controls). Finally, health and safety controls that are intended to detect the early signs of ill-health may also be required in certain circumstances (detective controls). Management of stress at work is an example where detective controls may be appropriate to identify early warning signs that stress is affecting staff.

The range of workplace hazards that should be considered when undertaking risk assessments will depend on the exact nature of the organization. Detailed guidance is available on the management of specific health and safety risks, including;

- dangerous machinery;

- pressure systems;
- noise and vibration;
- electrical safety;
- hazardous substances;
- lifting and manual handling;
- slips, trips and falls;
- display screen equipment;
- human factors and repetitive strain injury;
- radiation;
- vehicles and driving risks;
- fire safety;
- stress at work.

Property fire protection

One of the most common causes of loss and disruption for manufacturing, warehousing and leisure and retail businesses is fire. More than half the organizations that suffer a major fire fail to fully recover from the event. Fire is a particularly serious event for manufacturing, transport/distribution, retail and especially for residential, hospitality and leisure occupancies. There is also a strong link between the level of building security in place and the prevention of arson attacks.

When designing a fire risk strategy, it is important for the organization to evaluate the fire risks in relation to the common causes of fire at places of work. Most fires at work are caused by one or more of the following:

- electrical hazards;
- hot work;
- machinery;
- smoking materials;
- flammable liquids;
- bad housekeeping;
- arson.

The most important reason for having fire precautions in place is to protect the safety of people who may be affected by the fire. Careful attention should be paid to the adequacy of fire

exits and the provision of emergency evacuation signs. Also, buildings should be of proper construction and fire escape routes should be adequately protected, possibly by the use of sprinklers, if necessary.

Although the safety of people is the most important consideration in relation to fire safety, organizations should also evaluate the potential for serious fire and the disruption that could result. The application of loss-control techniques to fire prevention is very well established. Adequate attention should be paid to loss prevention, damage limitation and cost containment.

Property loss prevention involves the application of preventive controls to the avoidance of a fire. These preventive controls will include maintenance of the electrical installation, the avoidance of sources of ignition and the correct storage of flammable and combustible materials. Corrective controls will include the installation of sprinkler systems and the provision of fire separation arrangements.

The use of directive controls will reduce the impact of a fire and the amount of damage that the fire causes. Directive controls include directions and information for employees on actions to be taken in the event of a fire. These will include early notification to the fire authorities, as well as the use of the portable fire extinguishers by employees if this can be done safely. Finally, detective controls include the provision of fire and heat detectors as well as routine patrols by fire and security officers to detect any fire at an early stage.

IT security

One of the key dependencies for most organizations is the information technology (IT) infrastructure. The failure of a computer system can be a very disruptive event for many organizations. One of the best-established examples of disaster recovery planning (DRP) is in relation to the information technology infrastructure.

Loss of computer data can be very serious for an organization, and it is more likely to be associated with hardware problems than other issues such as software problems, electrical failure or human error. The consequences of IT failure can include:

- loss of business or customers;
- loss of credibility or goodwill;
- cash-flow problems;
- reduced quality of service;
- inability to pay staff;
- backlog of work or loss of production;
- loss of data;
- financial loss;

- loss of customer account information;
- loss of financial controls.

With increasing dependency on computer systems, it is important for organizations to identify the losses that could occur and take actions to manage the associated risks. It is generally considered that the main causes of loss associated with the IT systems are as follows:

- theft of computers and other hardware;
- unauthorized access into IT systems;
- introduction of viruses into the system;
- hardware or software faults and failures;
- user error, including loss or deletion of information;
- IT project failure.

Most organizations will need to set up an IT policy that is designed to ensure correct use of data as well as protecting the IT infrastructure of the organization. The policy should include information on responsibility for IT systems, details of backup procedures, anti-virus and spyware procedures, use of personal data, personal use of the internet and restrictions on personal e-mails.

Most organizations will allow a certain amount of personal use of computer systems by employees. However, this should not be allowed to become excessive and specific restrictions should be placed on internet access to inappropriate websites. Another area of concern to organizations is data protection and the use or disclosure of personal information by the organization. Most countries have extensive legal requirements in place related to the protection of personal data held on computer.

Computer and IT failures will occur from time to time and the organization should ensure adequate backup arrangements, so that only limited data is lost. Organizations with a very high dependency on their IT infrastructure should have detailed DRP in place. In many circumstances, these will extend to arrangements for an emergency duplicate backup computer facility, either available in a mobile trailer driven to the existing office location of the organization or at an alternative location.

The emergency backup facilities can range from a complete duplicate facility with fully up-to-date information (often referred to as a hot start facility) to an alternative computer system that has no data preloaded (referred to as a cold start facility). There are a range of options for backup systems that are a combination of these two approaches, and these are usually referred to as warm start facilities.

HR risks

All organizations require a workforce of employed staff/contractors and/or volunteers. Therefore, there will always be human resources risks attached to the operation of every organization, regardless of its size, nature and the range of activities undertaken by the organization.

There are a number of risk areas associated with the employment of staff and the utilization of the human resource within the organization:

- employee engagement and termination;
- legislative and regulatory compliance;
- recruitment, retention and skills availability;
- pension arrangements;
- performance and absence management;
- health and safety.

Large organizations usually have personnel and/or human resources expertise available in an HR department. There has been a general feeling that large organizations are more exposed to HR risks than smaller ones. This belief has been based on the thought that people know each other better in small organizations and there are fewer individuals involved, so closer working relationships exist across the whole organization. It has been assumed that these closer working relationships mean that the organization is less vulnerable to legal action or other disruption caused by personnel issues.

In recent times, however, it has become obvious that smaller organizations are also exposed to significant HR risks. In response to this realization, most small organizations now produce a staff handbook that sets out the terms and conditions of employment, including arrangements for sickness absence, maternity leave, appraisals and annual leave, behaviour at work and roles and responsibilities.

Organizations need to set down arrangements that will ensure full compliance with the relevant employment legislation, including diversity arrangements to ensure that there is no discrimination on the basis of ethnic origins or physical ability. When building on these basic legal requirements, organizations should look at the opportunities that will arise from having supportive, clear and beneficial recruitment, retention and employment practices.

Control of reputational risks

Brand protection

One of the most valuable assets of any organization is its brand name, and it is important to avoid damage to the organization or any of its brands. Damage to brand can occur for a number of reasons, including:

- changes in government policy;
- changes in the marketplace;
- new entrants into the marketplace;
- price and specification competition;
- counterfeiting and fake goods;
- inappropriate franchisee behaviour;
- failure of sponsor or joint-venture partner.

A trend in recent times has been the use of established brands to sell goods or services that have no obvious link to the brand itself. For example, supermarkets now sell insurance and other financial products, as well as selling petrol from forecourt garages. Extending or stretching the brand in this way represents a huge opportunity for many organizations, but the brand extensions have to be appropriate and credible as well as successful.

Most organizations recognize the value of their brands and have procedures in place to identify opportunities for brand extension. However, ownership of the brand within many large organizations is sometimes not well defined. Successful use of the brand to extend into new product areas and new business sectors should only be undertaken where there is clear responsibility within the organization for managing the brand.

As well as brand extensions, there has been a trend in recent times towards allowing branded concessions to be established within other organizations. It is now commonplace to see high-profile catering brands running the restaurant and cafe facilities in large department stores. This trend has developed at the same time as the increase in high-profile sponsorship deals. For example, many sports clubs have a new stadium that is actually called by the name of their main sponsor.

Many organizations operate on a franchise basis, whereby the brand is franchised to an individual or other business. These developments in branding enable maximum benefit to be gained from a high-profile brand. However, there are significant risks attached to these opportunities, and brand use and extension continues to be an issue that requires careful management.

Successful management of a franchise brand has many challenges. The expectations and requirements of the franchise or brand owner would be set out in a detailed contract in most

cases, although some franchise organizations have been in existence for a long time and the early franchisees may not have the same rigid contact conditions. Most franchise owners provide extensive training for franchisees, including training on the quality of products. A significant issue for many franchise owners is arrangements for procurement of supplies. Often, the franchise owner will prohibit procurement of supplies locally, so that the product delivered by the franchisee is always consistent.

Environment

One of the most rapidly developing concerns in society is global warming and how the activities of individuals and organizations might have an impact. Environmental concerns can range from issues to do with historical land contamination, contamination of water supplies, industrial emissions to atmosphere and the desire of organizations to be seen as green.

Disposal of waste is an issue of concern to all organizations. For organizations producing industrial waste, the legislation is extremely detailed on how the waste must be treated and the arrangements for discarding it. For commercial organizations that do not produce industrial waste or by-products, there are still issues of concern. The disposal of commercial waste can be costly and most countries require or (at least) encourage a large degree of recycling.

The concerns for many organizations therefore relate to minimizing the amount of commercial waste that they produce, as well as adopting other green policies. For many organizations in the public sector, recycling arrangements are detailed and recycling targets are important because of the greater scrutiny of the performance of public bodies.

Arrangements that may be investigated will include the procurement of supplies or raw materials that have less impact on the environment and/or are easier to recycle. Organizations may also wish to introduce a recycling policy and make specific arrangements for the collection of recyclable waste materials. For some organizations, there is also scope to look at travel arrangements and encourage employees to use public transport where this is feasible, as well as reducing the amount of travel that employees undertake.

For industrial operations, there are detailed standards, rules and regulations in place, with the enforcement agencies having considerable powers. As well as paying regard to the legislative requirements, these regulators will also pay regard to broader public opinion and seek to evaluate the following issues:

- What impacts to the environment may occur?
- How harmful are these impacts to the environment?
- How likely is it that these impacts will occur?
- How frequently and where will these impacts occur?

Control of marketplace risks

Technology developments

One of the main challenges facing organizations is keeping up with customer expectations and demands. This challenge is made more difficult by continuing developments in technology. Organizations supplying consumer goods that are technology-based face a continuous challenge, which can be turned into a continuous set of opportunities.

Changes in the technology used to provide home and mobile communications and entertainment have been considerable in recent times. Until relatively recently, home entertainment and mobile entertainment was based on CDs. Organizations operating in this area were confronted with the introduction of MP3 technology and had to make decisions regarding which technology to pursue. The investment required to change technology was considerable and the marketplace risks very significant. For the organizations that correctly identified (and influenced) the developments, the rewards have proved to be enormous. In a rapidly changing marketplace, technology advantages can be significant but the challenge of correctly identifying the most likely successful technology is always present and the investment required is huge.

Consumer decisions regarding new technology are led by convenience, quality, price and fashion. Another factor affecting consumer decisions and the availability of new technology is that significant developments in technology of this type occur on a worldwide basis. Therefore, only a very limited number of organizations have the resources to undertake the research required to develop products based on the new technology. Also, these are the same organizations that design, manufacture and supply goods that utilize the new technology.

In order to take advantage of these new technologies, many organizations have to enter into joint-venture partnerships, share expertise and share the cost of developing the new technologies. Selection of joint-venture partners can be difficult and correct decisions are essential. When developing a new entertainment technology that will be introduced across the world, attempts are sometimes made by competitors to agree the technology that will be adopted. This strategic approach has the advantage that research costs are shared and technology battles are avoided. However, the disadvantage is that the scope for a huge future competitive advantage is reduced.

Regulatory risks

One of the most difficult risk issues for many organizations is the regulatory risk. A key component of the COSO framework is the achievement of compliance by the organization. Compliance may appear to be a relatively straightforward issue, but there are often complexities associated with the potential for changes to regulations, changes in the regulatory environment and different regulatory requirements in different territories.

Different societies have different and changing views of certain commercial sectors. For example, the sex industry has different standards and different regulatory frameworks in different parts of the world. Also, gambling faces different public attitudes, different regulatory frameworks and variable restrictions on activities in different parts of the world. Ensuring regulatory compliance and maintaining good working relationships with regulators can be difficult, especially when public opinion is changing and/or regulatory frameworks are being developed or modified.

There has been a great deal of consideration recently of the difficulties associated with ensuring compliance in the purchase and delivery of multinational or global insurance programmes. Two major issues have received considerable attention. These are the payment of insurance premium tax in different territories and the acceptability of insurance provided in a country by an insurance company that has no presence in that territory. (Insurance written by an insurance company with no presence in a territory is referred to as non-admitted insurance.)

In relation to global insurance policies, the problems arise when a global policy is issued by a large company based in one specific country, but with the insurance coverage applying across all the operations of the organization and in several different countries. Each country will have its regulations regarding the payment of insurance premium tax on that part of the insurance premium that relates to the operations of the organization in that country. Also, many territories in the world do not allow non-admitted insurance policies.

The range of risk control options available to organizations seeking to achieve compliance is, of course, restricted. Compliance is a basic requirement of all business and commercial activities. Ensuring compliance may require co-operation with third parties and detailed advice from specialists with expertise in the discipline in that part of the world. In the example of insurance, it may be necessary for a local insurance company to be involved in the insurance programme in territories where non-admitted insurance is not allowed and this will add cost to the insurance programmes. Also, arrangements for the payment of insurance premium tax may need to be made through third-party fiscal representatives within the territory where the taxes are due.

Learning from controls

The various examples considered in this chapter give an oversight of the wide range of hazard risks that can be faced by an organization. There are many other examples of risks that have been discussed throughout this book. A constant feature of all types of hazard risks is that decisions have to be made on the most appropriate and cost-effective controls that should be introduced.

The analysis that leads to the identification of the most cost-effective level of control is illustrated in Figure 29.1. Figure 29.2 demonstrates the profile of expected losses before and after

a specific control is introduced. Whether the specific control is actually introduced may depend on the judgement of the organization. If it is considered that the risk has a low likelihood of materializing, then the cost of the control may be greater than the anticipated benefit at low likelihood.

This figure also illustrates that the cost of control needs to be taken into account when evaluating the reduced exposure to loss. Another important consideration is that attention should be paid to the need to achieve continuous improvement in the effectiveness and efficiency of the controls that are employed.

Controls should be reviewed on a continuing basis and Figure 29.3 provides a means of undertaking the continuous review that should be part of learning from controls. The phases involved in learning from business activities are often referred to as the 'plan, do, measure and learn' approach. This approach is also used in Appendix B, which considers the overall steps in the successful implementation of an enterprise risk management initiative.

This constant evaluation of controls will result in a number of benefits. It will ensure that the controls are effective in producing the result that is required and controlling the risk to the standard that is set out in the risk management policy. Also, the efficiency of the existing controls can be evaluated, so that it can be decided whether the current level of control is achieved in a cost-effective manner.

Another important advantage of seeking to learn from controls is that unnecessary and inappropriately complex controls will be identified and steps can be taken to remove the control,

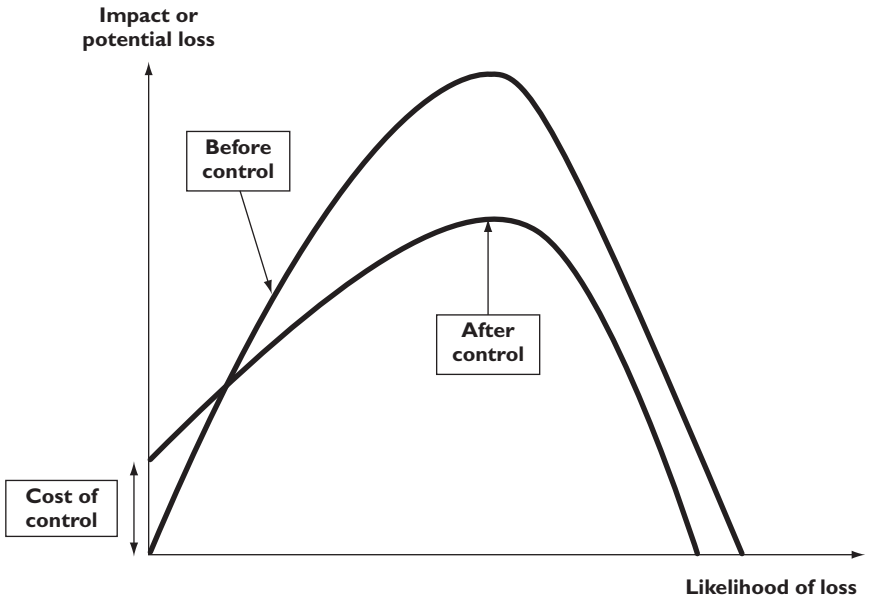


Figure 29.2 Cost–benefit analysis

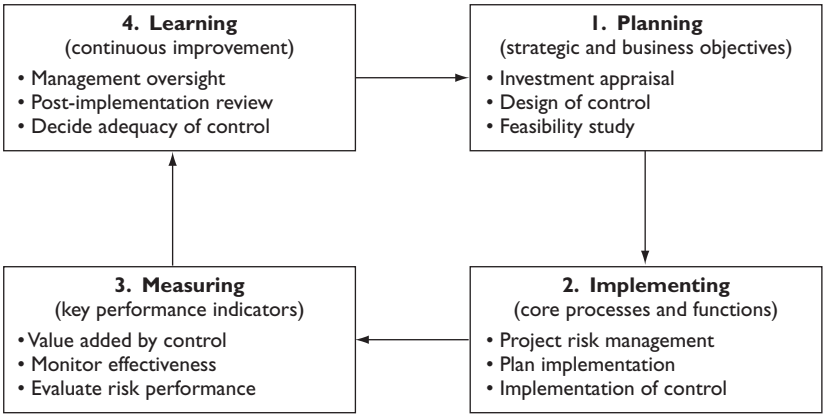


Figure 29.3 Learning from controls

modify it or replace it with a more cost-effective option. Risk assessment activities should take account of the continuing review of controls that is taking place, because the level of risk will be affected by the nature and quality of the controls. The role of monitoring controls is an area of expertise that is well established for internal audit.

Learning from controls may be mainly concerned with increasing their efficiency. However, it is also necessary to ensure that they are effective and they are the correct controls. Internal audit will assist with the evaluation of the effectiveness and efficiency of existing controls and this will assist with the process of learning from controls. The evaluation of controls should also pay regard to the level of reward that is being sought. Therefore, there is a need to evaluate strategy and tactics, as well as evaluating the effectiveness and efficiency of hazard controls.

Throughout this chapter, the emphasis has been on hazard controls, with details presented on some of the more common hazards that will be faced by many organizations. The ideas and principles explained in this chapter are also appropriate to opportunity management, and Figure 29.4 illustrates how the relationship between risk exposure and anticipated reward affects business decisions.

Initially, as risk exposure increases, a higher reward will be expected and the increase in reward is greater than the increase in risk exposure. Ultimately, there will be increasing exposure, but no increase in expected reward, so there is no benefit in taking that extra risk. In between these two situations, increasing risk exposure will produce a marginal increase in anticipated award.

It is in this intermediate area that the judgement of management is required as to whether the increase in risk exposure is within the appetite of the organization. Although it may not seem appropriate to increase risk exposure for a marginal increase in anticipated reward, this may be necessary to satisfy existing customer requirements or to help fulfil a longer-term business objective.

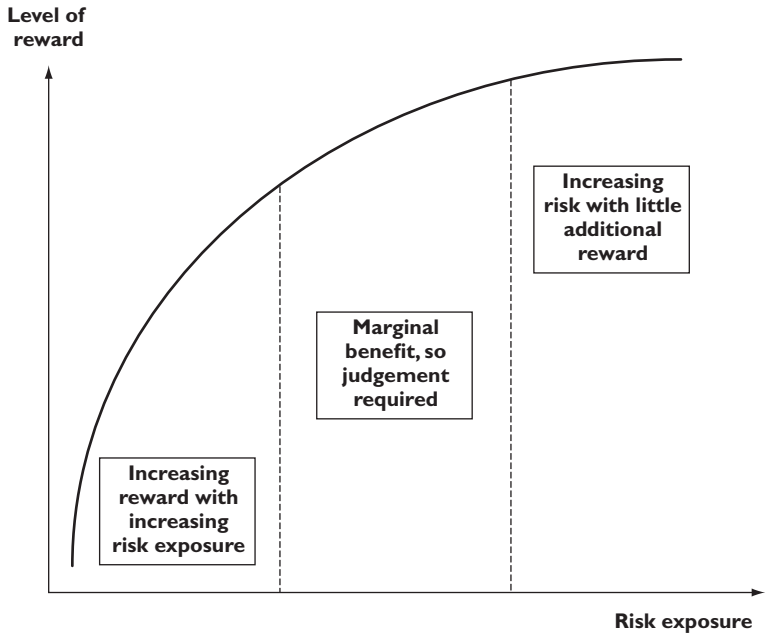


Figure 29.4 Risk and reward decisions

30
Insurance and risk transfer

Importance of insurance

Risk transfer is one of the main risk responses available in relation to hazard risks. This transfer normally takes place by way of insurance and it is often described as risk financing. The fundamental principle of insurance is that the insurance company is contracted to pay a certain sum of money in the event of defined circumstances arising or defined events occurring.

Insurance contracts can require the insurance company to pay for losses suffered directly by the insured. This is first-party insurance and includes property damage insurance. Other types of insurance contract the insurance company to pay compensation to other parties if they have been injured or suffer loss because of the activities of the insured. This is third-party insurance and includes motor third-party and public/general liability.

Insurance contracts are contracts of utmost good faith. This means that the insured party is required to disclose all information relevant to the insurance contract. If this information has not been disclosed, the insurance company or underwriter has the right to refuse to continue to provide insurance cover and may refuse to pay any claims that have arisen.

There are advantages and disadvantages associated with the use of insurance as a risk transfer mechanism. The advantages of insurance are that it provides indemnity against an expected loss. Insurance can reduce uncertainty regarding hazard events that may occur. It can provide economic benefits to the insured, because the loss may be greater than the insurance premium. Finally, insurance can provide access to specialist services as part of the insurance premium. These services may include advice on loss control.

The disadvantages of insurance include the delays often experienced in obtaining settlement of an insurance claim and the difficulties that can arise in quantifying the financial costs associated with the loss. There may be disputes regarding the extent of the cover that has been purchased and the exact terms and conditions of the insurance contract. Finally, the insured may

have difficulty in deciding the limit of indemnity that is appropriate for liability exposures. This may result in under-insurance and the subsequent failure to have claims paid in full.

There are alternatives to insurance when an organization wishes to transfer the financial consequences of a hazard event. Alternatives to insurance are sometimes referred to as alternative risk transfer or alternative risk financing techniques. The risk financing options available to an organization include:

- conventional insurance;
- contractual transfer of risk;
- captive insurance companies;
- pooling of risks in mutual insurance companies;
- derivatives and other financial instruments.

Organizations may decide to retain a certain amount of the financial consequences associated with the losses. Risk retention may be achieved by accepting a large excess or deductible on an insurance policy, deciding not to insure a certain risk exposure (self-insurance) or setting up a captive insurance company. A number of organizations with similar risk exposures may decide to set up a joint captive insurance company. This is often referred to as risk pooling or the establishment of a mutual insurance company.

History of insurance

Insurance has a very long history that can be traced back to Chinese and Babylonian traders. There is evidence that marine insurance had become universal among the maritime nations of Europe by the mid-1300s. In more recent times, the great Fire of London in 1666 gave rise to the modern insurance industry. In the 1680s, a coffee shop (Lloyd's) opened in London, which became the meeting place for parties wishing to insure cargoes and ships and those willing to underwrite such ventures.

Insurance developed rapidly during the 18th and 19th centuries. Prior to the formation of incorporated organizations, insurance policies were signed by individuals whose names and the amount of risk they were prepared to assume were written underneath the insurance proposal. This gave rise to the term 'underwriter'.

Modern insurance companies in the United States developed between the mid-1730s and mid-1750s. The development of insurance was frequently in response to major disasters, typically large fires. There was a significant fire in New York in 1835, and the great Chicago Fire of 1871 illustrated the costly nature of fires in urban areas and the need for insurance. The Chicago Fire of 1871 is considered in more detail in the box below.

Some insurance arrangements were also associated with protection for dependents following the death of the money-earning member of the household. These arrangements became more formalized with the establishment of friendly or benefit societies during the 19th century.

The development of liability insurance has a more recent history, spreading back perhaps only 100 years. Compulsory liability insurance is a requirement in many countries and it has an even more recent history of perhaps only 50 years. Compulsory liability insurance is normally restricted in most countries to employers' liability (or workers' compensation) and motor third party.

Chicago Fire of 1871

At about 9 o'clock on the night of 8 October 1871, a fire started in a cowshed behind a Chicago home. It had been an unusually dry summer and the flames jumped quickly from house to house, then from street to street. The blaze raced along from the southwest to the northeast, enveloping the business district. Then the lumber capital of the world, Chicago was a city built primarily of wood.

Chicago's business district was indeed impressive. With the development of the railroad and the economic boom that followed the American Civil War (1861–65), the city thrived. But the fire raged through four square miles of the metropolis; it demolished factories, stores, railroad depots, hotels, theatres and banks. Flames burned ships in the Chicago River and consumed nearly all the city's publishing and printing. In the end property damage totalled $192 million. Nearly 300 people died in the blaze and 100,000 were made homeless.

The rebuilding of Chicago was a tremendous endeavour. Insurance companies in the United States and Europe rose to the occasion, producing the sums they were obliged to pay for the damages. Cities in the United States and abroad sent $5 million in relief funds and thousands of donated books replenished Chicago's libraries. Before long Chicago began to attract entrepreneurs, businessmen and well-known architects, who found ways to profit from the reconstruction efforts.

Types of insurance cover

The different types of insurance cover that may be required by an organization are set out in Table 30.1. Generally speaking, there are three reasons why an organization will wish to purchase insurance cover. In summary, the reasons for buying insurance are as follows:

- legal and contractual obligations;

- balance sheet/profit and loss protection;
- employee benefit/protection of employee assets.

Table 30.1 provides more information on the different types of insurance that are available and the circumstances in which insurance should be purchased. In most cases, the purchase of insurance is not compulsory. However, most countries require that the purchase of insurance is compulsory in certain circumstances. Typically, these are the liability classes including insurance cover to compensate injured employees and for the parties involved in road accidents.

Table 30.1 Different types of insurance

Legal and Contractual Obligations

- Employers' Liability – compensation to employees injured at work
- Public Liability – compensation to public or customers
- Product Liability – compensation for damage or injury
- Professional Indemnity – compensation to client for negligent advice

Balance Sheet/Profit and Loss Protection

- Business Premises – damage to premises by adverse events
- Business Interruption – loss of profit and increase in cost of working
- Asset Protection – losses, such as:
  - Loss of cash
  - Goods in transit
  - Credit risk
  - Fidelity guarantee (staff dishonesty)
  - Machinery Breakdown (including computers)
- Motor Insurance – compensation following motor accident
- Terrorism – compensation for damage caused by terrorism
- Loss of a Key Person – compensation on loss of key staff member

Employee Benefit/Protection of Employee Assets

- Life and Health – benefits to employees that can include:
  - Life cover
  - Critical Illness cover
  - Income Protection
  - Private Medical costs
  - Permanent Health
  - Personal Accident
  - Travel injury/losses
- Directors' and Officers' Liability – legal and compensation costs

Apart from the compulsory classes, organizations can decide whether to purchase insurance. This decision will be based on the assessment of the risk and whether the nature and level of risk is within the hazard tolerance of the organization. The cost of insurance (premium) and the extent of insurance coverage are also important considerations when deciding whether to buy insurance. Typically, insurance is purchased for low-likelihood, but high-magnitude risks, such as flooding, hurricane damage and major fires.

Consider the example of the insurance needs of a publisher. In relation to legal obligations, the company realizes that it has to buy employers' liability insurance and motor third-party insurance. Also, it is a requirement placed on magazine distributors by the wholesalers that the company purchases libel and slander insurance. In order to protect the balance sheet and profit and loss account, the company needs to purchase property damage and business interruption insurance, together with credit risk insurance and goods in transit insurance.

The publisher may also decide to provide benefits to staff by way of life, critical illness and private medical insurance, as well as personal accident and travel insurance. For the benefit of directors of the company, directors' & officers' liability (D&O) insurance will be purchased. By undertaking this evaluation, in consultation with insurance brokers, the company has ensured that it has put in place an insurance programme that provides cover only where it is necessary, appropriate and cost-effective.

Evaluation of insurance needs

Table 30.2 provides a checklist for organizations to decide which types of insurance are required. There is a wide range of different types of insurance available and the specific activities and features of the organization will assist in deciding the scope of insurance that needs to be purchased. Sometimes, there is a shortage of insurance capacity and although the organization has decided that it wishes to purchase that type of insurance, it may not be available at an affordable cost.

There has been a tendency in recent times for organizations to look at the whole portfolio of risks that it faces. This enterprise risk management approach to risk has resulted in a careful review of how much insurance an organization wishes to purchase. For example, if there are significant risks within a project, but insurance is only available for limited risk exposures, purchase of insurance for only those limited risks may not be appropriate. The enterprise approach to risk management has reduced the use of insurance as a risk control mechanism for some organizations.

One of the features of the insurance market is that the cost of insurance varies significantly during different cycles of the insurance market. The market will cycle between soft market conditions (low premium) and hard market conditions (high premium) over perhaps a 6–10 year period. When the premium rates are high, organizations will tend to buy less insurance

Table 30.2 Identifying the necessary insurance

Feature of the Business Insurance Requirement		
1.	Business has employees	Employers' Liability
2.	Employees travel outside the country	Business Travel
3.	Members of the public could be affected	Public Liability
4.	Business supplies products or components	Product Liability/Recall
5.	Business provides professional advice	Professional Indemnity
6.	Theft or dishonesty by employees could occur	Fidelity Guarantee
7.	Business occupies business premises	Premises Insurance
8.	Premises has machinery or other stock	Contents Cover
9.	Business depends on machinery or computers	Engineering Insurance
10.	Business could be disrupted by fire, flood etc	Business Interruption
11.	Business is involved in transporting goods	Goods in Transit
12.	Business has motor vehicles on public roads	Motor
13.	Business provides life benefits to employees	Life and Health
14.	Certain staff are key to operation of business	Key Person
15.	Business would suffer in event of a bad debt	Trade Credit
16.	Business has directors and/or officers (D&O)	D&O Liability

and make greater use of a captive insurance company – as described below. When premium rates are low, organizations will purchase more insurance because the insurance becomes a more cost-effective control measure.

Purchase of insurance

When looking at the purchase of insurance cover, the organization will need to consider the following six aspects:

- cost;
- coverage;
- capacity;

- capability;
- claims;
- compliance.

The cost of insurance is defined by the insurance premium that is required from the organization. A second component of the cost is the level of self-insurance (including excess or deductible) that is imposed by the policy. This means that if a claim occurs, the organization will have to pay the first part of the claim before receiving any money from the insurance company.

Insurance policies usually have limitations, warranties and exclusions. These will state that claims will be refused in certain circumstances. These coverage issues need to be explored in detail by the organization purchasing the insurance to ensure that adequate coverage is available. The only reason for buying insurance is that claims will be paid when one of the identified events occurs. The history of the particular insurance company in relation to the payment of claims and the reputation of that insurance company will be important factors when deciding which insurance company to appoint.

For very large organizations with considerable assets, one insurance company on its own may not be willing to offer coverage up to the full value of those assets. When buying insurance, the organization will need to think about the capacity that the insurance company is willing to offer in relation to the value of the assets/exposure that need to be insured.

Many insurance companies offer services in addition to insurance. These may include loss control services and assistance with business continuity planning. The capabilities of the insurance company in these areas may be an important part of deciding which insurance company to choose.

An increasingly important issue for buyers of insurance is the financial security, status and capabilities of the insurance company. The nature of the business model operated by insurance companies means that they receive premiums at the beginning of the policy, but do not have to pay claims until some time later. This results in a positive cash-flow position for insurance companies and the associated opportunity to earn investment income.

However, diversification of insurance companies into higher-risk financial activities has resulted in significant losses for some insurance companies and a downgrading of their financial status. Also, low interest rates and poor performance of stock markets has resulted in a reduction in investment income. Accordingly, buyers of insurance need to pay greater attention to the financial status or credit rating awarded to individual insurance companies when making decisions about which company to use.

Reference has already been made to insurance claims and the vital importance of insurance claims in relation to insurance. The only reasons an organization buys insurance are to cover the increased cost of operation, recover the cost of repairing the damage and restoring the business following a loss. In respect of third-party insurance, it is the third-party injured person who will make the insurance claim.

The handling of insurance claims can be a detailed and forensic exercise. Sometimes claims handling involves complex legal processes involving specialist engineers and accountants. Property damage claims may be easier to quantify, but claims associated with the business interruption element of the loss can be very difficult to measure and agree.

If an organization has devised adequate business continuity plans, the disruption to the business and the size of the insurance claim will be much reduced. In risk management terms, depending fully on insurance to make good all losses is not sufficient. Every organization should look to its business continuity plans to ensure that arrangements are in place to guarantee minimum disruption should an adverse event materialize.

There is increasing concern about compliance issues in relation to insurance policies. Most countries have introduced insurance premium taxes and these must be paid on a national basis where an organization has assets in several countries. Sometimes, the requirement to pay taxes may be on a city or regional basis, with the payment going to the local fire brigade. Compliance issues have also extended to the production of the insurance contract before the policy period commences. Timely issuance of insurance policies is often referred to as 'contract certainty'.

There are also compliance concerns related to whether a policy is admitted/approved/accepted within every country where the organization has operations. This can sometimes form a restriction on the operations of captive insurance companies. Certain countries may not accept the validity of an insurance policy written by a non-admitted insurer, including a captive insurance company.

Captive insurance companies

A captive insurance company is an insurance company owned by an organization that is not otherwise involved in insurance. The purpose of a captive insurance company is to provide insurance capacity for the organization by using its internal financial resources to fund certain types of anticipated losses or insurance claims. The organization that owns a captive insurance company is often referred to as the parent of the captive, or simply the parent organization.

In general, captive insurance companies are domiciled in a location that has a favourable regulatory and accounting regime that encourages the establishment of captive insurance companies. Domiciles for captive insurance companies include Guernsey, the Isle of Man, Gibraltar, Malta, Luxembourg, Bermuda and Ireland. The nature of captive insurance companies can vary quite widely. In theory, such a company may write insurance business directly into other countries, although compliance issues surrounding non-admitted policies may need to be carefully considered.

It is more common for a captive insurance company to operate as a re-insurer, providing insurance cover to the main insurance company appointed by the organization. This arrange-

ment provides the insurance company of the organization, often referred to as the fronting insurer, with the means of receiving reimbursement for certain types of claims up to the financial limits or risk retention levels agreed with the captive insurance company.

A typical financial structure for a complex insurance programme is illustrated in Figure 30.1. The organization will accept deductibles or excesses on its different classes of insurance, and these may vary by class of insurance. The captive insurance company then accepts the next level of loss up to an agreed limit for any individual loss and also up to an agreed limit for total or cumulative losses during the policy year.

The primary or fronting insurer will then be responsible for payment of that part of larger losses that exceeds the captive insurance company limit. The fronting insurer will be responsible for payment of all losses once the cumulative totals for the captive have been breached. For statutory classes of insurance, the primary or fronting insurer will be responsible for the payment of the total claim.

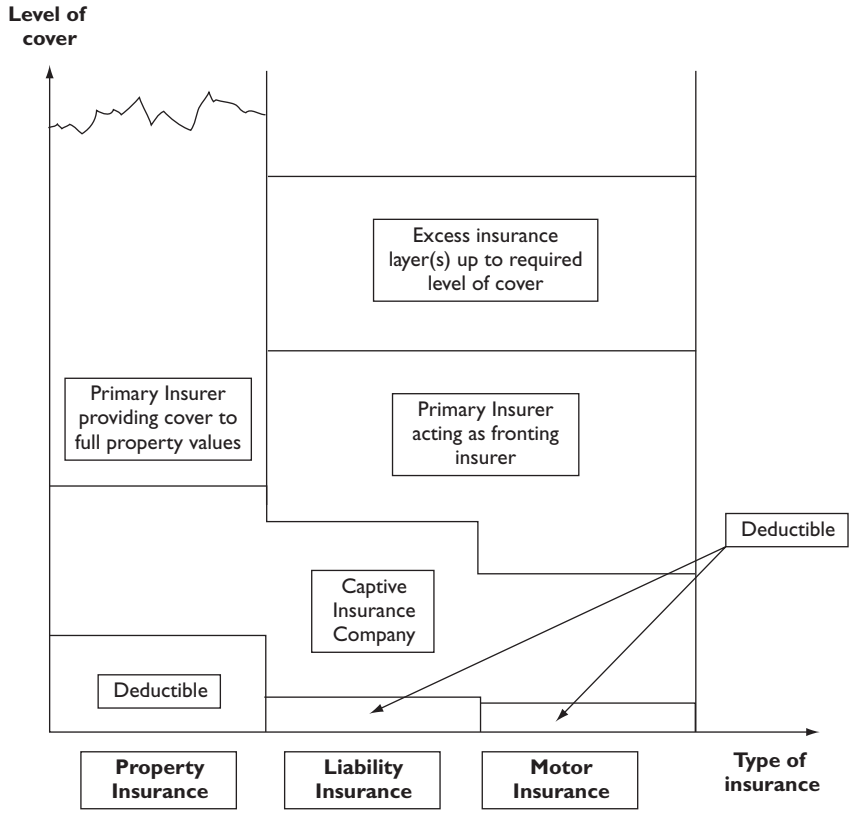


Figure 30.1 Role of captive insurance companies

The fronting insurer will then reclaim the money from the captive insurance company to the extent that the captive insurance company is liable. This can present a credit risk for the fronting insurance company, although this is usually overcome by the fronting insurance company not making any payment until it has received funds from the captive insurance company.

Some captive insurance companies accept business from third parties as well as providing insurance for the parent company. A typical example of a captive insurance company providing third-party insurance is extended warranty insurance policies offered by the retailers of electrical goods. Another example is that travel agents may set up a captive to provide travel cancellation insurance to customers. The customer will purchase a policy issued by a well-known insurance company, but the funding of the insurance will be provided by the captive by way of reinsurance of the fronting insurer. By setting up this arrangement, the travel agent should earn extra income and profit from its customers.

The advantages of captive insurance companies are as follows:

- Savings may be achieved in overall insurance costs because lower premiums are often set by captive insurance companies.
- The captive insurance company can gain access to reinsurance markets, where premium rates and risk capacity can be favourable.
- By being exposed to the cost of insurance claims, a greater risk awareness and greater concern about loss control can be achieved.
- Greater insurance cover can be offered by the captive insurance company than is available in the commercial market.
- Certain tax benefits may be available from having a captive insurance company, although these have reduced in recent times.

The disadvantages of captive insurance companies are as follows:

- The captive will be exposed to insurance claims that would otherwise have been paid by the commercial insurance market.
- The parent organization has to allocate capital to ensure adequate solvency of the captive insurance company.
- When large losses are paid by the captive, these are consolidated to the parent balance sheet and the organization ultimately pays these losses.
- Captives writing business in other territories will probably do so on a non-admitted basis and this may create compliance difficulties.
- Significant administrative cost, time and effort can be involved in the management of the captive by parent head office personnel.

Case study

Intercontinental Hotels Group – loss-control strategy

Process and framework

Intercontinental Hotels Group (IHG) has an established risk management process and framework. Long-term strategic goals are aligned with the IHG core purpose and include these key elements:

- safety and security of guests, employees and other third parties;
- brand strength supported by operational excellence in risk management at all hotels and corporate locations;
- maintenance and promotion of the reputation of the company.

IHG's approach has been to enable and support hotel owners, staff and corporate functions to manage risk effectively. This is accomplished by giving them a systematic approach and framework to follow and by providing them with tools to do the job. The risk management function aims to share specialist knowledge and capability globally.

A strategic framework for hotel safety and security has been designed for owned and managed hotels and shows the identified groups of risks and describes the management activities carried out to mitigate the risks. There are safety and security risk managers around the world who work with IHG general managers and their management teams in order to minimize the risks and keep the hotels safe.

Over the years IHG has developed risk management strategies to assess and treat individual types of risk. This has involved developing policies, standards and guidelines, raising awareness levels, training staff on the controls and systems which have been developed for their use and reviewing and reporting upon progress and continued risks.

Security risks, particularly the threat of terrorism, have increased. In recent years, IHG has developed an increasingly sophisticated response that is intelligence-led and risk-based. The security risk environment is highly dynamic and needs to be managed both centrally and locally in hotels. In common with all risk strategies, there are three elements that must be developed and maintained: physical and technical systems, people capabilities and processes and procedures.

The management activities are being adapted and applied to manage corporate risks. This initiative is led by the Executive Committee, facilitated by the Risk Management function and integrated with quarterly strategic reviews.

Business Review 2008

Part 6

Risk assurance and reporting

Learning outcomes for Part 6

- describe the nature and purpose of internal control and the contribution that internal control makes to risk management;
- outline the importance of the control environment in an organization and provide a structure for evaluating the control environment (CoCo);
- describe the activities of a typical internal audit function and the relationship between internal audit and risk management;
- describe the activities involved in an ERM initiative and how these can be allocated to internal audit, risk management and line management;
- outline the importance of risk assurance and identify the sources of risk assurance that are available to the board/audit committee;
- discuss the importance of risk reporting and the range of risk reporting obligations placed on companies, including Sarbanes–Oxley;
- provide examples of risk reporting approaches adopted by different types of organizations, including companies, charities and government agencies;

- describe the importance of corporate social responsibility as a component of corporate governance and outline the range of topics covered;
- describe the steps involved in the successful implementation of a risk management initiative, together with the barriers and actions.

Part 6 Further reading

Cabinet Office (2009) National Risk Assessment, www.cabinetoffice.gov.uk.

Canadian Institute of Chartered Accountants (1995) Criteria of Control, www.cica.ca.

COSO Internal Control – Integrated Framework (1992) www.coso.org.

Institute of Chartered Accountants in England and Wales (2002) Risk management for SME's, www.icaew.com.

Institute of Internal Auditors (2004) The Role of Internal Auditing in Enterprise-wide Risk Management, www.theiia.org.

Office of Government Commerce (2007) Management of Risk: Guidance for Practitioners, www.tsoshop.co.uk.

31 Evaluation of the control environment

Nature of internal control

The system of internal control within an organization plays an important part in the successful management of its risks. Internal control is concerned with the methods, processes and checks that are in place to ensure that a business or organization meets its objectives. There are alternative definitions of internal control and some of the key definitions are set out in Table 31.1. Internal controls can be considered to be the actions taken by management to plan, organize and direct the performance of sufficient actions to provide reasonable assurance that objectives will be achieved.

Table 31.1 Definitions of internal control

Organization	Definition of internal control
CoCo (Criteria of Control)	Internal control is all the elements of an organization that, taken together, support people in the achievement of the organization's objectives. The elements include resources, systems, processes, culture, structure and tasks.
COSO	A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: • Effectiveness and efficiency of operations • Reliability of financial reporting • Compliance with applicable laws and regulations.
IIA (Institute of Internal Auditors)	A set of processes, functions, activities, sub-systems, and people who are grouped together or consciously segregated to ensure the effective achievement of objective and goals.

British Standard BS 31100 defines a control as a 'measure to modify risk'. It also states that controls include any process, policy, device, practice or other actions designed to modify risk. Internal control incorporates the organizational and hierarchical structure, as well as planning and objective setting. The scope of internal control extends to evaluation of controls designed to support the organization in achieving objectives and executing strategy, but it also applies to the control of actions to ensure that the organization does not miss business opportunities.

When designing effective internal controls, the organization should look at the arrangements in place to achieve the following:

- maintenance of reliable systems;
- timely preparation of reliable information;
- safeguarding of assets;
- optimum use of resources;
- preventing and detecting fraud and error.

Effective financial controls, including maintenance of proper accounting records, are an important and well-established element of internal control. These financial controls help ensure that the company is not unnecessarily exposed to financial risks and that financial information used within the business and for public reporting is reliable.

Purpose of internal control

The primary purpose of internal control activities is to help the organization achieve its objectives. Typically, internal controls have the following purposes:

- safeguard and protect the assets of the organization;
- ensure the keeping of accurate records;
- promote operational effectiveness and efficiency;
- adhere to policies and procedures, including control procedures;
- enhance reliability of internal and external reporting;
- ensure compliance with laws and regulations;
- safeguard the interests of shareholders/stakeholders.

The internal control system includes internal control activities and the structure and responsibilities that relate to internal control activities. The purpose of this internal control system is to enable directors to drive the organization forward with confidence, in both good and bad times. A further purpose of the internal control system and internal control activities is to safeguard resources and ensure the adequacy of records and systems of accountability.

Control environment

The Criteria of Control framework, otherwise known as CoCo, produced by the Canadian Institute of Chartered Accountants (CICA) is a structured means of measuring the quality of the control environment within an organization. The control environment, which the COSO ERM framework labels as the 'internal environment', is a measure of the risk culture within the organization. The view taken by the CoCo framework is that if the control environment is satisfactory, risk management and internal control activities will be successfully and appropriately undertaken.

The structure of the CoCo framework is set out in Figure 31.1. The framework has four components, which are represented as a continuous cycle. The components are based on a sense of direction of the organization, a sense of identity and values, a sense of competence and a sense of evolution.

A number of organizations use the CoCo framework as a means of benchmarking compliance with the internal control component of the COSO ERM framework. This approach will, therefore, be based on a framework that is a combination of CoCo and the remaining seven components of the COSO ERM framework. Table 31.2 gives more information on the specific requirements of each of the four components of the CoCo framework, as set out below:

- purpose;
- commitment;
- capability;
- monitoring and learning.

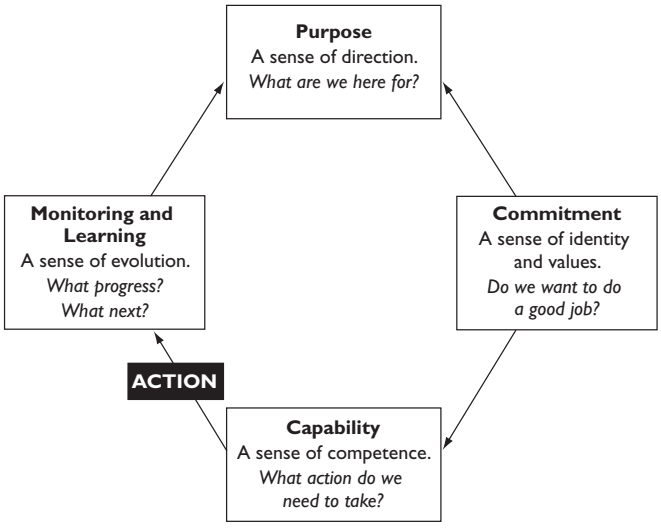


Figure 31.1 Criteria of Control (CoCo) framework

Reproduced with permission from Guidance on Control*, The Canadian Institute of Chartered Accountants (1995, Toronto, Canada).*

Table 31.2 Components of the CoCo framework

Purpose

- Objectives should be established and communicated
- Significant internal and external risks should be identified and assessed
- Policies should be established, communicated and practised
- Plans should be established and communicated
- Plans should include measurable performance targets and indicators

Commitment

- Shared ethical values should be established, communicated and practised
- HR policies should be consistent with ethical values
- Authority, responsibility and accountability should be clearly defined
- Mutual trust should be fostered to support the flow of information

Capability

- People should have the necessary knowledge, skills and tools
- Communication processes should support the values of the organization
- Sufficient and relevant information should be identified and communicated
- Decisions and actions within the organization should be co-ordinated
- Control activities should be designed as an integral part of the organization

Monitoring and Learning

- Environment should be monitored to re-evaluate controls
- Performance should be monitored against the targets
- Assumptions behind objectives should be periodically challenged
- Information needs and related information systems should be reassessed
- Procedures should be established to ensure appropriate actions occur
- Management should periodically assess the effectiveness of control

The rationale behind CoCo is explained in the framework as follows:

> *A person performs a task guided by an understanding of its purpose and supported by capability. The person needs a sense of commitment to perform the task well. The person monitors his or her performance and the external environment to learn how to do the task better and any required changes. In any organization of people, the essence of control is the four components set out above.*

There are similarities between the CoCo approach and the LILAC measure of risk awareness or risk culture that has been mentioned previously. The LILAC approach suggests that risk

management activities will be embedded when the risk culture displays leadership, involvement, learning, accountability and communication. Individual organizations should decide how they wish to measure the control environment/risk-aware culture within the organization. Whatever method is used to measure the risk culture, there is no doubt that it is critical to the successful implementation of risk management.

CoCo is an internal control framework, but it is described in this chapter because it is an established framework. There is a strong interface between risk management activities and internal control and therefore the CoCo framework provides a useful means of evaluating the risk culture of an organization. CoCo defines three major objectives of controls:

- effectiveness and efficiency of operations;
- reliability of internal and external reporting;
- compliance with applicable laws and regulations and internal policies;
- including objectives.

Features of the control environment

There are significant differences between COSO and CoCo, as well as several key similarities. CoCo has a broader approach to the control environment than is set out in COSO. To give two examples of the broader approach in CoCo, it recognizes that controls are required in the setting of objectives, strategic planning and corrective actions; it also recognizes that the control environment of an organization is important when making decisions.

When undertaking an evaluation of the control environment using the structure of CoCo, a company may discover that good scores were obtained for purpose, commitment and capability of the organization. However, the score for the monitoring and learning component may not be good enough. This information will enable the company to identify that it needs to pay more attention to the areas of challenging objectives and the assumptions that lie behind them. Better auditing of controls and a structured senior management review of risk management and internal control activities can then be introduced.

The main differences in approach between COSO and CoCo are that CoCo is more explicit about the following issues:

- identification of need to exploit opportunities;
- mitigation of weaknesses in business resilience;
- the importance of individual trust to the quality of the control environment;
- the need to periodically challenge assumptions.

There are two versions of COSO, and it is the COSO ERM framework (2004) that is considered in detail in this book. The early version of the framework is COSO Internal Control (1992) and the first component of the COSO Internal Control framework is called the control environment. The features of the control environment that are considered to be important by COSO Internal Control are:

- commitment and competence;
- audit committee;
- philosophy and operating style of management;
- organizational structure;
- assignment of responsibility and authority;
- human resources policies and practices.

CoCo framework of internal control

The first component of the CoCo framework is concerned with the establishment and communication of objectives, the significant internal and external risks faced by the organization and the policies designed to support achievement of the organization's objectives. Plans to assist with the achievement of objectives and the inclusion of measurable performance targets and indicators are also important aspects of the purpose component of CoCo.

When establishing and analysing the purpose of the organization, CoCo makes it clear that the risks and opportunities facing the organization should be analysed in detail. The importance of risk assessment and organizational resilience is emphasized, together with the importance of recognizing the sources and origins of risk.

The commitment component of CoCo is concerned with shared ethical values, including integrity. It is also concerned with human resource policies and practices and communication throughout the organization. Authority, responsibility and accountability are also included, together with the requirement to achieve an atmosphere of mutual trust.

The capabilities component of CoCo is concerned with the fact that people should have necessary knowledge and skills to support the organization's objectives, as well as its values. Sufficient relevant information should be identified and communicated, together with decisions and actions of different parts of the organization. Activity should be co-ordinated and designed as an integral part of the organization.

The monitoring and learning component of the CoCo framework is concerned with external and internal environments and the fact that they should be monitored to obtain information. Performance should be monitored against targets and indicators and assumptions behind the objectives of the organization should be periodically challenged.

The information needs and related information systems should be assessed when objectives change, and a procedure should be established and performed to ensure appropriate change actions occur in these circumstances. Finally, management should periodically assess the effectiveness of control in the organization and communicate results to appropriate stakeholders. An example of an organization evaluating its control environment is set out in the box below.

Evaluating the control environment

Many organizations have created their own formulas for educating employees about why controls are important and what adopting such measures means to them. The common element among these organizations is a commitment by senior management that embraces the internal control model.

Canada Post Corporation uses eight major groupings to evaluate the control environment, as follows:

- leadership;
- planning;
- customer focus;
- people focus;
- process management;
- partnership;
- business performance;
- continuous improvement.

During self-assessment workshops, executives receive the final results of all audit work performed throughout the year. The group then discusses business objectives for the coming year and the risks that could interfere with achieving them. The participants rate themselves on a scale of 1 to 10 for each of the criteria. Internal audit then compares the information it received directly from a business process to the information the group acquired about that process during other workshops.

Using the workshop results, internal audit develops an audit opinion on the effectiveness of controls and an audit plan for the coming year. Additionally, internal auditing provides a summary of the results to the board of directors to consider in its strategic planning session. The report includes a commentary on the company's five highest risks and five weakest controls.

Risk-aware culture

Ensuring a risk-aware culture in the organization is vitally important. A risk-aware culture will be achieved when all members of staff and management understand and accept the importance of adequate risk management. In addition, management and staff need to understand the role they will play in the successful management of risks and have a desire to fulfil that role enthusiastically.

There are many ways in which a risk-aware culture can be demonstrated. Clearly, one of the ways of demonstrating such a culture is to achieve high scores in a CoCo analysis. COSO ERM also has an internal environment component, although this is not as comprehensive as the CoCo framework. Nevertheless, evaluation of the internal environment and the level of risk awareness within the organization can be undertaken using the COSO ERM framework.

Many organizations regard the combination of COSO and CoCo as an ideal way of combining the detailed approach within CoCo with the more comprehensive approach of COSO. ISO 31000 refers to the context of risk management. Context has three components in ISO 31000, described as the internal context, the external context and the risk management context. Together, analysis of these three contexts will provide information on the status of the risk-aware culture in the organization.

A subset of a good risk-aware culture is a strong safety culture. Following a major rail crash at Ladbroke Grove near London Paddington railway station in 1999, the Ladbroke Grove Inquiry heard various definitions of the word 'culture'. Counsel to the Inquiry submitted that:

> *A good safety culture is the product of individual and group values, of attitudes and patterns of behaviour that lead to a commitment to an organization's health and safety management. Organizations with a positive safety culture are characterized by communication founded on mutual trust, by shared perception of the importance of safety and by confidence in the efficiency of preventative measures.*

Research by the Health and Safety Executive into the components of a safety culture produced a detailed report and the key components of the safety culture were identified as leadership, involvement, learning, accountability and communication. This gives rise to the acronym LILAC, which is described in more detail in Chapter 11. This represents an alternative approach to the purpose, commitment, capability, monitoring and learning components of the CoCo framework.

32
Activities of the internal audit function

Scope of internal audit

Internal control is concerned with the methods, processes and checks that are in place to ensure that a business organization meets its objectives. Because internal control is concerned with the fulfilment of objectives, there is a clear link with risk management activities. Internal control activities within a large organization are likely to be evaluated by the internal audit department. In some cases, the internal audit function may be outsourced to an external accountancy firm.

Although there is a distinction between the approach and activities of internal audit and of risk management, there are areas of common interest. It is generally accepted that risk management is an executive function that should be undertaken by the executive members of the organization. This leads to the conclusion that the risk management committee should be chaired by an executive board-level director.

Internal audit is primarily concerned with risk assurance, and this will be the concern of the non-executive audit committee in a large organization. Given that internal audit is validating the controls and procedures in place to manage risk, it is inappropriate for internal auditors to fulfil an executive function by assisting management with the identification, design and implementation of those risk control measures.

Financial assertions

A principal role of internal audit in the overall risk management process is ensuring accurate reporting. The scope of reporting can spread from informal reporting on risks and risk events through to formal reporting in the annual report and accounts of the organization. In organizations where the Sarbanes–Oxley requirements apply, internal audit will frequently get

involved in the certification of financial performance, prior to attestation of the results by an external auditor.

Both internal and external auditors use the concept of materiality. Materiality is a measure of the importance of an item of financial data. For example, external auditors will need to decide whether the non-availability of an item of information or the incomplete nature of that information is material to the overall financial performance of the organization.

Materiality is an important concept and may be used as a factor when deciding whether a risk is significant. There will be a relationship between the test of materiality used by auditors and the test used to determine whether a risk is significant. Typically, the materiality test used by external auditors will be about 0.05 per cent of annual turnover. So, for an organization with an annual turnover of £2 billion, the test of materiality is likely to be about £1 million. This figure may be too low to use as the benchmark test for significance of a risk. Typically, the benchmark test would be five times higher, or £5 million.

The presentation of financial data relies on five basic financial statement assertions, which are related to:

- existence of the information;
- completeness of the financial data;
- rights and obligations;
- valuation or allocation;
- presentation and disclosure.

It is important for risk managers to understand the basis of financial reporting and the agenda of the finance director. In order to demonstrate the benefits of risk management, it will be necessary to quantify the benefits and present them in terms that will be understood and accepted by the finance director, as well as external and internal auditors.

Risk management and internal audit

In many large organizations, the working relationship between risk management and internal audit can be difficult. Internal audit will be working to an agenda that concentrates on the effective implementation of efficient controls. In general, the head of internal audit will have a senior reporting line to the most senior non-executive member of the board, perhaps even the chairman.

The risk manager will often have a less senior reporting line, typically to an executive member of the board. This is likely to be the company secretary or finance director. The difference in reporting lines can be a frustration for the risk manager, but the complementary roles of risk

management and internal audit should be seen as an opportunity to ensure more effective implementation of the risk management protocols and procedures.

Both parties should look for areas where they can co-operate without compromising the overall aims of their individual contributions. For example, both risk management and internal audit should attend risk assessment workshops. Risk managers may facilitate the risk assessment workshop, but the responsibility for managing risk will always rest with the manager of each operational department. Also, the presence of an internal auditor at the risk assessment workshop should not be seen as a threat by line management.

Internal audit professionals require that control measures are identified in very precise terms that can be audited. The focus of internal audit activities is on the impact that the control measures actually have in practice. During an audit, internal auditors will request and be provided with information and data. The approach of the internal auditor is to test that information, so that the facts of the situation may be established. In summary, internal auditors take the somewhat challenging view that information plus testing equals facts.

An area where risk management and internal control can work together is in establishing the risk management/internal control priorities for the coming year. When an organization sets up a risk-based audit programme, it will be seeking to ensure that internal audit activities are focused on the priority significant risks facing the organization. The board may well be looking for a joint risk management/internal audit contribution that will achieve better strategic decisions, more successful delivery of projects and more efficient processes.

The introduction of a risk-based audit programme will be facilitated by ensuring that internal audit participate in risk assessment workshops and that risk management and internal audit produce a joint annual programme of work. The overall intention is to ensure that control measures discussed at risk assessment workshops are described in the risk register as fully auditable controls. The overall intention is to ensure that managers have greater awareness of their control responsibilities and fulfil those responsibilities in practice.

There are advantages and disadvantages in having a close working relationship between the risk management and internal audit. In many ways, there is a complementary fit between the two disciplines and there are benefits in having a common focus and co-ordinated planning related to the management of risk. Also, there is an opportunity for sharing best practice regarding risk management tools and techniques.

However, there are also disadvantages in a common approach. It is desirable that line management realize that responsibility for deciding the level of control of a particular risk, the responsibility for implementing enhanced controls and the responsibility for auditing compliance are separate issues. Also, there will often be different reporting relationships in an organization between risk management and internal audit. Finally, internal audit are proud of their independent status and closer involvement in the risk management decision making could compromise that independence.

Risk management outputs

When working together, risk management and internal audit should always concentrate on the outputs from the risk management process and the impact that is sought. The contribution of risk management is to ensure a greater chance of the achievement of the objectives of the organization and this is also a stated intention of internal audit activities.

Overall, risk management/internal audit outputs are intended to achieve enhanced performance of the organization in three important areas:

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

These outputs will be achieved by ensuring minimum disruption to routine operations from hazard risks, together with selection of effective processes that are appropriate for the organization. Selection of effective processes requires informed decision making and the successful implementation of projects. Risk management and internal audit should work together to achieve these outputs.

The most important decisions taken by an organization relate to strategy. Risk management and internal audit both have roles to play in helping the organization reach strategic decisions that result in the development of efficacious strategy. Risk management should ensure that risk assessment workshops address strategic decisions and internal audit should evaluate the quality of the strategic decision-making processes.

The required outputs from risk management/internal audit can be summarized as compliance, assurance, decision making and efficiency/effectiveness/efficacy (CADE3). Risk management and internal audit should work together to achieve these outputs. Due regard should always be paid to the desire of internal audit to remain independent in their activities. The need to retain this independence is another reason why internal audit should not become too closely involved in the executive role and responsibilities related to the management of a risk.

Role of internal audit

Figure 32.1 illustrates the range of activities that need to be undertaken in order to fulfil a successful ERM initiative. The diagram identifies those activities that are core to the work of the internal audit department. These activities include reviewing the management of key risks, evaluating the reporting of those risks and evaluating risk management processes.

The diagram also identifies activities that should not involve internal audit. These activities include setting the risk appetite, imposing risk management processes and taking decisions on

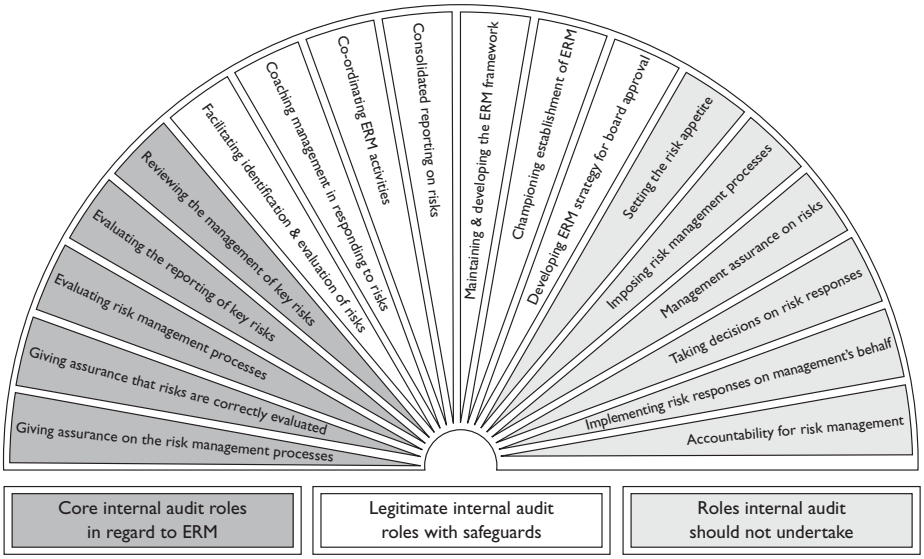


Figure 32.1 Role of internal audit in ERM

This diagram is taken from 'Position Statement: The Role of Internal Audit in Enterprise-wide Risk Management', reproduced with the permission of the Institute of Internal Auditors – UK and Ireland. For the full statement visit www.iia.org.uk.

risk responses. In between these two sets of activities there are activities where it is legitimate for internal audit to become involved, provided that suitable safeguards are in place. These activities include facilitating the identification of risks, co-ordinating ERM activities, developing the ERM framework and championing the establishment of ERM.

Establishing audit priorities is an important function of the audit department. In relation to risk management activities, internal auditors will need to establish their priorities for the testing of controls. There is an important interface between risk management and internal control. Risk management professionals are very good at assessing risks and identifying the appropriate type of control that should be in place. The risk register will often record current controls and make recommendations for the implementation of additional controls.

The core work of the internal auditor starts at this point. Having identified the critically important controls, the auditor will need to check that the controls are implemented in practice and that they are the correct and effective controls. The outcome of testing of controls is to ensure that the intended level of risk is actually achieved in practice. In other words, the control actually moves the level of risk from the inherent level to the intended current level in the way that was planned and often assumed.

If the control is not effective and efficient, it will need to be modified. This is another area where risk management and internal audit share expertise. Although these discussions on controls can be facilitated by risk management and internal audit, the ultimate decisions on

the controls and their anticipated effectiveness have to be made by the members of line management who are responsible for the controls.

Management responsibilities

An alternative way of allocating the responsibilities set out in Figure 32.1 is that internal audit is responsible for the activities that are identified as core internal audit roles. Risk management should facilitate and support the activities in the centre of the fan identified as legitimate roles for internal audit (with safeguards), and line management at the appropriate level should have responsibility for the roles identified as activities that internal audit should not undertake. This alternative means of allocating the responsibilities illustrated in Figure 32.1 is shown in Table 32.1.

Table 32.1 Allocation of responsibilities

Internal audit activities

- giving assurance on risk management processes
- giving assurance that risks are correctly evaluated
- evaluating risk management processes
- evaluating the reporting of key risks
- reviewing the management of key risks

Risk management support

- facilitating identification and evaluation of risks
- coaching management in responding to risks
- co-ordinating ERM activities
- consolidated reporting on risks
- maintaining and developing the ERM framework
- championing establishment of ERM
- developing RM strategy for board approval

Management responsibilities

- setting the risk appetite
- imposing risk management processes
- management assurance on risks
- taking decisions on risk responses
- implementing risk responses on behalf of management
- accountability for risk management

The working relationship between risk management and internal audit will vary between organizations. The roles and responsibilities that are defined will be a reflection of the structure that seems most suitable for an organization. The allocation of roles and responsibilities should take account of the guidance produced by the Institute of Internal Auditors discussed above.

A clear definition of the responsibilities of risk management, internal audit and line management is essential so that ownership of risk becomes clear. In summary, risk management can assist with the risk assessment process and the design of the controls. Internal audit can provide support by auditing the controls to ensure that they are effective and efficient and that they have been fully implemented.

However, the primary responsibility for the management of risk remains with the executive management of the organization. It is important that the activities of risk management and internal audit do not in any way diminish or undermine the ownership of risk by the management of the organization. This approach is also consistent with the statement in most of the risk management standards that risks should not be managed outside the context that give rise to the risk.

33
Risk assurance techniques

Audit committees

The outcomes and impact of risk management activities is often reported to an audit committee in a large organization. Audit committees have a range of responsibilities, including the obligation to obtain adequate risk assurance in the organization. Table 33.1 provides a list of typical responsibilities of the audit committee. Audit committees should be non-executive bodies that do not have executive responsibility for risk management. Similarly, they should not have responsibility for the identification of significant risks or the identification and implementation of critical controls.

The function of the audit committee is to seek risk assurance and check that the process for the identification of significant risks is appropriate. The audit committee should validate that the significant risks have been correctly identified, as well as seeking assurance that critical controls have been correctly implemented.

The audit committee is concerned with internal control in the organization. Internal control is described in the Turnbull Report as the whole system of controls, financial and otherwise, established in order to provide reasonable assurance of effective and efficient internal control and compliance with laws and regulations.

It is worth considering the role of the audit committee in relation to the requirements of the Turnbull Report. The report only applies to companies that are listed on the London Stock Exchange, although the principles set out in the Turnbull Report appear to be gaining wider acceptance and application. One of the requirements of Turnbull is that companies without an internal audit function should review the need for such a department on a routine basis.

Table 33.1 Responsibilities of the audit committee

External audit

- Recommend the appointment and re-appointment of external auditors
- Review the performance and cost-effectiveness of the external auditors
- Review the qualification, expertise and independence of external auditors
- Review and discuss any reports from the external auditors

Internal audit

- Review internal audit and its relationship with external auditors
- Review and assess the annual internal audit plan
- Review promptly all reports from the internal auditors
- Review management response to the findings of the internal auditors
- Review activities, resources and operational effectiveness of internal audit

Financial reporting

- Review the annual, half-year and quarterly financial results, the annual report and Form 20-F and the requirements of the Combined Code
- Review the disclosure made by the chief executive and group finance director during the certification process for the annual report

Regulatory reports

- Review arrangements for producing the audited accounts
- Monitor and review the standards of risk management and internal control
- Consider how the Sarbanes-Oxley processes have operated
- Develop a code of ethics for CEO and other senior management roles
- Annually review the adequacy of the risk management processes
- Receive reports on litigation, financial commitments and other liabilities

Even if the Turnbull requirements do not apply to an organization, it is still appropriate for the audit committee to ensure that it can fully respond to these questions, by ensuring that necessary information is collected. An important component of the Turnbull requirements is the acknowledgement of the limitations on internal control.

Expectations of internal control

A sound system of internal control reduces, but cannot eliminate, the possibility of poor judgement in decision making; human error; control processes being deliberately circumvented by employees and others; management overriding controls; and the occurrence of unforeseeable circumstances.

A sound system of internal control therefore provides reasonable, but not absolute, assurance that a company will not be hindered in achieving its business objectives, or in the orderly and legitimate conduct of its business, by circumstances which may reasonably be foreseen. A system of internal control cannot, however, provide protection with certainty against a company failing to meet its business objectives or all material errors, losses, fraud, or breaches of laws or regulations.

Role of risk management

The risk management policy should set out the roles and responsibilities for risk management and internal control. The purpose of risk management is to achieve compliance, provide assurance, support decision making and help ensure the efficiency/effectiveness/efficacy of operations, projects and strategy (CADE3).

When allocating risk management responsibilities, consideration should be given in respect of each of the significant risks faced by the organization to the separate allocation of responsibilities for:

- determining strategy;
- designing controls;
- auditing compliance.

For example, a head office department may decide on the appropriate level of security for an organization. The design of the appropriate controls may be the responsibility of the production department. This is appropriate because security risk may be an integral part of production that needs to be under the ownership of the production department. In other organizations, it may be appropriate for the security arrangements to be designed by a specialist security adviser or the head of security within the company. Auditing of compliance with the security arrangements is likely to be the responsibility of the internal audit department.

Even in a small organization, it may be important for responsibilities for the management of fraud risk to be separated between different employees or departments. In a small charity, for example, it may be appropriate for a non-executive board member to undertake the internal

control audit and thereby provide an objective view of the efficiency and effectiveness of the internal financial controls in place in the organization.

The role of the risk manager in the allocation of these responsibilities should be a facilitation role. The risk manager may facilitate a workshop designed to identify the fraud risks within the organization and allocate responsibilities for controlling them. However, the risk manager cannot be responsible for implementing controls or auditing compliance. Risk management and internal audit should restrict their roles to the evaluation of the effectiveness of the controls and assist with the identification of whether additional and/or different control measures should be introduced.

Risk assurance

Risk assurance is an important component of the overall risk management process. The audit committee will seek assurance that all of the significant risks are being adequately managed and that all of the critical controls are effective and that they have been efficiently implemented.

There are often discussions at audit committees about 'how seriously a particular department takes risk management and internal control'. The risk manager and the internal auditor will undoubtedly be able to offer an opinion. However, what the audit committee will require is an objective evaluation of the performance of that department. This objective evaluation of the risk culture within the department will form the main basis of assurance for the audit committee. There are other sources of assurance available to the audit committee and these are set out in Table 33.2 Depending on the nature of the organization, the audit committee may depend on some or all of these sources of assurance.

Table 33.2 Sources of risk assurance

- **Culture measurement** – by use of a recognized framework such as CoCo or COSO in order to gain a quantitative evaluation of the control environment
- **Audit reports** – produced by internal audit and external auditors on a range of issues including risk assessment, implementation, compliance and training
- **Unit reports** – produced by the unit itself on such issues as CRSA, response to audit reports and recommendations and reports on incidents that have occurred
- **Performance of the unit** – on risk-related issues, losses, significant weaknesses in control measures and details of any material losses suffered by the unit
- **Unit documentation** – on topics such as the risk management policy, health and safety policy, business continuity plans, disaster recovery plans and other relevant documentation

Assurance will also be required in relation to the risk management activities themselves. The review and monitoring stage of the risk management process is usually represented as an information and experience loop that provides feedback to the beginning of the process. When considering the review and monitoring activities that need to be undertaken, the following stages should be borne in mind:

- review of the process as it operates in the organization;
- review of the standards of risk control in force;
- review of the level of success in reducing risk exposures;
- review of the level of success in achieving business objectives;
- review of why a high-risk strategy, project or operation was successful;
- delivery of risk assurance across this whole range of activities.

When a company plans to borrow more money from the bank, it may be asked to demonstrate how the board obtains assurance that the management of significant risks is satisfactory. The sources of assurance available might include:

- evaluation of the risk culture of the organization;
- quality of audit reports produced by internal audit;
- quality of reports produced by the various departments;
- overall business success of individual departments.

The company may decide that the reports from internal audit and the quality of reports from departments will be the basis of risk assurance. The company can also introduce a control risk self-assessment (CRSA) process that will be based on the components as set out in the appendix to the Turnbull Report. Areas of weakness identified in the CRSA returns will be reported to the executive committee and remedial action will be required. All of these actions will provide the board with greater assurance and place the company in a better position to secure the additional funding from the bank.

Hazard, control and opportunity risks

When considering risk assurance, the organization will need to evaluate different issues, depending on whether the evaluation is related to strategy, projects or operations. Assurance on adequate management of hazard risks can be achieved by evaluation of the hazard risk performance of the department.

Depending on the risk priorities of the organization, the board or audit committee may require annual reports on certain hazard risks. Because of the importance of health and safety at work, boards usually receive annual reports on safety performance. Likewise, the audit committee will

wish to receive an annual report on the incidents of fraud that have been detected within the organization. This will be especially true of organizations that handle large amounts of cash.

Risks that are concerned with uncertainty and, in particular, the successful completion of projects are often the subject of a review by the board or audit committee. Within large organizations, it is typical to have a post-implementation review of a project. For example, if the board of a retail company has authorized the opening of a new store, the audit committee will require a review of the completion of the project for opening the store. This post-implementation review will evaluate whether the project was delivered on time, within budget and to specification. It is also common for the audit committee to require a further post-implementation review of the first 12 months trading of the new store.

Risk assurance related to strategy/opportunities is more difficult and somewhat less well developed. Nevertheless, there are an increasing number of examples of organizations that undertake opportunity evaluations. This has become increasingly common in the professional consultancy firms. When a new business prospect arises, many professional consultancy firms have an opportunity review committee that decides on whether the organization wishes to offer its services to the client prospect. This type of opportunity evaluation may initially be achieved by attaching a risk assessment to a new business proposal.

Control risk self-assessment

As well as undertaking physical audits, internal audit departments will often facilitate a process of self-certification of controls. Self-certification of controls is an arrangement whereby local senior management complete a regular (often annual) return confirming details of the level of risk assurance that has been achieved in the department.

This type of self-certification is generally known as control risk self-assessment (CRSA) and it is frequently undertaken as an electronic return or recorded on the intranet of the organization. The questionnaire for the control risk self-assessment can be based on the criteria set out in COSO or the Turnbull Report.

As well as providing confirmation of adequate levels of internal control and risk assurance, the CRSA return can also provide details of situations where significant weaknesses in controls have been identified. This information will enable the internal auditors to identify areas where additional controls may be required. Also, in addition to identifying significant weaknesses, the CRSA return can require information on any material failures that have occurred.

A benchmark test for identifying a material failure should be supplied and will be much lower than the test for materiality applied by external auditors. For example, an organization that had set a test of materiality at £1 million might require reports on the CRSA return of any failure in controls that resulted in an incident/loss in excess of £100,000 at departmental level.

Approaches to CRSA

The executive has recommended the use of an annual 'control risk self-assessment' (CRSA) exercise, to be conducted by Audit and Risk Assurance, as part of the annual review of Corporate Governance. Each year a sample of the Governance Policies will be chosen by the Governance Panel for inclusion in the CRSA exercise. Policy Custodians will be required to help formulate questionnaires and report back on the feedback received from services to Audit and Risk Assurance.

The findings from the CRSA exercise, together with the assessment of compliance against each of the supporting principles and work carried out by Audit and Risk Assurance in accordance to the annual audit plan will be drawn together into the Annual Governance Statement, for review by the Governance Panel, the Audit and Governance Committee and the Executive.

Benefits of risk assurance

Corporate governance is a major concern for all organizations and their stakeholders. Therefore, risk assurance should not be an administrative or box-ticking exercise. Organizations need to demonstrate that corporate governance is a priority for management. Many organizations recognize the need for openness of risk reporting. This requires effective communication processes to be in place at all times.

Having established good communication processes, the organization needs to ensure that there are positive messages to be communicated to stakeholders. Undertaking risk assurance activities will provide assurance to all stakeholders, including employees, suppliers, customers, government departments, external audit and internal audit.

Obtaining risk assurance is an important part of the corporate governance arrangements for all organizations, as well as being of benefit to the strategic, project and operational processes, activities and decisions of the organization. The benefits of adequate risk assurance are as follows:

- builds confidence with stakeholders;
- provides reassurance to sponsors and financiers;
- demonstrates good practice to regulators;
- prevents financial and other surprises;
- reduces the chances of damage to reputation;
- encourages the risk culture within the organization;
- allows more secure delegation of authority.

34
Reporting on risk management

Risk documentation

There is a wide range of risk management documentation that is relevant to risk management activities. Table 7.5 (page 74) lists the types of risk management documentation that may be required as follows:

- risk management administration;
- risk response and improvement plans;
- event reports and recommendations;
- risk performance and certification reports.

Documentation related to the risk management policy and procedures should describe the control environment or risk culture. Typically, the risk management policy will include a range of information, as set out in Table 7.2 (page 69).

Chapter 7 describes risk management documentation in detail but the subject is mentioned again here because of the importance of risk performance and certification reports. In fact, the importance of these documents has increased considerably in recent times, because of the introduction of the Sarbanes–Oxley Act of 2002.

Risk performance and certification reports include operational management reports as well as more formal declarations and certified reports to stakeholders. In certain cases, certification of the financial results of operations of the organization will be undertaken as a formal attestation by a third party. Typically, this third-party attestation will be undertaken by an external auditor. Such a written attestation will also include an evaluation of the effectiveness of the control activities related to financial reporting.

Sarbanes–Oxley Act of 2002

The Sarbanes–Oxley Act (SOX) was passed in response to a range of corporate scandals in the United States. These scandals involved misrepresentation of the financial status of various organizations, leading to misleading financial statements. The primary purpose of SOX is to ensure that information disclosed by companies listed on the stock exchanges in the United States is accurate.

SOX requires that controls are in place to ensure the accuracy of all information reported by the organization. Section 302 of the SOX requires that all data produced by the organization must be validated. In relation to financial statements, detailed analysis of risks that could result in misrepresentation of the financial results of the organization has to be undertaken. The procedures for compiling financial information and attestation of the financial disclosures by external auditors (as required by section 404) are very detailed and are considered by many to be extremely onerous and costly to undertake.

When complying with section 404 of SOX, the risk assessment is designed to identify weaknesses in the financial reporting structure. This is a very detailed process that requires considerable work by the internal audit department. The financial results of the organization and the evaluation of the financial reporting structure have to be reviewed by external auditors, who have to provide an attestation that they consider the results to be accurate.

SOX requirements state that an approved risk management framework should be used to evaluate risks to accurate financial reporting. The framework recommended for ensuring the accuracy of financial disclosures is the COSO Internal Control framework (1992). Note that the COSO ERM framework (2004) includes all of the requirements of the earlier internal control version of COSO. The SOX requirements apply to subsidiaries of US companies operating in other countries. They will also apply to organizations based in other countries if the company has a listing on a US stock exchange. Therefore, the internal control version of the COSO framework is used by companies in many countries in the world.

In order to comply with the requirements of Sarbanes–Oxley, many organizations have decided to set up a disclosures committee to validate all information disclosed by the organization. Because of the extensive application of SOX, many companies based in countries other than the United States have also been obliged to set up disclosures committees. The risk architecture shown in Figure 7.1 (page 68) for a large corporation includes a disclosures committee.

Compliance with the requirements of the Sarbanes–Oxley Act of 2002 is a costly and time-consuming exercise. Questions have been asked about whether the Act has been effective in improving the accuracy of reports from companies that are listed on US stock exchanges. These criticisms are relevant, given that the SOX requirements relate primarily to accuracy of reporting, rather than the achievement of enhanced risk management standards. A summary of some of the views of the CEOs of some US companies is presented in the box below.

SOX ineffective

Chief executives across the United States view the Sarbanes–Oxley law as reactionary and over-burdensome. Yet they still cite 'improper accounting practices' as the number one ethical issue facing business today. A survey of CEOs on business ethics by Georgia State University polled nearly 300 chief executives at both private and public companies.

Among its findings, most executives agreed that the Sarbanes–Oxley Act strengthened public and investor trust in corporate America, although it had done nothing to improve ethical standards at their businesses. Many agreed that the Act was an over-reaction to the ethical failures of a handful of executives and has proven burdensome and unnecessary.

Risk reports by US companies

Companies that are listed on a US stock exchange are required to make extensive disclosures about risk factors. These risk management reports are intended to be forward looking, rather than a commentary on the risks that have materialized in the past. These reports are contained in the periodic Form 10-K or Form 20-F filings. It is not unusual to find several pages dedicated to risk factors. Typically, this section of the filing will be between 3 and 10 pages long.

Table 34.1 provides a partial list of the industry, economic and environmental risks reported in Form 20-F for the company identified. Extracts from another example of the risk factors that are reported by a US listed company are set out below. It is normal for the list to be introduced by a comment, such as 'important factors that may cause future financial difficulties include, but are not limited to':

- regulatory developments and changes;
- competition in our businesses;
- decisions of competition authorities regarding proposed joint ventures;
- compliance with governmental regulations;
- general economic conditions;
- loss of a strategic customer;
- higher costs of insurance for terrorism, sabotage or hijacking;
- our ability to achieve cost savings;
- fluctuations in fuel costs;

- changes in currency and interest rates;
- disruptions at key sites and facilities;
- incidents resulting from the transport of hazardous materials;
- strikes, work stoppages and work slowdowns;
- disruptions due to employee illness as a result of influenza pandemic;
- market acceptance of our new service and growth initiatives;
- changes in customer demand patterns;
- the impact of technology developments on our operations;
- disruptions to our technology infrastructure;
- adverse weather conditions;
- if our sub-contractors' employees were considered our employees;
- changes in tax laws or their interpretation by authorities;
- higher costs related to implementation of the Sarbanes–Oxley Act;
- changes in environmental laws.

Table 34.1 Risk report in a Form 20-F

In relation to industry, economic and environment risks, the following have been identified for further detailed comment:

- Risk of expiration of patents or marketing exclusivity
- Risk of patent litigation and early loss of patents, marketing exclusivity or trademark
- Risk of expiration or earlier loss of patents covering competing products
- Failure to obtain patent protection
- Impact of fluctuations in exchange rates
- Debt-funding arrangements
- The risks of owning and operating a biologics and vaccines business
- Competition, price controls and price reductions
- Taxation
- Risk of substantial product liability claims
- Performance of new products
- Environmental/occupational health and safety liabilities
- Developing our business in emerging markets
- Product counterfeiting

The above is an example of a list of risk factors, but it does not include all of the items contained in the full list filed as part of Form 20-F. Each of the above risks would usually be described in more detail, by way of a detailed explanation of up to half a page. Additionally, the SEC is considering whether to require more detailed reports on the risk committee reporting structure in companies listed on US stock exchanges. The Securities and Exchange Commission (SEC) is the federal regulator of US stock exchanges and has the mission to protect investors, maintain fair, orderly and efficient markets, and facilitate capital formation.

Charities risk reporting

Risk reporting by charities is compulsory in most countries in the world. In general, there is an expectation that charities should have detailed risk management procedures broadly equivalent to those required of government departments or of companies listed on a stock exchange. A shortened version of the advice on risk reporting set out in the UK Charity Commission guidance is as follows:

> *The form and content of risk reporting should reflect the size and complexity of an individual charity. The Charity Commission is not seeking to standardise risk reporting. A narrative style report that addresses the key aspects will be an acceptable approach to reporting, provided that the report provides:*
>
> - *an acknowledgement of trustees' responsibility;*
> - *an overview of the risk identification process;*
> - *an indication that major risks have been reviewed or assessed;*
> - *confirmation that control systems have been established.*

It is recognized that some charities, particularly larger charities or those with more complex operations, will wish as a matter of best practice to expand on this basic approach in their reporting. Where this more detailed approach to reporting is adopted it will be desirable to address the following broad principles, describing how they have been incorporated into the risk management procedures of the charity:

- linkage between the identification of major risk and the operational and strategic objectives of the charity;
- procedures that extend beyond financial risk to encompass operational, compliance and other categories of identifiable risk;
- linkage of risk assessment and evaluation to the likelihood of its occurrence and impact should the event occur;

- ensuring risk assessment processes and monitoring are ongoing and embedded in management and operational processes;
- trustees review and consideration of the principal results of risk identification, evaluation and monitoring.

Most charities are already likely to consider risk in their day-to-day activities. In fact, it has been reported that many charities now see risk management and other governance requirements as the most significant challenges facing the organization. This appears to imply that charities are becoming more risk averse and spend more effort on compliance issues than on fundraising.

Even where a formal risk management process has not been completed, it will often be possible for aspects of the approach to risk to be drawn out for comment. A typical report on risk management for a small charity may be as follows:

- Risk assessment processes are in place to identify priority significant risks facing the charity.
- Risk management policies, processes and procedures are embedded into routine operations.
- Analysis of strategy is undertaken to identify significant risks that could impact the delivery of the strategy.
- Procedures are in place to ensure legal compliance, including routine reports on legal matters to the board of trustees.
- Trustees receive training on those risk management and corporate governance issues relevant to the charity.
- Trustees receive an annual report of risk management activities and evaluation of the control environment.
- Trustees also receive additional reports about any significant weaknesses in controls and details of any material failures of controls.

Public sector risk reporting

Attention to risk management in government departments and other parts of the public sector is mandatory in most countries. Much of the information on risk management in government bodies is freely available on websites and this information forms very useful reference material. However, because the information is publicly available, there is often no specific mention of the risk reporting to external stakeholders. The government in the UK has produced a set of principles on risk reporting. Table 34.2 sets out those risk reporting principles as openness and transparency, involvement, proportionality, evidence and responsibility.

Table 34.2 Government risk reporting principles

- **Openness and transparency –** Government will be open and transparent about its understanding of the nature of risks to the public and about the process it is following in handling them
- **Involvement –** Government will seek wide involvement of those concerned in the decision process
- **Proportionality –** Government will act proportionately and consistently in dealing with risks to the public
- **Evidence –** Government will seek to base decisions on all relevant evidence
- **Responsibility –** Government will seek to allocate responsibility for managing risks to those best placed to control them

There is usually extensive information on how the risk reporting structure will work within a government body. The information set out below is typical of a report by a UK local government authority:

> *All risks on the Strategic Risk Register are monitored via quarterly clinics. Reports from these clinics are forwarded to the Executive Committee twice per year. The Strategic Risk Register is reported to full Council through its inclusion in the annual strategic plan reporting. Service-specific business risks are included within service group plans and monitored through the directorates' performance management arrangements. This includes reporting, twice per year, to relevant Council Members.*

Annual risk report by a council

The Annual Risk Report provides information based on a full review of the strategic, critical or significant risks identified in the previous Annual Report.

Operational risks have been reviewed and updated as part of the service planning process. The assessments have been made following interviews with Directors and responsible officers and are based on the position as of the end of March.

This report covers the requirements of the annual report, which are detailed in the Council's Risk Management Strategy. Risk management forms an integral part of the Council's corporate governance arrangements.

Government Report on National Security

One of the biggest steps forward in risk communication in recent times has been the willingness of governments to be more open about security threats. For example, the UK government has recently published a document entitled the 'National Security Strategy of the United Kingdom'. This publication gives details of the threats to national security faced by the UK. More recently, the UK Cabinet Office published the National Risk Register.

Within this analysis, there is no mention of the objectives or key dependencies of the UK or the UK government. However, the threat analysis is robust and detailed. The main threat categories identified in the document are as follows:

- terrorism;
- war (including nuclear);
- international organized crime;
- civil emergencies caused by disease or weather.

The document provides detailed analysis of the various threats and the measures that are in place to minimize these threats. The report also discusses the drivers that are changing the risk profile of nations. These drivers include:

- political;
- climate;
- competition for energy;
- poverty/inequality/poor governance;
- globalization – economic, technological and demographic.

This analysis by the UK government is an interesting example of the detailed risk assessment being undertaken at national level. It demonstrates that risk management is now embedded into the heart of national government. The fact that risk management has been embraced by national governments indicates that the importance of risk management is recognized at the highest level.

35
Corporate social responsibility

CSR and corporate governance

Figure 19.1 (page 178) illustrates corporate social responsibility (CSR) as a part of the overall corporate governance requirements of an organization. All types of organizations should be aware that good corporate social responsibility standards can enhance reputation and build stakeholder value. Conversely, incidents, events and losses associated with poor standards of social responsibility can create bad publicity and destroy stakeholder value.

The importance of good standards of corporate social responsibility is widely recognized and achieving good standards can enhance the organization by:

- protecting and enhancing reputation, brand and trust;
- attracting, motivating and retaining talent;
- managing and mitigating risk;
- improving operational and cost efficiency;
- giving the business a licence to operate;
- developing new business opportunities;
- creating a more secure and prosperous operating environment.

There are a variety of definitions available for corporate social responsibility. It is generally accepted that CSR is a wide-ranging agenda that involves organizations looking at how to improve their social, environmental and local economic impact and their influence on society and human rights. The CSR agenda also extends to consideration of fair trade issues and the elimination of corruption. Before corporate social responsibility became a widely used term, several organizations used to refer to social, ethical and environmental (SEE) concerns. The CSR agenda includes all of the issues previously included in the SEE agenda.

There is no doubt that CSR is an issue for large multinational companies as well as for small, locally based businesses and the public sector. Indeed, it is relevant to all types of organizations, including charities. The European Commission definition of corporate social responsibility is as follows:

> *Corporate Social Responsibility is the concept that an enterprise is accountable for its impact on all relevant stakeholders. It is the continuing commitment by business to behave fairly and responsibly and contribute to economic development, while improving the quality of life of the workforce and their families, as well as of the local community and society at large.*

CSR and risk management

The scope of issues covered by CSR is set out in Table 35.1. The range of topics extends from health and safety concerns to broader considerations related to employees, customers, suppliers, the community, the environment and products/services provided by the organization. Both the CSR and risk management agendas are very broad and they have a significant overlap.

Table 35.1 Scope of issues covered by CSR

Health and Safety

- Commitment to a programme of activities to achieve continuous improvement in health and safety performance

Employees

- Aim to deliver a competitive and fair employment environment and the opportunity to develop and advance – subject to personal performance

Customers

- Strive to provide high-quality service and products and good value for money in all dealings with customers

Environment

- Reduce impact on the environment, including factors contributing to climate change, through a commitment to continual improvement

Suppliers

- Working with suppliers to ensure that worker welfare/labour conditions and environmental practices meet recognized standards

Community

- Aim to be a responsible corporate citizen through support for appropriate non-political and non-sectarian projects, organizations and charities

Products/Services

- Designed not to unintentionally or by design cause death, injury, ill-health or social disruption, hardship or detriment

Many of the issues listed in the table are risk-based subjects, including health and safety at work and environmental impact. However, management of these issues simply as risks will fail to fully address the CSR agenda. Nevertheless, this is a good starting point. Many risk assessment workshops consider corporate social responsibility and social, ethical and environmental considerations within the topics that are evaluated.

When assessing the CSR agenda, risk managers should take the opportunity to bring risk management tools and techniques to a broader agenda. The risk management approach of risk assessment, identification of control measures and auditing of compliance is an approach that can be transferred to corporate social responsibility and, indeed, to the broader corporate governance agenda.

CSR and reputational risk

Most organizations consider CSR to be a reputational issue and see the component parts of CSR as hazard risks. Such organizations will consider that they need to reform their processes and procedures in order to comply with these requirements. This may well be an accurate starting point for many organizations. However, as Figure 4.2 (page 44) illustrates, what starts off as a hazard risk can develop into a control risk and eventually into an opportunity.

As with other areas of risk management, organizations should seek to develop their level of sophistication in relation to CSR. Having got to the stage of complying with the CSR obligations, organizations should then look at the opportunities that are available. For example, it is now commonplace for supermarkets to offer goods that have been procured on a 'Fair Trade' basis and gain additional sales from offering this range of products.

Corporate social responsibility is an area of concern where it is likely that public opinion will be ahead of the thinking within many organizations. CSR issues therefore represent a great opportunity for an organization to develop corporate social responsibility plans and actions that respond to public opinion. Treating the CSR agenda as a dynamic, proactive set of issues will enable the organization to gain reputational advantage.

CSR and stakeholder expectations

Many organizations have stakeholders that they do not necessarily want. This is certainly the case for several energy companies. Exploration for oil, coal and minerals is carefully scrutinized by environmental pressure groups. Even if they are 'unwanted stakeholders', environmental pressure groups are valid stakeholders in these organizations and can bring a considerable influence to bear on the activities of the organization. Environmental pressure groups have demands that are firmly within the CSR agenda.

The list of issues in Table 35.1 provides an indication of the stakeholders who are likely to have an interest in the CSR agenda. Employees, customers, suppliers and the general community are the key groups that are stakeholders in the CSR agenda of an organization. For CSR issues associated with the environment, it is fair to say that everybody is a stakeholder in the behaviour of organizations, when that behaviour impacts the environment.

An example of the impact that a pressure group can exert is demonstrated by the following report on the website of the environment action group Greenpeace. This report relates to the proposed disposal by Shell of the Brent Spar oil storage facility in the mid-1990s.

Shell Brent Spar

In 1995, Greenpeace activists occupied the Brent Spar oil storage facility in the North Sea. Their purpose was to stop plans to scuttle the 14,500 tonne installation. The action was a part of an ongoing campaign to stop ocean dumping and pitted Greenpeace against the combined forces of the UK government and the world's then-largest oil company.

Spontaneous protests in support of Greenpeace and against Shell broke out across Europe. Some Shell stations in Germany reported a 50 per cent loss of sales. Chancellor Kohl raised the issue with the UK government at a G7 meeting. But despite the UK government's refusal to back down on plans to allow the Spar to simply be dumped into the ocean, public pressure proved too much to bear for Shell and in a dramatic win for Greenpeace and the ocean environment, the company reversed its decision and agreed to dismantle and recycle the Spar on land.

The decision led to a ban on the ocean disposal of such rigs by the international body which regulates ocean dumping. Before the Brent Spar campaign, a number of oil companies had been planning sea-dumping of obsolete installations, such as oil storage buoys (like Shell's Brent Spar) and oil rigs. Greenpeace's action and the support of people throughout Europe ensured that no such structures have been dumped to this day.

Supply chain and ethical trading

Failure to ensure appropriate ethical behaviour is increasingly recognized as a major business risk. Newspaper reports describing bribery and other forms of dishonesty have serious consequences for corporate reputation and future profits. Easy access to information on the internet can result in organizations being investigated and exposed for unethical trading and/or unfair treatment of suppliers.

If the unethical behaviour extends into illegal activity, this can undermine the organization itself. Illegal behaviour and condoning actions that are outside the governance rules of the organization can have serious consequences. The perceived need to bribe officials in certain territories is both unethical and illegal.

There are several areas where unethical trading can result in damage to reputation, the loss of future profitability and a refusal on the part of the customers and suppliers to deal with the organization. These issues include:

- failure to comply with rules and regulations;
- trading with undesirable overseas governments;
- excessive payments to political parties;
- tax evasion or dubious tax arrangements;
- inappropriate criticism of competitors;
- false allegations against competitors;
- unethical alliances with competitors.

Another feature of the supply chain that may result in allegations of unethical trading relates to the sourcing of products produced in socially unacceptable working conditions. Also, the quality of products and failure to provide value for money can result in damage to reputation and may be associated with unethical trading. The report below shows how goods that fall short of current safety standards can result in serious adverse publicity and damage to reputation.

Mattel recalls toys

US toymaker Mattel has recalled more than 18 million toys worldwide, the second such recall in two weeks. Chinese-made die-cast toys have been recalled because their paint contains lead. It has also recalled toys containing small magnets that can come loose.

The company blamed the amount of lead in the paint on a sub-contracted Chinese company using paint from unauthorized suppliers. The recall is the latest in a series of alerts about Chinese products in the United States, raising fears in Beijing that the 'Made in China' label is being seriously damaged. Chinese officials have announced a series of measures to tackle the problems.

The other toys recalled contain small, powerful magnets. There had been 400 reports of magnets coming loose since Mattel recalled 2.4 million magnetic play sets in November 2006. It is concerned that 'if more than one magnet is swallowed, the magnets can attract each other and cause intestinal perforation or blockage, which can be fatal.'

When a sports club decides that it wants all merchandise for sale to fans to be ethically sourced, it needs to look at the controls that can be placed on the importer to ensure that it only obtains merchandise from ethically produced sources. The club could require the importer to produce a routine CSR report as part of the contract terms and conditions. This report will include the following information:

- details of the policy that the importer has on ethical behaviour of suppliers;
- confirmation of the contractual terms and conditions of manufacture;
- statement that manufacturers do not sub-contract work, unless authorized;
- details of staff training, accident/absence rates and pay/conditions;
- results of audits/physical inspection of manufacturing premises.

The club can then advertise to fans that all goods are ethically sourced and encourage other teams in the league to do the same. This will gain good publicity and promote the club as having high corporate social responsibility awareness.

CSR reporting

Positive reporting on corporate social responsibility issues can be a significant benefit for an organization. This will be especially true when the organization operates in an area where the public is suspicious. The public may not be sympathetic towards a number of organizations, because of public perception of the business sector and/or the organization itself. When an organization operates in a sector that does not have universal public support, there may be benefit in producing an ethics policy for the organization. The importance of the ethics policy will be reinforced if the organization also undertakes an ethics audit.

For example, a sector that does not have full public support is gaming and gambling. Therefore, organizations operating in this area should seek to enhance the reputation of the sector by working with competitors on social responsibility standards for problem gambling. An individual organization can then gain further benefit by being able to demonstrate that it exceeds the minimum standards established for the sector.

Many organizations now include comment on corporate social responsibility in their annual report and accounts, and some produce a separate CSR supplement. The production of a report on corporate social responsibility activities enables the organization to gain advantage from the CSR agenda.

Where an organization has a positive story to tell about CSR achievement, it will have taken a CSR agenda from the need to reform to the position where the organization can demonstrate that it does conform. The next stage in this developing sophistication is for the organization to demonstrate that adherence to a CSR agenda enables it to better perform and more successfully fulfil stakeholder expectations.

36
Future of risk management

Review of benefits of risk management

Much of this book is concerned with risk management input into operations. It is likely that operations will be impacted by hazard risks and so the focus of risk management in relation to operations is on hazard management. In order to achieve the maximum benefit from risk management input into operations, organizations need instead, however, to focus on loss control. Loss control is a combination of loss prevention, damage limitation and cost containment. In Figure 26.5 (page 241), the contribution of risk control and loss management is demonstrated, together with the contribution that insurance can make as one of the well-established control measures employed as part of hazard management.

Projects should be completed on time, to budget and to specification/performance. Inevitably, there will be a considerable amount of uncertainty associated with all projects. The contribution of risk management is to minimize these uncertainties. Management of the risks within projects is a style of control management. The application of control management is illustrated in Figure 27.2 (page 251), in which risk exposure is mapped against increasing uncertainty. The figure illustrates the 4As of control management.

Risk management input into strategy focuses on the risk assessment of the various strategic options available to an organization. The contribution of risk management to successful strategy is, therefore, focused on the decision-making process. Figure 27.3 (page 252) illustrates the 4Es of opportunity management and plots risk exposure against potential reward. Organizations undertaking strategic risk management will complete a careful review of viable new business prospects and undertake detailed risk assessment before making strategic decisions.

The overall benefits of risk management can be summarized in a number of ways. By undertaking a risk management initiative, less disruption to operations, successful delivery of projects and better strategic decisions are the expectations. Also underpinning risk management initiatives will be the desire for adequate risk assurance. These components

– the compliance, assurance, decision-making and efficiency/effectiveness/efficacy – provide the acronym CADE3.

Using the structure of the FIRM risk scorecard, an organization will be able to demonstrate the benefits that it has obtained from a risk management initiative. It is likely that the following benefits will have been delivered to a theatre that has been pursuing a structured proactive risk management approach for about three years:

- financial benefits arising from better allocation of funds, monitoring of expenditure and reduced exposure to fraud;
- infrastructure benefits that have included fewer failures of the IT systems and reduced staff absence rates;
- reputational benefits from ethical sourcing policies and use of organic food in the restaurant, as well as successful niche productions in the theatre;
- marketplace benefits resulting in 89 per cent occupancy rates, up from 83 per cent three years ago, as well as increased spend in the theatre by patrons.

The theatre will continue to develop the risk management initiative and continue to obtain benefits. Risk management activities are now embedded within the management culture of the organization.

Steps to successful risk management

In order to improve the risk management performance of an organization, a risk management initiative will be required. The nature of this initiative will depend on the size, complexity and nature of the organization. There is no single correct approach to implementing risk management in an organization. The drivers for undertaking risk management and the expected outputs and impacts will vary between organizations.

Although there is no single correct approach, Table 36.1 sets out some of the key steps in achieving successful risk management. Appendix B provides an extended description of the issues mentioned in Table 36.1. The appendix also draws together the acronyms used throughout this book and lists the various risk management tools and techniques associated with each stage in the implementation of a successful enterprise risk management initiative.

The initial, and perhaps most important, step is ensuring that the risk management initiative is sponsored by a member of the board or a senior member of the executive committee of the organization. Information on the successful introduction of a risk management initiative is also available in the various risk management standards and frameworks discussed throughout this book.

Table 36.1 Achieving successful risk management

- Sponsorship of the project by a board or executive committee member
- Develop a shared perception of risk within the organization
- Identify the risks within an agreed classification system
- Define the role of the risk manager as facilitator
- Develop the role of the risk management committee
- Produce the profile of risks using an agreed risk recognition technique
- Develop a risk management culture within the organization
- Ensure that risk management is aligned with the business process
- Determine the risk appetite of the organization
- Quantify the cost of risk controls
- Demonstrate that risk management is making a contribution
- Describe the contribution to objectives and corporate governance
- Undertake a management review of all risk management activities
- Ensure that maximum benefits continue to be delivered

Although it is important to have an overall plan relating to the implementation of the risk management initiative, it is also vital that the risk manager identifies barriers to the implementation of the initiative in some detail. The potential barriers and enablers to the successful implementation of a risk management initiative are set out in Table 36.2. There are many factors that will influence the effectiveness of the approach, including:

- senior management influence within departments;
- external influences, including corporate governance;
- nature of the business, its products and culture;
- corporate attitudes, including previous RM experiences;
- origins of the risk management department.

Identification of barriers, as set out in Table 36.2, leads to the ability to put in place actions to overcome them. These include the fact that successful risk management requires the commitment of all parties and that implementation will only be as good as the least committed member of a department. Analysis of these barriers within the context of the specific organization will lead to the identification of the best options to ensure that risk management delivers the optimum benefits.

There is no single action that will ensure adequate implementation and no single time frame by which implementation will be fully achieved. It is the experience of many organizations that full implementation of all stages of the approach may take between two and five years.

Table 36.2 Implementation barriers and actions

Barrier	Action
Lack of understanding of risk management and belief that it will suppress entrepreneurship	Establish a shared understanding, common expectations and a consistent language of risk in the organization
Lack of support and commitment from senior management	Identify a sponsor on the main board of the organization and confirm shared and common priorities
Seen as just another initiative, so relevance and importance not accepted	Agree a strategy that sets out the anticipated outcomes and confirms the benchmarks for anticipated benefits
Benefits not perceived as being significant	Complete a realistic analysis of what can be achieved and the impact on the mission of the organization
Not seen as a core part of business activity and too time-consuming	Align effort with core processes and achievement of the mission of the organization
Approach too complicated and over-analytical (risk overkill)	Establish appropriate level of sophistication for risk management framework and undertaking risk assessments
Responsibilities unclear and need for external consultants unclear	Establish agreed risk architecture with clear roles and accepted risk responsibilities
Risks separated from where they arose and should be managed	Include risk management in job descriptions to ensure that risks are managed within the context that gave rise to the risks
Risk management seen as static activity not appropriate for a dynamic organization	Align risk management effort with the mission of the organization and with the business decision-making activities
Risk management too expansive and seeking to take over all aspects of the company	Be realistic: do not claim that *all* of the business activities within the organization are risk management by another name

One of the important considerations regarding the time frame for implementation will be the documentation methodology. If a comprehensive risk management information system (RMIS) is to be introduced, the timescale for successful and complete implementation may be extended.

Changing face of risk management

As with any management initiative that becomes embedded within the way the organization operates, a successful risk initiative is bound to develop and become more sophisticated. Developments in the discipline of risk management, especially during the past 10 years, have been dramatic. Also, the level to which risk management requirements have become embedded within corporate governance has been extensive.

Many new developments of risk management have appeared during that time. In the 1990s, risk management practitioners used to talk about integrated or holistic risk management, but now the universally accepted terminology for the broad application of risk management across the whole organization is enterprise risk management (ERM). Similarly, operational risk management (ORM) has been established and developed very substantially during a shorter time period of perhaps five years.

In many ways, the fact that the risk management discipline continues to develop and adapt itself to changing circumstances can be seen as beneficial. However, there is a danger that risk management practitioners will be seen to be delivering an ever-changing and therefore inconsistent message.

That is not to say that risk management should become a static discipline, but it is important to remember that changing the basis on which risk management analysis and advice is offered and appearing to be changing the very nature of the risk management process will cause confusion and lack of interest amongst the senior board members.

Any review of the changing face of risk management has to acknowledge the global financial crisis and the role that risk management played in the development of this situation. As the global financial crisis developed, newspaper and television reports constantly repeated two messages: 'risk is bad' and 'risk management has failed'. Neither of these statements is true. It is essential that organizations take appropriate risks, and the failures that led to the global financial crisis were failures in the application of risk management, not failures of risk management itself.

It is undoubtedly the case that taking too much risk may be inappropriate and can result in failure of the whole organization. However, the experience of many organizations is that they almost always get away with it, or (at the very least) manage to survive. A detailed understanding of the level of risk embedded in the organization is not intended to put a stop to all bold strategic decisions. Risk awareness should not prevent an organization embarking on a high-risk strategy, but the decisions will be taken with full awareness of the risks that are involved.

Organizations should continue to look for opportunities and, from time to time, acknowledge that there is a good opportunity that looks very risky. The organization may still have an appetite for embarking on that risky strategy, but the next stage of discussion should be about how

to manage the risks so that they remain within the risk capacity of the organization, and how to measure the risks so that the board remains aware of the actual risk exposure.

The global financial crisis does not represent a failure of risk management. It represents a failure to completely and correctly apply risk management procedures and protocols. Figure 13.2 (page 128) illustrates the risk appetite of a risk-aggressive organization. When an organization is risk aggressive, it limits the range of risks that the board will consider, as there is limited scope for identifying risks as high likelihood and high impact. In other words, the universe of risk for that organization is severely restricted and will exclude risks that should receive the board attention.

If the organization is risk aggressive and operates to a model in line with Figure 13.2, very few priority significant risks will be identified. This will result in the organization creating a 'closed universe of risk' that potentially restricts broader discussion and analysis. However, there is nothing inherently incorrect about an organization being risk aggressive. If an organization is risk aggressive, there is an increased need to revisit risk assessments, challenge the scope and results of risk analysis activities, and ensure that a highly dynamic approach to risk management is maintained at all times and at all levels in the organization.

In addition to the concerns about risk management raised by the global financial crisis, certain other challenging issues for risk management exist. The concepts of risk appetite and the upside of risk are useful ideas, but more development work is required before the definitions and successful application of these concepts can bring guaranteed benefits.

Concept of risk appetite

As risk management develops and becomes more sophisticated, certain of the terms that are used become central to the successful application of the discipline. These include risk appetite. It is intuitively obvious that an organization needs to have a feeling for the level of risk that it is willing to accept. Several approaches to the definition and application of the concept of risk appetite are discussed in this book.

Nevertheless, the definition and application of the concept of risk appetite remains a considerable difficulty for risk management practitioners. It is the case that current risk management standards, as well as those that are under development, all state that organizations should recognize their risk appetite at an early stage.

This appears to contradict a key tenant of risk management, which is to say that risks should not be managed out of context. Just as risks should not be managed out of context, so the identification of risk appetite out of context is illogical and probably impossible. Risk appetite has to be identified within the context of the organization, its strategy, projects and routine operations.

There can be no doubt that the topic of risk appetite will receive more attention in future, and risk management practitioners need to get a better understanding of what this concept means and how it can be applied. The riskiness index described in an earlier chapter takes a somewhat different approach.

Organizations, just like individuals, do not actively seek risk. An individual may be described as a risk taker, but the reality will be that such a person enjoys activities that have a high level of risk attached. It is the activity that appeals to the individual in the first instance, not the actual risk. People may be identified as risk takers because they have a high-risk hobby or pastime. That does not mean that the risk taking for this individual will extend to crossing a busy road without looking. In other words, risk taking has to be seen within the context of the activity and the intended rewards.

Organizations are similar in that it is the strategy, project or activity that appeals to the board, not the actual risk. An organization may embark on a risky strategy, approve a risky project or be operating risky processes. However, it is the business drivers and imperatives that are the primary concern for board members, not the level of risk involved. It is more often the case that the level of risk comes with the defined strategy, rather than the risk appetite defining the strategy.

Concept of upside of risk

Another issue of fundamental difficulty for risk management practitioners is that of the upside of risk. There are many approaches to the upside of risk and most of them are valid, coherent and helpful. In particular, the idea that organizations should undertake an assessment of opportunities that come their way is clearly good management. The outcomes of successful risk management have already been described as compliance, for assurance, decisions and efficiency/effectiveness/efficacy (CADE3).

At its most simplistic, and specifically in relation to hazard risks, the upside of risk is that there is less down side. However, that is not a very compelling reason for senior managers to support a risk management initiative. Perhaps the most easy to explain and the most compelling thought is that the upside of risk is the ability to pursue a business opportunity that competitors would be unwilling to embrace. It would also be part of the explanation to say that competitors would be too risk averse to take such a high-risk opportunity.

With so much talk about the upside of risk, it has become a problem for risk management practitioners. The range of analyses from less down side to formalized opportunity management is wide and lacks focus. The board of an organization is not going to be persuaded by such a wide-ranging and-ill defined set of concepts and approaches. Clearly, the discipline of risk management needs to get a better understanding of the upside of risk and sell the message to the board.

Perhaps there is also scope for the risk management standards to take a more coherent approach to the upside of risk. An approach employed in some risk management standards is that the 4Ts should be extended to include the fifth T of 'take the risk'. Very often, the established standards fail to recognize that the organization will be taking the opportunity and the intended rewards, rather than deliberately taking the risk for its own sake.

Future developments

Chapter 6 considered some of the better-known risk management standards. A risk management standard is a combination of a risk management framework and a description of the risk management process. On this basis, the best-established risk management standard was the Australian Standard AS 4360, which was withdrawn in favour of ISO 31000 in 2009. The other risk management standard in common use is the IRM risk management standard published in 2002.

British Standard BS 31100 was published in 2008 and is a useful addition to the available risk management standards and frameworks. Also, the publication of ISO 31000 in 2009 leads to the possibility that there may be international standardization of risk management standards in due course.

COSO is a risk management framework and is widely used because of its association with the requirements of the Sarbanes–Oxley Act of 2002. The CoCo internal control framework is described in Chapter 31, and the approach adopted by CoCo is that when an adequate control environment (or risk-aware culture) has been established, an appropriate level of control will be achieved.

This final chapter has been a review of the benefits of risk management, together with a consideration of the practical steps required to successfully implement a risk management initiative. The chapter has also considered the changing face of risk management and the difficulties that such a rapidly developing discipline faces in continuing to persuade the board of organizations that any new or revised approach to risk management is more valid than previous versions of the same discipline.

Finally, this chapter has considered two of the most difficult issues for risk managers: risk appetite and the upside of risk. Greater clarity has to be brought to these issues regarding the definition and application of these concepts. The key message for risk management practitioners is that the board is interested in the level of risk exposure faced by the organization, but sees it as a consequence of the strategy, projects and operations of the organization.

When confronting these challenges for risk management, practitioners should be cautious about how these difficult concepts are addressed in formalized risk management standards. Development work on British Standard BS 31100 and ISO 31000 has included detailed discussions on how to represent the upside of risk within the standards.

Management initiatives often come and go. A particular approach becomes fashionable for a while and then fades away. It is unlikely that this will happen to risk management, because the requirement to have risk management procedures in place has become mandatory in many sectors. Also, the global financial crisis has resulted in a detailed analysis of the benefits that risk management can bring and how these can be achieved. The brief article below illustrates how risk management is valued around the world and why it is here to stay.

Risk management is here to stay

Every day, managers and employees practise risk management by making decisions on what to do, and how and when to do it. In both our personal and business lives our decisions are based on a variety of factors. Do I have the time or money? Do I need help to accomplish this? Enterprise risk management (ERM) is a change in philosophical focus for individuals from the 'I' to the 'we'. Does the organization have the capacity? Has the organization set aside the funds? Will this impact other business units?

ERM is not just a passing trend. It is here to stay and is being driven by both governance issues and the demands of the citizen. Companies, charities and public sector organizations have successfully embraced ERM.

Risk management does not have to be complex or a heavy resource user. It can be tailored to meet the needs of the organization in its early stages and modified as the level of sophistication and comfort with the process grows. It is a systematic and proactive approach to managing risk. This means that high-risk exposure areas are understood, managed and controlled to an acceptable level of exposure so that the organization is properly protected to minimize negative consequences. It allows the organization to focus on what is important to control versus what is easy to control.

Case study

BP – risk reporting

In 2008, the audit committee reviewed reports on risks, controls and assurance for the BP business segments (Exploration and Production, Refining and Marketing), together with alternative energy, information technology and services, the proposed reorganization of the group finance function and BP's trading function. The committee also reviewed BP's long-term contractual commitments and the provisions made for environmental remediation and decommissioning.

A joint meeting with the safety, ethics and environment assurance committee was held to review the general auditor's report on internal controls and risk management. A further joint meeting was held in early 2009 to assist the board in its assessment of the effectiveness of internal controls and risk management in 2008.

The committee discussed key regulatory issues during the year as part of its standing agenda items, including the quarterly internal audit findings report and a review of the company's evaluation of its internal controls systems as part of the requirement of section 404 of the Sarbanes-Oxley Act. The effectiveness of BP's enterprise level controls was examined through the annual assessment undertaken by the internal audit function.

The lead audit partner from the external auditors attends all meetings of the audit committee at the request of the committee chairman. The committee held two private meetings during the year with the external auditors without the presence of BP management, in order to discuss issues or concerns from either the committee or the auditors.

Performance of the external auditors is evaluated by the audit committee each year, with particular scrutiny of their independence, objectivity and viability. Independence is maintained through the limiting of non-audit services to tax and audit-related work that fall within defined categories. This work is pre-approved by the audit committee and all non-audit services are monitored quarterly.

During the year, the audit committee evaluated the performance of the internal audit function and agreed to the proposed programme of work for the year (being satisfied that it appropriately responded to the key risks facing the company and that the function had adequate staff and resources to complete its work).

The audit committee received an annual certification report from the group compliance and ethics function, together with quarterly reports that highlighted financial issues raised through the group-wide employee concerns programme. The committee further received quarterly updates from internal audit on instances of actual or potential fraud.

Annual Report and Accounts 2008

Appendix A: Glossary of terms

The table below sets definitions and (as necessary) cross references for 101 of the risk management terms used in this book. The reference column provides information on the location within the book where further information is provided, including reference to a relevant figure or table when appropriate. The relationship between the various acronyms is shown in the implementation guide set out in Appendix B.

There is an international standard related to risk management vocabulary and definitions. This is ISO/IEC Guide 73 'Risk management – Vocabulary – Guidelines for use in standards'. Where appropriate and to the extent that is possible, the definitions used in Guide 73 are referenced in this book.

However, it is not possible to use a unified terminology because risk managers in different disciplines use their own words and definitions. Indeed, the various risk management standards produced around the world use different terminology and definitions. ISO Guide 73 attempts to provide a unified language of risk, but it may take some time for these definitions to be universally adopted.

Term	Definition	Reference
Accept	See 'Tolerate'	Chapter 27
Avoid	See 'Terminate'	Chapter 27
Benchmark test	Series of established criteria to determine whether a risk is significant to the organization	Chapter 15 Table 15.1
BIA	See 'Business impact analysis'	Chapter 18
Business continuity plan	Plan to ensure continuity of business operations in the event of a serious incident that impacts the organization	Chapter 18
Business impact analysis	Analysis to assess the potential damage, loss or disruption that would be caused by the failure of critical business processes	Chapter 18

Term	Definition	Reference
CADE3	See 'Compliance, assurance, decisions and efficiency/effectiveness/efficacy'	Chapter 5
Captive insurance company	Insurance subsidiary, owned by an organization, to participate in the insurance programme for that organization and sometimes to provide insurance for the customers of the organization	Chapter 30 Figure 30.1
Chief risk officer	Job title for risk manager appointed to the board of the organization	Chapter 9
Compliance, assurance, decisions and efficiency/ effectiveness/efficacy	Summary of the main benefits derived from a successful (enterprise) risk management initiative	Chapter 5
Contractual transfer	See 'Treatment'	Chapter 27 Table 27.1
Control	Actions taken to reduce the likelihood and/or magnitude of a risk	Chapter 28
Control environment	Overall attitude, awareness and culture of the organization regarding risk management and/or internal control, referred to in the COSO (ERM) framework as the 'internal environment'	Chapter 31 Table 31.2
Control risk	Category of risk that is associated with the management of uncertainty	Chapter 1
Control risk self-assessment	Self-audit exercise completed by a department or business unit to report on current status of control and control activities	Chapter 33 Table 33.4
Control vector	Illustration on a risk matrix of the change in risk likelihood and/or risk magnitude achieved by an individual control	Chapter 26 Figure 26.4
Core process	Set of co-ordinated business activities designed to deliver a stakeholder expectation or shared stakeholder expectation, which may be strategic, tactical or operational	Chapter 21 Figure 20.1
Corporate governance	Set of activities and policies that control the way in which an organization is directed, administered and/or controlled	Chapter 19 Figure 19.1

Term	Definition	Reference
Corporate social responsibility	Management of an organization to take account of the impact of activities on customers, suppliers, employees, communities, other stakeholders, as well as the environment	Chapter 35 Table 35.1
Corrective control	See 'Treatment'	Chapter 28 Table 28.1
Cost containment	See 'Loss control'	Chapter 16
CRO	See 'Chief risk officer'	Chapter 9
CRSA	See 'Control risk self-assessment'	Chapter 33 Table 33.4
CSR	See 'Corporate social responsibility'	Chapter 35 Table 35.1
Current risk	The level of a risk that currently exists, taking into account the controls that are already in place, sometimes referred to as 'net risk' or 'managed risk', but most frequently as 'residual risk'	Chapter 15 Figure 15.3
Damage limitation	See 'Loss control'	Chapter 16
Detective control	Type of control designed to identify that a hazard risk has materialized, so that actions can be taken to avoid further or greater losses	Chapter 28 Table 28.1
Directive control	Type of control based on giving directions to people to behave in a certain way and/or follow established procedures	Chapter 28 Table 28.1
Disaster recovery plan	Plan for use in the event of a serious loss, such as IT failure, fire or earthquake to enable the organization to recover from the disaster	Chapter 18
DRP	See 'Disaster recovery plan'	Chapter 18
Eliminate	See 'Terminate'	Chapter 27
Embedded risk management	See 'Leadership, involvement, learning, accountability and communication'	Chapter 11 Table 11.1
Enterprise risk management	For a range of definitions of 'enterprise risk management', see Table 25.1	Chapter 25 Table 25.1

Term	Definition	Reference
ERM	See 'Enterprise risk management'	Chapter 25
Frequency	See 'Likelihood'	Chapter 1
GRASP	See 'Guardian of the risk architecture, strategy and protocols'	Chapter 9 Table 9.2
Guardian of the risk architecture, strategy and protocols	Suggested description of the range of activities and responsibilities undertaken by a typical risk manager, as related to the 'risk management framework'	Chapter 9 Table 9.2
Hazard risk	Category of risk that is associated with the management of pure risks, or the control of events that can only undermine key dependencies and/or the achievement of objectives	Chapter 1
Heat map	See 'Risk register'	Chapter 8
Impact	The size and nature of the consequences of a risk materializing, as compared with the magnitude of the event itself	Chapter 15
Inherent risk	Level of a risk before any control activities are applied, sometimes referred to as the 'gross level' or 'absolute level' of the risk	Chapter 15 Figure 15.3
Insurance	See 'Transfer'	Chapter 30
Internal audit	Internal to the organization (although maybe outsourced), yet independent group of people, or set of activities, monitoring the effectiveness and efficiency of control activities	Chapter 32
Internal control	For a range of definitions of 'Internal control', see Table 31.1	Chapter 31 Table 31.1
Leadership, involvement, learning, accountability and communication	Set of attributes that should be present in order to achieve successful embedding of (enterprise) risk management in the organization	Chapter 11 Table 11.1
Likelihood	Evaluation or judgement regarding the chances of a risk materializing, sometimes referred to as 'probability'	Chapter 15

Term	Definition	Reference
LILAC	See 'Leadership, involvement, learning, accountability and communication'	Chapter 11 Table 11.1
Loss control	Range of activities to reduce the potential impact of hazard risks on the organization, including loss prevention, damage limitation and cost containment	Chapter 16
Loss prevention	See 'Loss control'	Chapter 16
Magnitude	Size of the event when a risk materializes, sometimes referred to as 'severity' of the event – to be compared with the impact or consequences of the risk materializing	Chapter 1 Figure 1.1
Material failure	Failure of controls in an organization, resulting in loss of a magnitude that is considered important by auditors	Chapter 33
Nolan principles	Set of principles that should govern the behaviour of the people in public life	Table 19.2
Operational risk	Risk that can impact the key dependencies or corporate objectives of an organization, with the impact materializing immediately the risk occurs Defined in Basel II and BS 31100 as 'risk of loss or gain, resulting from inadequate or failed internal processes, people and systems or from external events'	Chapter 23
Operational risk management	Approach to risk management associated, in particular, with banks, insurance companies and other financial institutions, where the measurement of the level of 'operational risk' is required by Basel II or similar requirement	Chapter 23
Opportunity risk	Category of risk that is associated with the management of speculative opportunities, where the intention is to benefit from the investment	Chapter 1
Organization	Any corporate entity that exists to achieve a mission, fulfil corporate objectives or deliver stakeholder expectations	Chapter 1
ORM	See 'Operational risk management'	Chapter 23

Term	Definition	Reference
PACED	See 'Principles of risk management'	Chapter 5 Table 5.1
PRAM	See 'Project risk assessment and management'	Chapter 22 Table 22.1
Preventive control	Type of control that is designed to eliminate the possibility of an undesirable risk materializing	Chapter 28 Table 28.1
Principles of risk management	Set of attributes that define the features of a successful (enterprise) risk management initiative, summarized as proportionate, aligned, comprehensive, embedded and dynamic (PACED)	Chapter 5 Table 5.1
Project risk	Risk that could cause doubt about the ability to deliver a project on time, within budget and to specification/performance/quality Defined in BS 31100 as 'Risk relating to delivery of a product or service, especially with the constraints of time, cost and quality'	Chapter 22
Project risk assessment and management	Process developed by the Association for Project Management (APM) that enables the successful analysis and management of the risks associated with a project, often referred to as PRAM	Chapter 22 Table 22.1
Proportionate, aligned, comprehensive, embedded and dynamic	See 'Principles of risk management'	Chapter 5 Table 5.1
RASP	See 'Risk management framework'	Chapter 7
Reduce	See 'Treat'	Chapter 27 Table 27.1
Residual risk	See 'Current risk'	Chapter 15 Figure 15.3
Response	Stage in the risk management process that involves decisions on how to respond to the risks faced by the organization, including (for hazard risks) decisions regarding whether to tolerate, treat, transfer or terminate (4Ts); the risk response is referred to in some standards as treat or treatment	Chapter 27 Table 27.1

Term	Definition	Reference
Retain	See 'Tolerate'	Chapter 27 Table 27.1
Risk	For a range of some of the accepted definitions of 'Risk', see Table 1.1	Chapter 1 Table 1.1
Risk appetite	The level of risk that it is acceptable to the organization, encompassing the hazard risks that it is willing to tolerate, the control risks that it is willing to accept and the opportunity risks in which it is willing to invest Defined in BS 31100 as 'Amount and type of risk that an organization is prepared to seek, accept or tolerate'	Chapter 26 Figure 26.2
Risk architecture, strategy and protocols	See 'Risk management framework'	Chapter 7
Risk assessment	Means by which significant risks to the organization are evaluated and prioritized by undertaking the activities of 'Risk recognition' and 'Risk ranking'	Chapter 13
Risk assurance	Means by which an organization receives reasonable assurance that the significant risks are being adequately controlled	Chapter 33 Table 33.3
Risk capacity	Maximum level of risk to which the organization should be exposed, having regard to the financial and other resources available	Chapter 26 Figure 26.2
Risk exposure	Level of risk to which the organization is actually exposed, either with regard to an individual risk or the cumulative exposure to the risks faced by the organization	Chapter 26 Figure 26.2
Risk management	For a range of the recognized definitions of 'risk management', see Table 4.1	Part 1 Table 4.1
Risk management framework	Set of activities that support the risk management process, referred to in this book as the risk architecture, strategy and protocols (RASP) Defined by ISO Guide 73 as a set of interrelated activities and rules for co-ordinating and directing risk management processes within an organization	Chapter 6 Table 7.1

Term	Definition	Reference
Risk management information system	Computer software system and/or part of the intranet of the organization that records and communicates a range of risk management information	Chapter 12 Table 12.2
Risk management process	Co-ordinated range of activities that deliver management and control of risks within the organization, referred to in this book as recognition, ranking, responding, resourcing controls, reaction planning, reporting and review (7Rs)	Figure 4.1 Table 4.3
Risk management standard	Guidance to organizations on the design and implementation of risk management and made up of a description of the risk management process, together with advice on establishing a suitable risk management framework	Chapter 6
Risk map	See 'Risk matrix'	Figure 1.1
Risk matrix	Presentation of risk information or risk analysis on a 2 x 2 graph, sometimes referred to as a risk map or heat map, and often used to provide a graphical representation of the information contained in the risk register	Figure 1.1
Risk profile	See 'Risk register'	Chapter 8
Risk ranking	Stage in the risk assessment process that rates and prioritizes individual risks according to the likelihood of occurrence and the impact (or sometimes magnitude) of the risk should it materialize, also referred to as risk analysis, risk evaluation or risk estimation	Chapter 13
Risk recognition	First stage in the risk management process, which involves the organization in the identification of all of the risks that it faces	Chapter 13
Risk register	Profile and record of the risks faced by an organization, with particular emphasis on the significant risks, the controls currently in place, additional controls that have been identified and responsibility for control activities	Chapter 8

Term	Definition	Reference
RMIS	See 'Risk management information system'	Chapter 12 Table 12.2
Sarbanes–Oxley Act of 2002	US legislation that encourages use of the COSO Internal Control framework (1992) to ensure that the information disclosed by companies listed on the stock exchange is accurate	Chapter 34
Severity	See 'Magnitude'	Chapter 15
Significant risk	Risk with the ability to impact about the benchmark test for significance for the organization	Chapter 15 Table 15.1
Significant weakness	Weakness in controls in an organization with the potential to cause a significant or material loss	Chapter 33
Stakeholder	Persons or groups of persons with an interest in the activities of the organization	Chapter 20
Strategic risk	Long-term or opportunity risk that can impact the key dependencies or corporate objectives of an organization, with the impact materializing some time after the action or event occurs Defined in BS 31100 as 'Risk concerned with where the organization wants to go, how it plans to get there and how it can ensure survival'	Chapter 3
Tactical risk	Medium-term, control or uncertainty risk that is associated with change, projects and the means by which the organization will deliver strategy	Chapter 3
Target risk	The ultimate level of risk that is desired by the organization when all cost-effective/necessary controls have been implemented	Chapter 15 Figure 15.3
Terminate	Risk response that is appropriate when the level of risk is not acceptable to the organization, also referred to as 'avoid' or 'eliminate'	Chapter 27 Table 27.1
Tolerate	Risk response option that is appropriate when the level of risk is acceptable to the organization, also referred to as 'accept' or 'retain'	Chapter 27 Table 27.1

Term	Definition	Reference
Transfer	Risk response option for risks that the organization wishes to transfer to another party, usually by means of insurance or contractual transfer	Chapter 27 Table 27.1
Treat	Risk response option for risks that the organization believes can be further treated by the introduction of cost-effective (corrective) controls, also referred to as 'control' or 'reduce'	Chapter 27 Table 27.1
Upside of risk	Additional benefits available to the organization by taking risk – for a range of descriptions of the 'Upside of risk', see Table 17.1	Chapter 17 Table 17.1

Appendix B: Implementation guide

The table below provides a detailed overview of the steps involved in the implementation of a successful enterprise risk management (ERM) initiative. It uses the structure described in Figure 29.3 (page 275) to indicate the steps involved in learning from controls.

Successful implementation of an ERM initiative is an ongoing process that involves working through the 10 steps set out below on a continuous basis. Also, because it is sometimes difficult to recognize the distinction between planning, implementing, measuring and learning, the 10 steps in implementing an ERM initiative are presented under the headings:

- planning/implementing;
- implementing/measuring;
- measuring/learning;
- learning/planning.

The information in the table below is an extended version of the steps involved in achieving successful risk management, as set out in Table 36.1 (page 329). In addition to identifying the 10 steps involved in the successful implementation of an ERM initiative, the table also describes the concepts or tools and techniques that are required to deliver each step.

Many acronyms are used in this book and these are referenced in the table below to show where they fit into the overall implementation of risk management in general, and ERM in particular. In addition to identifying the acronyms relevant to each step, the table also provides reference to the chapter of the book where further information can be found.

The steps set out below relate to the implementation of an overall enterprise risk management initiative. Much of this book is concerned with the implementation of risk management in relation to specific individual risks. ERM is the overall philosophy that consolidates the management of individual risks into a unified and consistent approach to risk across the whole enterprise.

Activity		Concepts/tools and techniques	Acronym	Reference
	Planning/implementing			
1.	Identify intended benefits of the enterprise risk management initiative and gain board support	Risk appetite Corporate governance	ERM CADE3	Chapter 5 Chapter 19 Chapter 25 Chapter 26
2.	Plan the scope of the ERM initiative and develop common language of risk	RM sophistication Upside of risk Stakeholder expectations	PACED 7Rs	Chapter 5 Chapter 17 Chapter 20
3.	Establish the risk management strategy, framework and the roles and responsibilities	Risk management policy Risk architecture Level of risk maturity	RASP 4Ns	Chapter 6 Chapter 7 Chapter 10
	Implementing/measuring			
4.	Adopt suitable risk assessment procedures and an agreed risk classification system	Risk protocols Risk management guidelines Risk classification systems Risk description	FIRM PESTLE COSO	Chapter 8 Chapter 9 Chapter 13 Chapter 14
5.	Establish risk significance benchmarks and undertake risk assessments	Benchmark tests of significance Risk register		Chapter 8 Chapter 15
6.	Determine risk appetite and risk tolerance levels and evaluate the existing controls	Risk appetite Risk matrix Loss control	4Ts PCDD	Chapter 13 Chapter 16 Chapter 26 Chapter 27 Chapter 28
	Measuring/learning			
7.	Ensure cost-effectiveness of existing controls and introduce improvements	Risk improvement plans Reaction planning	BIA BCP/DRP	Chapter 16 Chapter 18 Chapter 29
8.	Embed risk-aware culture and align risk management with other management tasks	Control environment Resource allocation Risk communications Business model	LILAC	Chapter 11 Chapter 12 Chapter 21 Chapter 31

Activity		Concepts/tools and techniques	Acronym	Reference
	Learning/planning			
9.	Monitor and review risk performance indicators to measure ERM contribution	Audit plan Sources of risk assurance	RMIS	Chapter 12 Chapter 33
10.	Report risk performance in line with legal and other obligations and monitor improvement	Risk reporting Turnbull/Sarbanes–Oxley	COSO CoCo	Chapter 32 Chapter 34

Index

NB: page numbers in *italic* indicate figures or tables

THIS PAGE IS INTENTIONALLY LEFT BLANK