EDINBURGH
BUSINESS SCHOOL
HERIOT-WATT UNIVERSITY

# Strategic Risk Management

**Professor Alexander Roberts**

**Dr William Wallace**

**Mr Neil McClure**

RK-A2-engb 1/2012 (1024)

This course text is part of the learning content for this Edinburgh Business School course.

In addition to this printed course text, you should also have access to the course website in this subject, which will provide you with more learning content, the Profiler software and past examination questions and answers.

The content of this course text is updated from time to time, and all changes are reflected in the version of the text that appears on the accompanying website at http://coursewebsites.ebsglobal.net/.

Most updates are minor, and examination questions will avoid any new or significantly altered material for two years following publication of the relevant material on the website.

You can check the version of the course text via the version release number to be found on the front page of the text, and compare this to the version number of the latest PDF version of the text on the website.

If you are studying this course as part of a tutored programme, you should contact your Centre for further information on any changes.

Full terms and conditions that apply to students on any of the Edinburgh Business School courses are available on the website www.ebsglobal.net, and should have been notified to you either by Edinburgh Business School or by the centre or regional partner through whom you purchased your course. If this is not the case, please contact Edinburgh Business School at the address below:

Edinburgh Business School
Heriot-Watt University
Edinburgh
EH14 4AS
United Kingdom

**Tel** + 44 (0) 131 451 3090
**Fax** + 44 (0) 131 451 3002
**Email** enquiries@ebs.hw.ac.uk
**Website** www.ebsglobal.net

# Strategic Risk Management

**Professor Alexander Roberts** PhD, MBA, FCCA, FCIS, MCIBS.
Director, Centre for Strategy Development and Implementation.
Professor Roberts is Professorial Fellow of Edinburgh Business School (EBS), the Graduate School of Business at Heriot-Watt University. Professor Roberts is a doctoral (PhD) graduate of the London Business School (1987). He lectures, researches and consults for major organisations on strategy development and implementation and related issues. The practical relevance of his work is underpinned by 15 years in senior management, including 10 years at executive director level within multinational subsidiaries of American and European based businesses. Professor Roberts founded the Doctorate in Business Administration (DBA) in Strategic Focus programme at EBS.

Professor Roberts is author of the forthcoming MBA/DBA distance learning texts in *Making Strategies Work* and is joint author, with Dr Wallace and others of the texts in *Project Management*, *Strategic Risk Management*, *Mergers and Acquisitions*, *Introduction to Business Research*, *Business Research Methods* and *Applied Business Research*.

**Dr William Wallace** BSc (Hons), MSc, PhD, MCIOB, MAPM.
Senior Teaching Fellow, Centre for Strategy Development and Implementation.
Dr Wallace is Senior Teaching Fellow of Edinburgh Business School (EBS), the Graduate School of Business at Heriot-Watt University. Dr Wallace chairs the MBA/DBA courses in Project Management and Strategic Risk Management. Dr Wallace has an extensive range of academic and industrial experience. The work for both his first degree and masters degree (Loughborough 1983) established a project management and risk management academic framework. After completing his PhD (Heriot-Watt 1986) he worked as a senior practitioner in, and consultant to, a number of public and private sector organisations, before returning to academia in 1995. He served as a member of the Heriot-Watt University Faculty Board of Engineering from 1997 to 2001 and on the Heriot-Watt University External Studies Committee 1998–2001.

**Mr Neil McClure** BSc(Hons), MBA, ACII, MIOSH.
Risk Management consultant.
Mr McClure is a professional risk management consultant with considerable experience in the field of risk management. Mr McClure gained his professional qualifications in insurance while working as a loss prevention advisor with one of the UK's largest commercial insurers. He then joined a specialist risk management consultancy offering clients advice on their risk management capability. From here Mr McClure joined a specialist risk management consultancy which provided global clients with advice and reviews of their risk management capability. He went on to found his own risk management consultancy. Mr McClure is now group risk manager one of Scotland largest private companies, a role which he describes as immensely varied and challenging.

First Published in Great Britain in 2003.

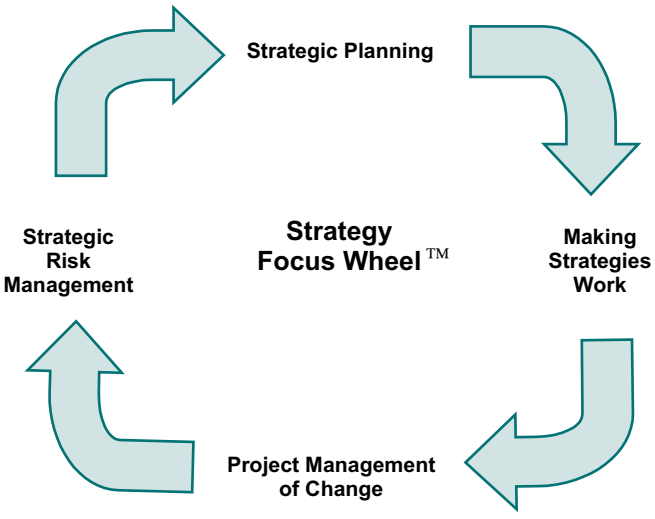
# Contents

# Preface

Risk management has come a long way from its origins in engineering and health and safety. It is now used on a wide range of applications across a range of commercial, industrial and other forms of enterprise. More and more organisations are establishing and developing risk management facilities, both as an internal initiative and in response to statutory and regulatory external pressures. A review of job advertisements in the press suggests that risk managers are often amongst the most highly paid of senior employees. By the end of this preface you will gain some idea of why they should be so highly valued.

In a world of rapid change, organisations that can identify the need for change, design the changes required and implement these changes more effectively and efficiently than others are more likely to survive and prosper. Those that cannot adapt to change are likely to perish. The Centre for Strategy Development and Implementation at Edinburgh Business School, Heriot-Watt University, was founded by Professor Alex Roberts in 2001 to address these issues.

The core of the Centre's work lies in four interrelated areas as shown in the Strategic Focus Wheel™ below. These four areas form the basis for separate Edinburgh Business School distance learning texts.




**The Strategic Focus Wheel™**

A. Roberts and A. MacLennan

The wheel is used to focus the efforts and resources of organisations on delivering their intended strategic objectives, and has four core elements.

- **Strategic planning** revolves around identifying the options available to an organisation and selecting the most appropriate. If strategic planning is done poorly, even the best implementation capability is unlikely to compensate.
- **Making strategies work** is a process for connecting the high-level strategic plan to the day-to-day activities that are critical to its delivery.

- **Project management of change** ensures completeness and control over the physical realisation of the chosen strategy. Project management provides a comprehensive set of tools and techniques that enable managers to plan and implement change effectively and increase the likelihood of achieving the various objectives of the change process. Used effectively project management is a central element of the wheel in that it makes things happen and delivers results.
- **Strategic risk management (SRM)** identifies, monitors and manages the risk profile of the organisation. Major changes in this profile can result in the need to revise or change the elements listed above and, in particular, to devise new strategic plans. Alternatively, changes may be due to the implementation of a new strategy. Strategic risk management covers four primary risk areas or levels. These are *strategic risk*, *change or project risk*, *operational risk* and *unforeseeable risk*. These basis risk types are discussed in more detail later in the module.

This text, *Strategic Risk Management*, is concerned with the risks that impact at all three of these levels.

The Edinburgh Business School Centre for Strategy Development and Implementation sees strategic risk management as a key tool for assisting in the management of change and associated risks because of its proven usefulness in a vast range of change situations. This is equally true whether designing and erecting a new building (changing a collection of materials, labour and other resources into a finished building), designing and implementing new organisational systems such as the human resource management function, or designing and implementing a new strategy for a whole organisation.

No matter what business an organisation is engaged in, it is exposed to risks. Risk and reward go hand in hand, and the significance of risk to the success or failure of a business is now even greater as technology allows actions and changes to be executed faster than ever before. In the modern world uncertainty has increased, but so have the opportunities for success. To succeed in this environment, managers must be able to manage risks in order that they can achieve their objectives for success. Human nature focuses upon the upside, and expects that the decisions, strategies, projects and operations will go well. No one would suggest that organisations should all become pessimists, but it is becoming increasingly clear that an organisation is much more likely to achieve a successful outcome if it plans and actively manages the risks across the enterprise. This course on strategic risk management is intended to equip modern managers with the knowledge and skills they need to manage risk at all levels of the organisation. It will show how risk management is a fundamental part of the strategic planning and implementation process, and how vital strategic risk management is in projects and operations.

The course is concerned with risk as a collective or integrated concept. Most approaches to risk and risk management concern themselves with one particular risk aspect or application. This limitation is acceptable provided the interest of the risk manager is restricted to the aspect or application concerned. Many organisations, however, operate under conditions of complex risk where it is not practical or desirable to consider specific risk areas in isolation. Organisational risks are linked together. Variations or changes in one specific risk do not occur in isolation. There are invariably linkages between risks that lead to corresponding variations in linked groups or clusters of risks.

In practice, organisations make decisions within a complex network of risks. Some risks are greater than others, and some risks are linked together more strongly than others.

Decisions that affect one risk have a direct impact on risks elsewhere. This concept of an interlinked schedule is referred to in the text as the *risk interdependency field*. It is argued that the *enterprise-wide view*, with its concomitant need to involve the entire organisation, is more accurate and useful than taking a restricted specific view. The enterprise-wide view allows managers to see the full complexities of the risks and dependencies that exist within the organisation and also to gain an appreciation of the likely effects or consequences of alternative decisions.

The text begins with a basic introduction to risk and risk management. These sections explore the background to risk and examine the main components likely to be encountered in any risk management system. The text goes on to consider strategic, change (project), operational and unforeseeable risk as separate risk interest levels or areas. These risk levels are then combined into the risk interdependency field, where risks are considered on an enterprise-wide basis, and where the relationships between risks at different levels and within different functions are made clear. Finally the *enterprise-wide risk management* with *risk interdependency field configuration process model* is developed and discussed.

This text in *Strategic Risk Management*, as part of the Strategic Focus Wheel™, is an *integrated text*. As a component of the wheel strategic risk management works with the other wheel disciplines to provide an organisation with tools and control that allow it to achieve strategic focus. Strategic risk management in this context is not a stand-alone discipline and cannot be regarded in isolation. The text makes frequent references to other Edinburgh Business School Master of Business Administration and Doctorate in Business Administration texts. The *Strategic Risk Management* text is designed to be read as a stand-alone document, but the discipline has to be considered in the wider context as being part of a larger collection of disciplines. Other disciplines such as the Project Management of Change are included in this text in sufficient detail to allow the reader to develop an understanding of project management in the context of its strategic risk management applications. Readers who wish to develop a greater understanding of project management are referred to the Edinburgh Business School distance learning text *Project Management*. References are made in the same way to a range of other Edinburgh Business School distance learning texts, including:

- *Strategic Planning*
- *Making Strategies Work*
- *Project Management*
- *Mergers and Acquisitions*
- *Corporate Governance.*

In order to develop a command of strategic focus, risk managers need to develop an understanding of the interrelationships between these disciplines as well as an understanding of the various risk levels and interdependencies between these levels across the full range of organisational activities.

Note also that this text is concerned with strategic risk management from a generic point of view. The text does not refer specifically to financial risk management as there are already two appropriate Edinburgh Business School distance learning texts: *Financial Risk Management 1* and *Financial Risk Management 2*.

The authors have made every effort in the text to illustrate fairly and without prejudice the concepts of risk management and their application, and on occasion they have made reference to named corporations and, by implication, their employees. All such references

are made in good faith for educational purposes and in no way does the appearance of a named corporation imply that the corporations so named, or their employees have been, or are, negligent in matters of risk management and it would be completely erroneous of any reader to draw such unwarranted and untrue conclusions, and nor does the absence of a named corporation imply anything similar or to the contrary.

# List of Abbreviations

| | |
|---|---|
| ACWP | actual cost of works performed |
| ADR | alternative dispute resolution |
| AGAP | all goes according to plan |
| AIB | Allied Irish Banks |
| ANZ | Australia & New Zealand |
| AOA | activity on arc |
| API | American Petroleum Institute |
| ART | alternative risk transfer |
| AT&T | American Telephone and Telegraph |
| BA | British Airways |
| BAA | British Airports Authority |
| BAC | budget at completion |
| BC | budgeted cost |
| BCP | business continuity plan |
| BCWP | budgeted cost of works performed |
| BCWS | budgeted cost of works scheduled |
| BIA | business impact assessment |
| CBA | cost–benefit analysis |
| CBA | critical business activity |
| CBoT | Chicago Board of Trade |
| CCR | change control response |
| CCS | change control section |
| CD | compact disc |
| CDES | computerised database estimating system |
| CEO | chief executive officer |
| CEV | certainty equivalent value |
| CFC | chlorofluorocarbon |
| CMS | configuration management system |
| COR | change order request |
| C-PIP | change project implementation plan |
| CPM | critical path method |
| CRO | chief risk officer |
| CSDI | Centre for Strategy Development and Implementation |
| CSF | critical success factor |
| CV | cost variance |
| CVI | cost variance index |
| DIY | do it yourself |
| DMS | draft master schedule |
| DRP | disaster recovery plan |

| | |
|---|---|
| DVD | digital versatile disc |
| EAC | estimate at completion |
| EBS | Edinburgh Business School |
| ECTC | estimated cost to complete |
| EH&S | environmental health and safety |
| EMV | expected monetary value |
| ETTC | estimated time to complete |
| EVA | earned value analysis |
| EWRM | enterprise-wide risk management |
| FAA | Federal Aviation Authority |
| FSA | Financial Services Authority |
| FX | foreign exchange |
| GAAP | generally accepted accounting principles |
| HR | human resources |
| ICA | Institute of Chartered Accountants |
| ISO | International Organisation for Standardisation |
| IT | information technology |
| KBA | key business activity |
| KEI | key environmental indicator |
| KPI | key performance indicator |
| LPE | London Petroleum Exchange |
| LSE | London Stock Exchange |
| MBR | market business risk |
| MCPT | merger customer protection team |
| MFR | market financial risk |
| MIT | merger integration team |
| MMP | multi-line multi-year product |
| MPT | merger project team |
| NCR | National Cash Registers |
| NPV | net present value |
| OBS | organisational breakdown structure |
| OfGEM | Office of Gas and Electricity Markets |
| OPEC | Organisation of Petroleum Exporting Countries |
| PC | personal computer |
| PCCS | project cost and control system |
| PERT | program evaluation and review technique |
| PEST | political, economic, social and technological |
| PII | professional indemnity insurance |
| PLE | project logic evaluation |
| PMS | project master schedule |
| PORV | pilot-operated relief valve |
| PR | public relations |
| PVAR | project variance analysis reporting |

| | |
|---|---|
| RBS | risk breakdown structure |
| RIF | risk interdependency field |
| SFR | speculative financial risk |
| SIT | specialist integration team |
| SOW | statement of work |
| SPP | strategic project plan |
| SRM | strategic risk management |
| SWOT | strengths, weaknesses, opportunities and threats |
| TCAS | traffic collision avoidance system |
| TOC | train operating company |
| VaR | value at risk |
| WAP | wireless application protocol |
| WBS | work breakdown structure |
| WHIF | What Happens IF |
| WP | works performed |
| WS | works scheduled |
| WTI | West Texas Intermediate |

# Module 1

# Introduction

## Contents



## Learning Objectives

By the time you have completed this module you should understand:

- the concept of risk;
- the concept of risk and opportunity;
- the basic levels of risk impact and types of risk;
- how risks can be classified;
- the idea of exposure, sensitivity and the risk profile;
- the concept of risk conditions and decision making;
- the concept of risk management.

*Note that these areas are covered in more detail (with examples and applications) in Modules 2 and 3.* The level of detail in this module is restricted as the objective of the module is to give a basic overview as an introduction to the subject rather than attempting to develop a detailed knowledge and understanding. Module 1 is intended to prepare the reader for the more detailed development that takes place in subsequent chapters.

## 1.1 Introduction

Module 1 introduces the concept of risk and risk management. The module explains how risks exist both inside and outside the organisation, and examines the level of threat that various risks can pose. It describes how the level and complexity of these risks tend to increase as a function of organisational size and complexity. It goes on to consider some basic risk types and risk classification systems, and examine the risk conditions under which decisions can be made. The module ends with an exposition of how risk management as a discipline has evolved in response to a growing demand from organisations to be able to manage and control these risks effectively.

## 1.2 The Concept of Risk

The English word 'risk' originates from the French word *risque*. The English word 'risk' is actually quite modern, having entered the language around 1650. It was first used in a formal legal sense in insurance documents that date to around 1730. People who lived before these dates were of course just as familiar with the idea of risk and reward as their descendants. For example, the English privateers who harried the Spanish treasure ships in the Caribbean and Central America in the late 16th century realised fully that they were engaged in a high-risk occupation. However, they also realised that this high-risk activity offered potentially very great rewards. They were prepared to take those risks because they offered potentially high returns. The privateers could make more money in one successful raid than they could make in a lifetime of normal paid employment. On the negative side, they could easily be killed or captured. The privateers did not call the negative aspect risk but they understood that it was something that had to be encountered and dealt with in order to have the chance of making a lot of money very quickly. They also understood that the risk had to be there. The potential gains from their actions would not have existed without the risk element.

Today the world is full of risks. The number of risks that exist increases as a function of both human and organisational evolution and development. As organisations become larger and more complex they tend to face an increasing array of complex and diverse risks. New forms of risk emerge all the time. Information technology (IT) risk is an obvious example. As organisations develop they tend to take advantage of the latest technology. They buy the latest computers and run the latest software. As these organisations use more and more IT, they become increasingly dependent upon it. They also develop an increasing IT risk in that the business may be crippled if (for any reason) the IT systems fail. IT risk was not a major consideration before so many companies became dependent on electronic data storage and communications. In 1970 IT risk was virtually non-existent. By 2000 it was one of the most significant risks facing virtually all commercial and industrial organisations.

In addition, as dependence on IT increases, new associated risks emerge. The risk of system failure can, to some extent, be reduced by ensuring that adequate safeguards and back-up systems are in place and that the IT support staff are sufficiently trained and aware. Associated external risks can, however, be much harder to control. In recent years the risk of malicious interference, fraud and theft through IT 'hackers' has increased dramatically. Electronic intruders pose an increasing threat to IT-dependent organisations and are responsible for more and more significant costs, in terms of both prevention and rectification. Yet hackers did not exist just a few years ago. The concept of 'hacking' into other people's servers became viable only as sufficient levels of technology made it a possibility.

Increasing reliance on IT also renders the complex organisation more vulnerable to relatively simple external risks. Anybody who has been in the middle of a Powerpoint presentation when there is an external interruption in power supply will appreciate this! An organisation that is reliant on IT is much more exposed to power supply interruption than an organisation that is not as reliant on IT. Increasing reliance on IT also generates exposure to relatively simple internal risks. A simple projector bulb failure renders the most detailed and well thought out Powerpoint presentation useless. The wise lecturer makes sure that he or she always has standby slides ready for use on the 'good old' overhead projector, although even this basic and relatively simplistic teaching tool is exposed to the risk of bulb failure.

Risks of course are not just limited to organisations. Individuals face varying degrees of risk in many aspects of everyday life. Depending on one's personal attitude one might consider the following list to represent personal activities that may generate a high level of risk:

- parachuting;
- rock climbing;
- smoking cigarettes;
- betting money on horses;
- investing in dot.com companies;
- playing poker for high stakes;
- entering a relationship;
- getting married.

These are activities rather than the risks themselves. Getting married (in the simplest sense) is financially risky in that a person assumes joint financial responsibility with a partner. It could be suggested that sharing financial risk through marriage actually reduces financial risk for an individual because the partner's income represents a cushion in the event of a negative event such as a pay cut or redundancy. It could be argued that the real financial risk involved in getting married comes if the couple end up falling out and decide to get a divorce. Divorce represents a high risk to a person's future financial standing, at least in the short to medium term.

Risk is an inherent factor of virtually every human endeavour. Human beings naturally consider risk and reward as part of any decision-making process, and people make decisions constantly, whether major or minor, directly or subconsciously. If a gambler is placing a bet on a horse, he or she might consider a whole range of variables that relate to the possible outcome of the race. These might include the fitness of competing horses, the skill of the competing jockeys, and how well the conditions suit the competing horses. Another gambler who is playing poker may have no idea what the competition has to offer and so uses a more intuitive, less structured and less formalised approach to assessing the potential risks and rewards of folding or playing.

Between the two extremes of 'scientific' and 'intuitive' risk and reward consideration, the human reasoning and evaluation of any particular event is based on decision making within the limits of what are acceptable and non-acceptable outcomes. The gambler does not like to lose, but there is a difference between losing what he or she can afford to lose and losing what he or she cannot afford to lose. The maximum loss limit that is affordable defines the upper limit of the range of acceptable outcomes. Losses above this limit are not affordable and are, therefore, unacceptable, irrespective of the size of the potential reward.

The consideration of risk and reward is the basis of risk analysis. Risk analysis can be considered as a basic function of the *human cognitive process*. People evaluate potential risks and rewards in terms of the range of acceptable outcomes when deciding on whether or not to do something. The human mind considers risk and reward as a form of model in which possible events and outcomes *(scenarios)* are considered in terms of possible actions. The possible gains are then balanced against the possible losses, and a subjective (or possibly objective) decision is made as to whether or not that outcome is acceptable. This process is the basis of decision making under *conditions of risk*. Human beings all perform this basic reasoning process many times every day, albeit on a subjective basis and often at a subliminal level.

It should be made clear that risk is not a negative concept. The universe is characterised by constant change, and the world in general is characterised by uncertainty. Change is a

dynamic mechanism and influences almost everything. Organisations and individuals evolve in much the same way as any other organic entity does. The evolutionary process itself has developed so that entities react to changes in the environment. Those entities that evolve most effectively are those that can adapt most efficiently to change.

Change is time driven, and observers can only look in one direction on the time continuum. As a result, very few events are certain apart from death. This listing can perhaps be extended to tax and death once society evolves to a reasonable level of civilisation. In such an environment all actions and endeavours must be subject to some degree of change and therefore uncertainty and therefore risk. However, risk is necessary in order for opportunity to exist. If a person or an organisation wants to develop an opportunity, they have to accept the risks that inevitably accompany that opportunity. The key issue is to be able to identify those risks and then manage them so that they do not threaten the continued existence of the person or organisation. The obvious extension is the development of a risk management system in which risks can be controlled at acceptable levels while corresponding opportunities are exploited.

Risk has a number of other positive attributes. Risk intimidates competitors. Every organisation has its own *risk appetite* and its own range of acceptable outcomes. There has to be a limit beyond which any organisation dare not go. If one organisation can raise the stakes to a level where the competition becomes intimidated, then that organisation inherits the opportunity to exploit that risk. This concept applies just as much to organisations as it does to a poker player when he or she continually raises the stakes on a particular hand.

Risk is a dynamic entity. There is always a temptation to see risk management as a static system when in fact risk management is not just about identifying potential negative events and then taking precautions against them. It is about looking at the complex world of business, analysing the myriad opportunities that present themselves, and then making an informed decision on which is the best one to accept. The equation is complicated by the fact that the apparent *risk universe* at any one time is in fact dynamic. The risk profile that faces an individual or organisation changes rapidly in response to changes in the environment. Even across the course of a single day the impact and likelihood of impact of a range of risks can change.

## 1.3 The Basic Risk Types

Strategic, change and operational risks are considered in more detail in Module 4, Module 5 and Module 6 respectively.

The number of possible sources and combinations of sources of risk is almost beyond classification. The primary classification typologies revolve around the origin of the risk and around the nature of the effect.

The most obvious initial classification of risk is to differentiate it in terms of the *risk level* within the organisation on which it impacts. The obvious classification in this respect is as listed below.

- strategic risk;
- change or project risk;
- operational risk;
- unforeseeable risk.

Over and above this basic classification, risk can also be classified in terms of the specific nature of the risk, its origin and characteristics, and the extent to which the risk is dependent upon or linked with other risks. A second possible classification is listed below.

- financial and knowledge risk;
- internal and external risks;
- speculative and static risks;
- risk interdependency.

It is important to appreciate that these classifications overlap. A *speculative* risk could exist at a *strategic level* or at an *operational level*. An *unforeseeable risk* could arise because of risk *interdependency* with another risk.

Each of these basic risk types is discussed in more detail in the following sections.

## 1.3.1 Strategic Risk

Strategic risk relates to risk at the corporate level, and it affects the development and implementation of an organisation's strategy. An example is the risk resulting from an incorrect assessment of future market trends when developing the initial strategy. In developing a strategy, an organisation makes an assessment of market conditions today. It then goes on to forecast the various changes that will occur in the market over a period of time. For example, a company manufacturing personal computers (PCs) might decide to adopt a strategy to include the development and introduction of faster and faster operating speeds. In doing so the company will presumably analyse the current market and decide that market research indicates that there will be a continuing high demand for faster and faster PCs. The strategic risk element applies in terms of whether or not that strategic decision was correct. It is reasonable to say that one example of strategic risk is the risk that the strategic decision is wrong.

Strategic risk includes risk relating to the long-term performance of the organisation. This includes a range of variables such as the market, corporate governance and stakeholders. The market is highly variable and can change at relatively short notice, as can the economic characteristics of the country or countries in which a given organisation is operating The corporate governance risk of the organisation includes risk relating to the reputation of the organisation and the ethics with which it operates. Examples include the reputation of the organisation and its desire to maintain that reputation, perhaps at the expense of innovation or new developments. Stakeholder risk includes the risk associated with the shareholders, business partners, customers and suppliers. Shareholder attitudes can change quickly if dividends fall.

Some typical examples of strategic risks are listed below.

1. **The strategic plan might be incorrect.**
   - Incorrect assumptions may have been made.
   - The environment may have been incorrectly assessed.
   - Sufficient resources may not be available.
   - The plan might not actually represent where the organisation really wants to go.

2. **The original strategic plan may have been correct but internal changes may have compromised it.**
   - Internal reorganisations may have led to a loss of efficiency.
   - Required changes in operational processes may not have been introduced.
   - Planned changes may not have delivered what was required.
3. **The original strategic plan may have been correct but external changes may have compromised it.**
   - The external environment may have changed significantly.
   - New competitors may have emerged.
   - New competing products may have been released.
   - Statutory controls may have changed.

Strategic risk is generally more difficult to manage than operational or change/project risk. Strategic risk tends to be applicable over a long term and is therefore very much time dependent. Most operational processes tend to continue without significant change over relatively long periods of time. Many small- to medium-sized change projects are designed and implemented within a relatively short timescale. They are unlikely to be affected by long-term changes in the political or economic environment.

Strategic risks also tend to be more complex and difficult to model and assess than operational and change/project risk. It is relatively simple to analyse attendance records for employees and from that make a prediction on likely sickness and absenteeism rates through the course of a project. It is much more difficult to assess the likelihood of occurrence of a significant change in the level of competition that is characteristic of a given sector. This depends on a whole range of complex and long-term variables that are very difficult to consider in a form that can be used for modelling and extrapolation.

In considering strategic risk management, the organisation is looking to move from current position A to desired position B as shown in Figure 1.1.

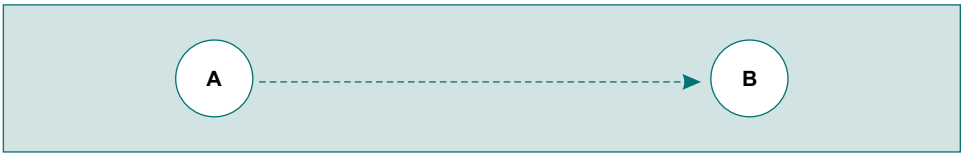



**Figure 1.1 Current and desired positions**

*Point A: current position.* This is where the company is now. The position is determined by a number of factors including market position, size, vulnerability, gearing, asset base and so on.

*Point B: desired position.* This is where the company directors want to be in X years' time. Again, this position can be determined and described using a wide range of variables.

The direct route to B represents the course upon which the company wishes to progress. In charting this course, the strategic risk manager can appreciate that there will be a range of both foreseeable and unforeseeable risks impinging upon this course. Some will be large risks; some will be small. Some may occur and some may not. Each one that does occur will affect the course of progression of the organisation from A to B. The organisation's strategy to get from A to B is really the collective management of these numerous competing risks, as shown in Figure 1.2.


**Figure 1.2 Strategic risk**

The risks that stand between position A and position B cannot be accurately determined. They may affect the achievement of the strategy more in some areas than in others. Wholly unforeseen events might affect the viability of navigating between A and B. The net result is that the company evolution suffers deflections as it attempts to implement the strategy or stay on course. Some risks have a greater impact than the strategy foresaw. Some have a lesser impact. The net result is a general divergence or 'set' from the desired course, as shown in Figure 1.3.

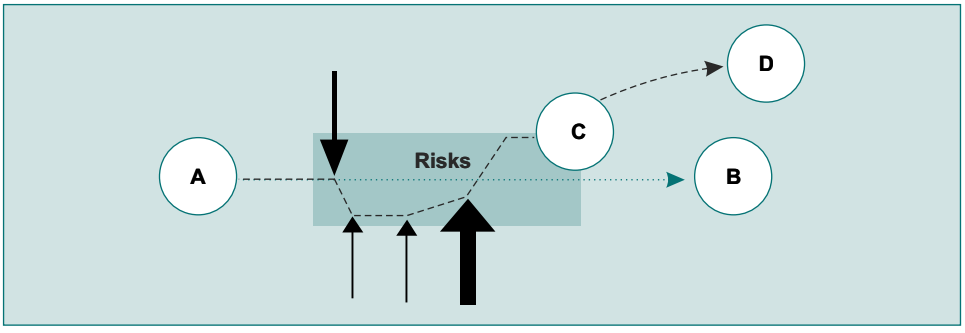



**Figure 1.3 Strategy displacement**

The effect of those risk impacts is that the strategy course A to B no longer applies. The evolution of the company has been driven off course by risk occurrences that were greater, or less, than expected when the strategy was designed. They are presumably also beyond the limits of correction that are available through the use and application of management reserve or contingencies.

In addition, new strategies may be formed within the organisation. These may serve to reinforce or deflect the original strategy.

In order to take account of these variations, most strategies allow a variance envelope. This permits divergence up to a certain limit, after which a warning is sounded. The variance envelope typically contracts as a function of time. As the company nears desired position B, the allowable margin of error must diminish, as shown in Figure 1.4.

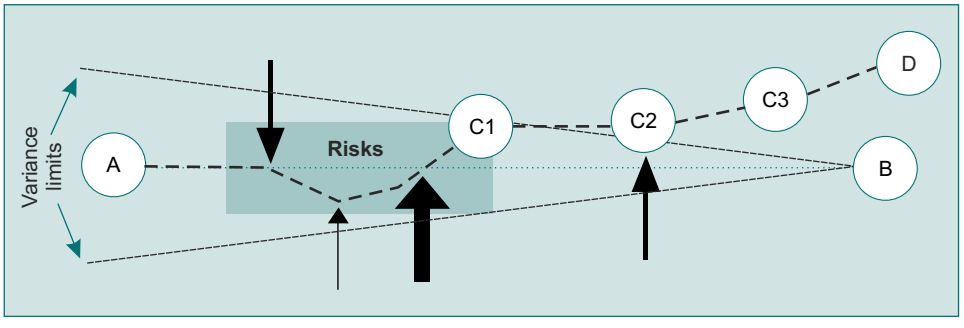



**Figure 1.4 Strategy implementation variance envelope**

In Figure 1.4 the early shifts from course are acceptable as they remain within the overall limits of acceptability for the variance envelope. The later divergences, in this case C3 and D, move outside the limits of acceptability.

Strategic risk management is concerned with the identification and management of these risks in order to ensure that the organisation finishes up within an acceptable distance of the original goal. If the implementation process is resulting in a transgression from the required course, the strategic risk management system should be able to detect this and (at least to some extent) predict the consequences. This information then acts as the basis for justifying any necessary corrective actions. The final stage is to ensure that any corrective actions are, in fact, succeeding so that an eventual successful or acceptable, or better, outcome will be achieved.

Strategic risk is considered in more detail in Module 4.

### 1.3.2 Change Risk

Change risk can operate at numerous levels within the organisation. Changes can be imposed by variations elsewhere either within or outside the organisation. Alternatively, changes can be planned and engineered by the organisation as a way to achieve objectives. An example of an imposed change would be the realised requirement to install a new production line in order to meet a sudden and unforeseen increase in demand for a product. Alternatively, if this increase in demand had been foreseen the organisation might have initiated the change itself in order to ensure that it could meet the increase in demand. Project risk operates at the programme or project levels. Most organisations evolve and develop by the use of projects, which are themselves actions for achieving change. An example of a project risk is the risk of damages becoming payable for late completion.

Change risk relates to both planned and imposed change. Planned change is necessary in order to implement strategies, whereas imposed changes arise from internal and external forces.

Internal planned change is often carried out in response to the strategic plan. If a new product is to be developed, a new production facility may have to be established. This requirement generates an operational risk. It also generates a change risk in that the current operational procedures are to be changed. In most cases the planning and implementation of the change will be treated as a project. In other words, setting up the new production system will probably be subject to time, cost and performance limits. In addition, the planning and installation of the new production system is clearly a project. In line with projects generally, the characteristics of the process are listed below.

- It is not the main process or production of the organisation.
- It has a relatively short time span.
- It has a clear start and finish.
- It is relatively complex (compared with everyday production).
- It has clear time, cost and performance objectives.
- It (probably) involves the use of multidisciplinary teams.

Assuming that the planned change can be approached as a project, the obvious way to organise the planning and implementation processes is to use project management. As a discipline, project management offers a range of tools and techniques for the management

and control of time, cost, quality and any other project objectives that may have been set. In this context, project management is sometimes referred to as a 'tool for managing change'.

Project management as a tool for managing change is developed fully in the Edinburgh Business School distance learning text *Project Management*.

Change can also be imposed by external events. In this case the change is not part of a strategy or plan; it is imposed upon the organisation, and the organisation has no choice other than to make an appropriate response. An example of an imposed change is the need to develop and release a new product in response to the actions of a competitor.

Change risk is considered in more detail in Module 5.

### 1.3.3 Operational Risk

Operational risk relates to the production process. This includes the process itself, the asset base, the people within any project teams, and the legal controls within which the organisation operates.

Operational risk can be defined as 'the risk of direct or indirect loss, resulting from inadequate or failed internal processes, people and systems or from external events'. Operational risk also effectively includes anything that can impact on the overall performance of the organisation and on the ability of the organisation to create value. Operational risk therefore includes events such as mistakes or missed opportunities.

The primary element of operational risk management is that the control, monitoring and assurance activities of the organisation should be based upon a comprehensive business risk assessment that identifies and ranks risk by their significance to the company. In determining significance, the risks must be considered first in the context of the likelihood of their occurring and second in terms of their impact. It is this latter aspect of impact that needs to be well defined. Traditional measures have focused on a financial value or the potential for injury, and, although these aspects must be considered, the main consideration is the way that risk impacts upon strategic objectives.

The process of operational risk management includes the product itself, its suitability for market demand, marketing and sales and delivery. People risks include risks associated with human resources and staff development. Legal risks include contractual issues, together with statutory obligations and liability.

Operational risk is considered in more detail in Module 6.

### 1.3.4 Unforeseeable Risk

Unforeseeable risk is the type of risk that cannot be accurately forecast before it occurs. Some risks may be reasonably anticipated, such as a change in interest rates over a five-year period. In developing a strategic plan for an organisation, it will be assumed that there will be some variation in interest rates and that this variation will be contained within reasonable limits. In the UK, under current stable conditions (2002), a planner might make the assumption that interest rates can be expected to vary by plus or minus 2 per cent over the next three years and by plus or minus 3.5 per cent over the next five years. The plan should allow for sufficient reserve to be built into the system to cover these expected variations. However, every so often there may be a sudden and unforeseeable increase in interest rates, such as in the UK in 1993 on 'Black Wednesday', when the UK government raised interest rates several times in one day in a vain attempt to try to influence the value of the pound.

Unforeseeable risks can sometimes be allowed for up to a point by the use of contingencies built into the overall plan. However, these can absorb only so much of the impact, and once they are consumed, the only option may be for a tactical response using resources from elsewhere within the system.

In any plan, there will always be an element of unforeseeable risk. It is never possible to plan for every eventuality. No matter how careful the planning process, it is virtually impossible to include every event or variable that could generate a risk. It is important that the risk manager is aware of such limitations, and ensures that adequate allowance is made so that the effects of any such unforeseeable risks can be contained.

Events such as fire, flood and subsidence are generally insurable. An organisation can set up an insurance contract with an insurer and can transfer liability for such events to the insurance company. In most cases it would be standard practice to pay a premium and retain an excess.

Such events can also be mitigated by taking appropriate precautions, such as commissioning flood defences ahead of the event.

Unforeseeable risks can also be countered, to some extent, by the establishment of reserves. A programme of works could have spare time built into it in the form of (for example) an extra 10 per cent time allowed for each activity or additional sums built into cost estimates. Most estimators allow a *reserve* or *contingency* sum, either built into each rate or as a lump sum contained as a separate amount in the estimate. At an operational level it is standard practice to include a *management reserve* over and above any operational budgets or cost limits to allow for unforeseen eventualities.

Most organisations develop some form of *business continuity plan* (BCP) as a set of procedural processes so that these can be activated in the event of a major unforeseen impact. The BCP acts as an emergency back-up so that the continuity of the business can be maintained as far as possible until the effects of the impact can be corrected. A BCP often incorporates or runs in conjunction with a *disaster recovery plan* (DRP). A DRP is designed to enable operational procedures to be re-established as quickly as possible in the event of a major impact. An example is a total IT failure, possibly caused by a failure of the central server or a disruption to the mains power supply.

Unforeseeable risk is considered in more detail in Module 7.

### 1.3.5 Financial Risk and Knowledge Risk

Financial risk and knowledge risk are examples of specific risk types as opposed to risk levels. These risks can apply at any of the four risk levels discussed above.

#### Financial Risk

Financial risk includes market, credit, capital structure and reporting risks. This particular risk heading is easily the most heavily covered in the literature on risk management. Financial risk is considered in detail in the Edinburgh Business School distance learning texts *Financial Risk Management 1* and *2*.

## Knowledge Risk

Knowledge risk includes the information that is stored using IT, hardware and software, information management, knowledge management and planning. IT is an increasingly important area for many organisations. Most modern companies could not operate without complex computer support; the risk of a major IT failure is the nightmare scenario for many large organisations. As the level of IT use increases, so organisations become more exposed to knowledge risk. Essentially this is the risk of the organisation's not being able to access crucial business information. Companies also face new and rapidly changing IT-based threats such as hacking, sabotage, malicious interference and espionage. These are all intrusions that can limit access to crucial business information.

*Note*: Knowledge risk is not the same as IT risk (see below), although knowledge risk is linked to IT risk in most modern organisations. Knowledge risk involves a disruption of access to information, whereas IT risk relates specifically to a disruption to information technology, whether knowledge based or otherwise.

Knowledge risk can also be non-IT based. In many ways the real value of an organisation lies in its people. In most successful organisations there are a relatively small number of very important people. These people fulfil key roles and functions, and are essential for the continuing success of the enterprise. They carry a combination of natural ability and acquired specific knowledge about the organisation. In most cases, the knowledge base of these individuals is not written down or formally recorded in any way. If the person is lost the chances are that his or her knowledge goes too. This lack of knowledge transfer is often a major problem when a key person leaves the organisation for whatever reason. This effect is often encountered immediately after an acquisition. The statistics show that key people in an acquired company often leave the parent company within a relatively short period of the acquisition being completed. Typical reasons include:

- disillusionment;
- resentment;
- loss of power and/or authority;
- loss of motivation and commitment;
- inability or unwillingness to adapt.

The loss of key people knowledge can be a significant consideration. In many acquisitions the value of the acquired company is often considered in terms of the stocks and assets of the company. The due diligence analysis is usually restricted to a straightforward evaluation of the assets of the company. Individual knowledge is generally not taken into account in the calculations. However, depending on circumstances, a considerable part of the value of an acquired company is attributable to the key people who ensure that it operates successfully. This value might not show up on the balance sheet but it is essential in terms of the organisation's ability to add value. If some or all of the key people leave after the acquisition, the true value of the acquisition could be diminished. As discussed above, post-acquisition migration is a common phenomenon, and the consequences for the success of the acquisition are often not adequately addressed.

## 1.3.6 External and Internal Risks

Within the framework of risk levels there are two obvious further elements of classification depending on the origin of the risk.

*Internal risks* originate within the organisation, whereas *external risks* originate from the environment. Internal risks are to some extent calculable and controllable. External risks may be calculable but they are generally outside the control of the organisation. An obvious internal risk is that of an employee acting fraudulently. The risk emanates purely from within the organisation, and there is no direct external involvement. An external risk may be created by fluctuations in the general level of economic activity. Stock market conditions can be influenced by relatively unforeseeable external risks such as the sudden demise or bankruptcy of large organisations (for example Enron and WorldCom in 2002).

An example of an *external strategic* risk is the risk resulting from the emergence of a new major competitor into the same market, such as Microsoft entering the computer games market with the X-box console in 2001. Microsoft is such a big player that its emergence must affect the strategic planning and response of existing major players such as Sony. An example of an *external change or project* risk would be unforeseen ground conditions affecting the completion date of a new civil engineering project, as happened with the Humber bridge in the UK in the 1970s.

Some examples of external and internal risks are considered below.

### External Risk

External risks take numerous forms. They impinge upon the organisation and present a risk to the organisation that then has to be assessed and (if necessary) addressed. Some examples are discussed below.

- **Interest rate risk** Interest rate risk is a form of financial risk. This type of risk is evident where changes in interest rates directly affect the value of assets and liabilities on the company balance sheet and also off-sheet items such as derivatives. The value of items of plant or equipment can be expressed in terms of the discounted net present value (NPV) of all the future cash incomes that will be generated by that machine. Interest rates are integral to the NPV calculation. If interest rates rise, the value of the machine goes down. Interest rates are controlled by national banks or by government, and are outside the control of individual organisations.

- **Volatility risk** Volatility risk affects items where the volatility of an underlying risk factor changes and this directly affects items within the organisation's portfolio. In the case of purchased options, a decline in volatility means that there is less chance of the option expiring profitably. For written options volatility works the other way round, and lower volatility increases the risk of a profitable expiry.

- **Convexity risk** Convexity risk is a market risk that is closely related to interest rate risk. This relates to items such as bonds, where the value drops in inverse proportion to rises in interest rates but not as a linear inverse proportionality. Generally, the amount of the bond price change depends on the level of interest rate change. Large changes in interest rates can lead to very large variations in bond prices.

- **Time-dependent risk** Time-dependent risk relates to items where there is a fixed time limit for something to happen. A typical example is an insurance policy. An organisation may take out insurance cover for a specific amount of time and for which agreed premiums are payable. If the organisation does not claim on the insurance policy within the timescale for expiry, the result is a net loss to the organisation. Each day that passes leaves one less day for the policy to be activated and therefore add value to the organisation.

- **Competitor risk** There is always a risk of changes in the competition base. Such changes could be major or minor but they will all impact to some extent on the organisation. New competitors can suddenly appear in established markets. Alternatively, established competitors can suddenly decline because of single catastrophic events or because of a longer-term inability to respond to changes in the market.
  Competitor risk includes more subtle changes in what the competition does, such as making changes to an established product or other forms of innovation and development. For example, a university might find that its student numbers suddenly decline because a competing university has introduced some kind of grant support funding. Students may migrate to the competing university not as a result of that university offering better courses but simply because the competing university is offering something else that is attractive to students (money).
  Changes in competitor profile and behaviour are one type of impact that can seriously affect strategy implementation. A major change can invalidate an existing strategy and generate a need for a significant change or shift in direction.

- **Customer demand risk** The demands of the customer base change and develop rapidly. This applies more in some markets than in others. The demand characteristics of customers for carpets tends to be more or less static. Carpets today are made using more or less the same materials and processes that were used ten years ago. In other industries market demand can change very quickly. Popular music is one example. The Spice Girls were all conquering in the EU and US popular music sectors in the mid-1990s. In some ways they were held up as popular icons for girls throughout the West and, to some extent, in Japan and the Far East. However, tastes changed, and their fall from prominence was sudden and rapid. The Spice Girls' music was still the same, but the notoriously fickle and changeable popular music demand shifted suddenly and irrevocably.
  Some sectors are affected by a market demand that expects constant change. An example is the home PC market. People have come to expect to see PC design and capacity changing almost constantly. There is a demand for ever more powerful and flexible machines that can run the latest software, and people expect the system to be able to handle new and complex peripherals. This expectation for constant innovation and change was, to some extent, caused by the PC manufacturers themselves in the early late 1980s, when the popularity of home PCs started to take off. The manufacturers spent a lot of money investing in research and development in what was then a new industry. The only way they could cover these research and development costs was by constantly upgrading and modifying their systems so that people would keep buying the latest versions. The idea of constant changes stuck, and it is now very much a standard perception within the customer base.

- **Exposure risk** All companies are exposed to different levels of risk, and different risks will affect them in different ways. The risk profile is a measure of an organisation's exposure to risk. Factors such as borrowing and gearing ratio will affect the firm's exposure and its ability to survive changes in the environment such as interest rate changes. Some organisations can be particularly exposed in some areas and not in others. A company making lawnmowers is exposed to the risk of a bad summer. If it rains, a lot of people will not do much gardening and they will wait until next year to buy a new lawnmower. The lawnmower manufacturer's risk profile includes the risk of poor weather. This same risk would not appear on the risk profile of an automobile manufacturer, from whom production and demand are more or less unaffected by the weather.
  Exposure risk is particularly important where an organisation relies upon a small number of variables or even on a single variable. The classical example is the exposure of oil producers to world oil prices.

- **Shareholder risk** A firm that depends on equity has to keep the shareholders happy. If shareholder confidence declines, the effects on the company can be significant. In particular, they can affect the company's ability to raise capital. Shareholder confidence and willingness to retain shares can be affected by a wide range of internal and external variables. An example of this type of behaviour is the performance of Railtrack shares between 1997 and 2001. Railtrack was the national railway infrastructure provider in the UK. It was responsible for all the track, signals and associated engineering works. There was a series of high-profile rail crashes through the mid to late 1990s, with the worst being at Ladbroke Grove in October 1999, in which 31 people were killed and over 400 injured. The crash was caused by the driver of a local service proceeding past a red (danger) signal. In doing so, he took his train directly into the path of an oncoming express. The impact derailed both trains and started a fire. Railtrack received a considerable proportion of the blame, as the signal that was passed was considered to be partially obstructed and unclear. There was bad publicity in the media, and Railtrack's image suffered a severe setback. Ordinary share prices were already falling, having peaked at £17.68 in August 1998. By August 2000 shares were down to under £10.00, and by August 2001 they were down to £3.00. The ordinary share price performance has seriously affected the value of the company, and was outside Railtrack's control. This is an example of a company failing to manage its operational risks, so that its reputation suffered, leading to a collapse in investor confidence.

- **Political risk** The government of the home country and of relevant neighbouring countries where the company has expanded can represent a major risk. Government fiscal policy and the consequent performance of the economy can make the difference between success and failure in a new venture. An example of this is the decision of the UK government not to enter the European exchange rate mechanism and not to join the euro. Most other countries in the EU have elected to join the single currency, but the UK and some other EU members have remained outside. This situation has resulted in difficulties for some UK manufacturing companies, as the value of the pound against the euro has remained high and has made it difficult for UK exporters to compete with some other European countries.

- **Legislative risk** Governments constantly change existing statutes and introduce new ones, and companies take on legally binding duties when they sign contracts. Some statutory requirements, such as environmental legislation, impose a direct charge on organisations for consuming energy or using environmentally damaging practices such as making use of landfill waste sites. In the UK, local authorities have to pay a *landfill tax* for every tonne of refuse that they dispose of in landfill sites. Other statutes impose indirect costs through the need to comply. An example is the increased overhead cost of complying with the ever-increasing quantity of health and safety legislation.

## Internal Risk

There are many possible internal risks. These are the risks that originate from within the organisation and over which, at least in theory, the organisation should have some degree of control. Some examples are listed below.

- **Operational process risk** Operational process risk includes issues such as human resources risk, staff availability risk and capacity limit risk. An organisation might have a particularly efficient set of marketing and salespeople, or there may be a sudden market-driven increase in demand for the product. If this has not been foreseen and planned for, the organisation could quickly reach its capacity limit and become unable to meet demand, resulting in the opportunity being lost and perhaps in the loss of business to rival organisations. The UK lawn tennis championships are held every year at Wimbledon in London. The current centre court has seating for about 10 000 people. Every year the club receives around 100 000 applications with payment for seats at the final. The club allocates these on a lottery basis and returns the applications that were not successful to the disappointed applicants. The ground is at its capacity limit. Even though it could sell ten times as many tickets as it actually does, it is unable to do so as it does not have the necessary seating.

- **Legal risk** Legal risk includes errors arising from contracts or insurance policies that provide levels of protection and liability that are different from the levels perceived. The most dangerous type occurs where the organisation has a contract that it believes to be enforceable when, in fact, it is not enforceable. Typical reasons for this may be the insolvency of subcontractors or sudden changes in statute. An example is the celebrated UK case of the London Borough of Hammersmith. In 1981 the Borough had for years been negotiating and executing 'swap' deals with major UK banks. The UK upper house decided that local authorities in fact had no capacity to enter into swap transactions and the contracts were therefore *ultra vires*. This ruling had a major impact at the time, as it affected nearly 150 other councils running swap deals with 75 major banks. The total losses to the counter parties as a result of the ruling were in the region of £1 billion.

- **Liquidity risk** Liquidity risk is one specific type of financial risk that can arise from the organisation's own activities. It is the risk that cash income and current balance totals are insufficient to cover cash outgoings. This can sometimes lead to a requirement to liquidate assets in order to generate cash, a process both costly and damaging. Most large organisations have liquidity plans and liquidity contingencies in place to counter this risk. Market liquidity risk is a specific type of liquidity risk. This relates to the risk that changes in the market will make it difficult to liquidate losing transactions (transactions that are clearly going to lose money).

- **Supply chain risk** The supply chain is the chain that connects the firm's inputs through the production and operational processes to the organisations's outputs. Supply chains can be highly complex and interrelated, and a problem in one part may lead to far-reaching consequences in other parts of the chain. Typically, the more efficient the supply chain, the higher the degree of dependence that the purchasing organisation has upon it. The two main risks that affect the purchasing company are *supplier production continuity* (the risk of breaks in supplier production) and *supplier reliability* (the risk that components purchased from suppliers may have quality problems).

- **Competence risk** Employee and management competence represents a significant risk to an organisation. Poor leadership can lead to losses in production and reduced staff morale. Poor communication can lead to misunderstandings and errors. Failure to modernise and move with the times is another common risk associated with poor management. Poor workmanship or competence has led to the downfall of many organisations that developed a reputation for their products or failures. An example is the demise of the UK automobile manufacturer *British Leyland* through the 1970s. A more recent example of failed management has been the UK retail chain Marks and Spencer. This company has, for many years, acted as a cornerstone of the UK retail trade. There is a Marks and Spencer on every high street in every city in the UK, and there used to be a number of stores in prominent locations in France and Germany. The company was doing very well up to 1998, with a good reputation for high-quality women's clothes and food. However, levels of competition changed, and the senior management levels within the company did not reorganise their strategy quickly enough. The public perception of the company changed very quickly, and UK retail profits fell from £872 million in 1998 to £420 million in 2000. Over the same period, the ordinary share price fell from £5.30 to £1.70.
  The figures for the downfall of Marks and Spencer are spectacular, to say the least. They occurred because the people in charge allowed things to stay the same, thinking that would be enough. Based on past performance this was, to some extent, true. The fate of Marks and Spencer lies with the current management team. The company is now going through a European reorganisation in an effort to re-establish its previous public image.
  *Note*: The fortunes of Marks and Spencer improved significantly during the latter half of 2001 and throughout 2002. Senior management realised that the chain had problems and implemented effective corrective measures. The mainland Europe outlets were still lost, but fortunes in the UK improved significantly.

- **Complexity risk** Complexity risk is very much a phenomenon of modern electronic systems. Some systems have been developed to a stage of complexity where it makes the system very difficult to understand and interpret quickly. An example of this was the shooting down of Iranian Airlines flight 655 on 3 July 1988. The missile control officer on board the *Aegis* radar cruiser USS *Vincennes* mistook the airliner contact for an enemy fighter and ordered that a surface-to-air missile be fired at it. The airliner was hit, and everybody on board was killed. The *Vincennes* captain later complained that the system was so complex that it was difficult to use under battle conditions. In addition, it did not filter useful information from irrelevant information, and consequently quick and accurate interpretation was very difficult.

- **IT and technology risk** Information technology (IT) and other forms of technology provide increasingly important internal risk. Modern organisations are generally very reliant on IT, and a significant proportion of organisations cannot function effectively without it. This internal dependence creates a significant risk to the organisation if the system fails or changes have to be made. Modern banks use computers for virtually all aspects of their operations. Even at branch level all transactions are entered onto the central computer, even if some paperwork such as receipts and paying-in slips still exists. If the main system goes down for any reason, the tellers have no way of executing a transaction. Even the money dispensers and cash machines rely on the same system and cannot function without it. This level of reliance would have been unthinkable only 20 years ago.

  IT also opens up the risk of IT fraud and deception. This can also be an external risk. Modern computer networks and mail servers are relatively secure; programmers and systems managers try to put as many security checks and controls in the system as possible. However, an internal 'mole' who really understands the system can often reach higher levels within the system than he or she is authorised to go to. In UK universities it is common for internal student 'hackers' to break into the payroll programs, or to leave obscenities and other unsavoury material in the files of unpopular lecturers.

  The risk associated with IT and its software can also manifest itself when organisations are trying to expand or develop their systems. At this time, many companies find that they have old legacy systems that are not compatible with modern hardware and software. Worse still, they will often find that their main operational functions are based on such systems. They are therefore left with the option of completely replacing their IT set-up or of running an old system and a new one. There are obviously significant risks associated with the selection of either option.

  Typical reasons for IT systems failure are:
  - power failure;
  - defective hardware;
  - defective software;
  - infection by malicious virus;
  - lack of back-up and stand-by provision;
  - absence of key IT support staff;
  - internal malicious damage;
  - use of outdated protection systems.

  The effects could be:
  - loss of system records;
  - interruption in operational capability;
  - delays in making or receiving payments;
  - interruption of web page;
  - loss of orders;
  - loss of future work because of the interruption;
  - loss of reputation;
  - requirement to purchase replacement equipment;
  - requirement to re-train staff;
  - disruption of related services.

  The significance of these effects tends to increase as organisations become increasingly reliant upon their IT support functions.

- **People risk** This type of risk relates particularly to individuals within the organisation who leave, and take specialist knowledge or contacts with them. Senior people who have developed detailed operational knowledge over years can be very difficult to replace. Alternatively a sales manager may have all the necessary contacts for customers, whose orders are critical to the future success of an organisation. In addition, there is always the risk that they will take their expertise to a rival and attempt to use it there. This can often be avoided by consideration of some kind of covenant on intellectual property rights or approaching customers. The effects of the person leaving can be controlled by the maintenance of accurate records and the establishment of proper *succession planning*.
  *Note*: People risk is linked to knowledge risk (see above) in that key people might leave and take their knowledge with them. People risk, however, can result from the loss of information (for example business contacts) as well as a loss of knowledge (for example how to manage a part of the business effectively).

- **Residual risk** Residual risk is the risk that remains after whatever levels of risk treatment and response have been carried out. It will be recalled that it is not generally possible to eradicate all risk, nor is it desirable to attempt to do so. From a cost point of view alone it is rarely practical to try to achieve a risk-free state. Achieving zero risk in most situations is prohibitively expensive. Most organisations will aim for a level of residual risk offering the best compromise between cost increase and risk reduction. Levels of residual risk may be very low such as in the case of aero engine components. These have to be manufactured to the highest standards and are consequently very expensive. They are still not 100 per cent perfect but they are almost so. In other cases residual risk can be relatively high. An example is cigarette design. The characteristics such as nicotine content and tar levels are, to some extent, regulated by government. The companies themselves impose some risk control, such as the inclusion of a filter. However, the finished product still represents a considerable risk to health, and manufacturers have to print warnings to this effect on the packets. The existence of government health warnings is evidence of a significant level of residual health risk in a finished product.
  Such practices also involve a residual risk for the manufacturer. In the US there have been a number of high-profile litigation cases where smokers have been successful in claiming compensation from the large cigarette manufacturers on the grounds that they knowingly manufacture and sell products that are harmful. Although such cases, and the case law to which they contribute, are still very much in their infancy, there is growing evidence to suggest that the large cigarette manufacturers are at risk from further large compensation claims in the future.

## 1.3.7 Speculative and Static Risks

A further classification that is often encountered relates to the nature of the risk. Risks can be either speculative or static.

*A speculative risk* is one that can lead to gain or loss. The net outcome can be either positive or negative. A *static risk* is one that can only result in a net loss.

A gambler puts forward a stake in the hope of winning more money. A bet on a horse is a speculative risk as it can lead to a net gain (if the horse wins) or a net loss (if it loses). A fire in a building is a static (or pure) risk as it can only lead to a net loss. This risk can be mitigated by the use of fire prevention measures, and can perhaps be transferred by the use of a fire insurance policy. However, if a fire does occur it can only result in a net loss as the

insured organisation will have to pay the insurance premium plus any excess and will have to bear the cost of lost production and disruption.

Buying shares in an external company therefore represents an external speculative risk. The performance of the shares depends on wholly external factors, and the value of the shares can either increase or decrease over time. To extend the classification further, a life assurance company that decides to invest its funds purely in company shares is taking a *strategic internal speculative risk*.

A large-scale internal reorganisation is another example of a *strategic internal speculative risk*. The reorganisation could be successful or it could be unsuccessful. The value of the internal reorganisation to the company covered could be positive or negative. The reorganisation could also constitute an *operational risk* in that the temporary disruption caused by the reorganisation could interrupt productivity. In addition, the reorganisation itself involves a degree of *change* and will probably be carried out as a *project*. The reorganisation therefore also constitutes a *change risk*. One event or action can result in the generation of a series of different risks that impact at different levels within the organisation.

It is important to appreciate as early as possible that the various risk types are linked. An event that is precipitated by external forces may generate risks at different levels. An event that generates a change risk can also generate an operational risk. The change in operational risk can, in turn, generate a new strategic risk. The various risk types and levels cannot be considered in isolation. This is the concept of risk interdependency, which will be discussed in more detail in Module 8.

Some examples of speculative and static risks are considered below.

## Speculative Risk

Speculative risk is dynamic. It is concerned with both positive and negative values, or with potential gains and losses to the organisation. Speculative risk is concerned primarily with the risk to all the stakeholders within the company, whereas speculative financial risk is restricted to equity holders. Speculative risks can change over time and can shift between likely positive and negative values.

Speculative risk is measured by changes and variations in the general market place. It is unavoidable, as it relates to factors that are outside the control of the decision maker, and it could result in positive or negative impacts. Speculative risk therefore provides the organisation with the potential for profit and loss on trading. Obvious examples would include:

- share flotations;
- competitor activities;
- investment in research and development;
- release of new products;
- general economic activity.

In addition, speculative risk can be split into two primary components. These are *business risk* and *financial risk*.

- **Speculative business risk** Speculative business risk (SBR) arises from the company trading with its assets. SBR is a risk to the company as a whole and is therefore distributed among the shareholders, creditors, employees and all other stakeholders.

- **Speculative financial risk** Speculative financial risk (SFR) arises from the gearing ratio, which is a measure of the financing of the organisation. SFR is the risk of the annual dividend falling to zero, so that equity holders make no return on their share holdings.

### Static Risk

Static risk considers losses only. It looks at potential losses and seeks to implement safeguards and protection in order to minimise the extent of the loss. The obvious example is an insurance policy. Like market risks, static risks can change over time, and the level of protection provided by countermeasures can also vary.

Static risk refers to risks that only provide the potential for losses. Considerations of specific risk are therefore generally concerned with making sure that the company performs at a given level. It is most concerned with making sure that losses or problems are minimised. Obvious examples would include:

- fire insurance;
- third party and public liability (consequential loss) insurance;
- tortious liability (professional indemnity) insurance;
- personnel insurance;
- other optional forms.

Clearly, static risk can be reduced and controlled to some extent. However, market risk will always remain. One of the components of portfolio theory holds that risk takers cannot expect to gain reward for taking risks that can be avoided. Reward can be expected only from taking speculative risks. In other words, an efficient market will not offer reward for static risks. The best strategy therefore, if appropriate, is to diversify. The organisation can reduce the effects of static risks by insuring against them (where relevant) and by diversifying. Acquisitions and mergers provide a means of allowing the organisation to evolve into new areas. By expanding the range of new areas within the organisation, the organisation spreads the static risk and makes the system more resilient against market risk shocks, such as a sudden change in statute or in government fiscal policy.

Speculative and static risk types overlap with the generic headings discussed earlier. Opening a new production line would be an example of a *strategic speculative risk*. A company's all risks insurance policy to cover injury to persons and property would be an example of an *operational static risk*.

## 1.3.8 The Concept of Risk Interdependency

The various risk types discussed above do not exist in isolation. In practice there are interrelationships between them. In developing a strategic plan an organisation identifies the strategic risks that could affect implementation. However, there are also inherent change risks associated with the implementation of the strategy. These risks could originate from internal changes necessary for the implementation of the strategy and from external changes impacting on the implementation of the strategy. The implementation of the strategy itself may require internal operational changes. These changes generate change risks that in turn can generate operational risks. Impacting risks from outside the organisation can generate forces that can affect all risk levels within the organisation.

It is important to appreciate that all the various types of risk are interconnected, and a variation in one type can impact on the various other types. This concept of risk interdependency is discussed in more detail in Module 8.

## Time Out

### Think about it: Risk interdependency

*Background*

By July 2002 the French media giant Vivendi was worth about 15 per cent of what it was worth in July 2001. Share values dropped from $120 to $20. During the same period, debt rose steeply. The poor performance of the company over this two-year period led to the dismissal of the company's controversial top person, Mr Jean-Marie Messier. The main reasons were financial, and were very much related to a complex interdependency of different levels of risk.

Mr Messier was originally seen as a visionary business leader. He transformed what was originally a French sewage utility into a global telecommunications and media giant. At one point Vivendi was ranked second only to AOL Time Warner. Starting in 1995 Mr Messier led an aggressive and highly successful series of high-profile acquisitions including MP3.com (an on-line music company), Canal Plus (TV and films) and Houghton Mifflin (educational publishing). These acquisitions were followed by the subsequent acquisitions of Universal Music Group and Universal Studios. During this acquisitions period Vivendi's stock more than doubled, and reached a level of nearly $300 per share in mid-1999. Vivendi also launched a series of high technology new ventures. Vizzavi was launched in 1999.

*So what went wrong?*

Operationally, Mr Messier made a number of enemies within the French business community. He was widely regarded as being somewhat brash and arrogant. In addition, he developed and used a very American-style attitude to business and, for both political and cultural reason, this generated a certain resentment among other French business leaders.

The original strategic vision was to acquire successful companies in both established and new high technology areas such as dot.com companies and mobile telephones. The strategy was very much aligned towards the rapidly expanding dot.com sector. This sector underwent a rapid and relatively unforeseeable decline between 1997 and 2000, and to some extent Vivendi's fortunes went with it.

In some ways Vivendi made the same mistake as the UK company Marconi. Both companies moved from areas where they had an established success base into areas where there was current rapid growth. They developed strategies to included this transition because they thought that the acquisitions would secure a market share in new and high potential sectors. The relatively established players in these new fields were already uneasy about future prospects. Several large telecommunications companies were already concerned as early as 1997, but Vivendi, as a new player, was less experienced and less able to see the initial warning signs.

As the high-tech sector moved into decline, Vivendi was left with a number of companies worth only a small proportion of what Vivendi had paid for them. In addition, Vivendi was burdened with a large debt. The result was a loss of nearly €14 billion in 2001.

The situation deteriorated still further in July 2002 when allegations about the company's accounting practices were made public. On 1 July 2002 the French newspaper *Le Monde* printed allegations that the company had used questionable accounting practices.

The allegations were based on the assertion that Vivendi had tried to add €1.5 billion to its accounts for 2001 as part of a complicated and involved transaction with BSkyB. *Le Monde* suggested that the move had been blocked by French regulators. In many ways this development could not have occurred at a worse time for the company as there had been a series of recent exposures of financial irregularities in the US involving companies such as Enron, WorldCom and Xerox.

Enron and WorldCom both used the accounting firm Anderson. Anderson also acted as advisor to Vivendi.

*So where does Vivendi go from here?*

By 2002 some analysts were saying that Vivendi might actually be worth more if it were to be split up into separate companies again. There were also some signs that American investors might be prepared to buy back the US parts of the company. Such buy-backs would incur a significant overall loss but would at least go some way towards reducing the debt mountain faced by the company. This would give the company some time and much needed room for manoeuvre.

*Risk interdependency*

Vivendi's fortunes provide an example of the interdependency between the various risks that it faced. The primary strategic risks related to moving from one sector to another. The move looked good at the time, but it was very much subject to external change risk. Incurring a large debt to acquire high-tech companies meant that Vivendi was exposed to any negative change in the high-tech sector. In addition, the debt burden directly affected the operational approaches used by the various acquired companies. In addition, the operational specialisations of the various companies within the group led to a lack of synergy. The various specialisations were to some extent just too far apart for them to be able to complement each other.

The strategic risk in moving across sectors was compounded by the operational risk in trying to incorporate differing operational styles within one organisation. The whole assembly was particularly sensitive to any change risk arising from variations in the performance of the telecommunications sector. The relatively unforeseeable high-tech decline of the late 1990s imposed a direct change risk on the adopted strategy.

Another company with less high-tech exposure might have been able to respond more effectively. The most recent development of accounting irregularities has exacerbated the situation still further. Accounting irregularities represent an operational risk. The exposure of the practice has impacted the already considerable strategic risk faced by the organisation. The urgent necessity to raise cash has placed the company in a position where it will almost certainly have to sell off some of its assets and make large-scale cost reductions. These actions, together with the consequent reorganisations that will be necessary, represent change risk that could have a direct influence on operational capability.

***Questions:***

- What was the relationship between strategic and change risk?
- How could the company have made better provision against the change risk presented by the changing high-tech sector?

## 1.3.9 Summary

This section has considered a limited number of internal and external risk types. The list as given is not intended to be exhaustive, and it should be apparent that a business observer can probably see risk in every activity in which the business is involved, particularly where there is external or internal reliance on a particular asset, resource or assumption. The list is intended to develop an overview of some of the risks that can affect an organisation. The most important single factor is that the risk types are interdependent. This factor cannot be over-emphasised as it is of crucial importance and (more important still) it is ignored by most types of conventional silo-based risk management systems, i.e. where departments in an organisation operate as separate entities.

### Time Out

**Think about it: Risk types**

Organisations face a range of risk types. The overall risk profile can contain a complex and dynamic range of risk types, which are interrelated and which vary as a function of time. In addition there are overlaps between some of the risk types. A scope risk is also a management risk. A decision on which parts of the organisation to insure and which not to insure is a scope risk decision and is also clearly a management decision. In turn, the consequences of this decision could indeed be considered as a direct financial risk. There are both multiple and discrete interrelationships between numerous risk types in most complex risk assessment processes.

The significance of different combinations of risk types can be very different. On Monday 17 September 2001 the Dow Jones index fell 7 per cent. This was an all-time record in terms of the number of points lost on the Dow Jones Industrial Average, which is the main blue chip index in New York, although there was a larger percentage drop (22.6 per cent) on 19 October 1987. The fall was caused by the World Trade Center terrorist (political risk) attack (the attack being an external risk as far as Dow Jones companies were concerned). There were large sales (shareholder risk) in companies directly affected such as leisure, tourism, airlines and hotels (specialisation risk), although shares in defence and weapons such as Sturm Ruger (handguns) went up significantly in value.

These losses occurred despite the US Government Federal reserve (the Fed) dropping interest rates to the lowest levels since the 1960s (interest rate risk).

Not all of the overall losses were directly attributable to the attacks, nor were they regarded as truly representative. The Dow Jones represents only 30 stocks, all of which are 'old economy' companies. The corresponding fall on Nasdaq, which represents newer high-tech companies (IT and technology risk) was considerably smaller. In addition, many analysts reflected that Wall Street was only coming into line with Europe and the Far East, where average values fell by some 10 per cent over the six days that the New York Stock Exchange was closed (complexity risk).

Hopefully it can be seen that the risk influences on individual companies are complex and interrelated, and change dynamically over time.

***Questions:***

- Given the range of risks that can impact on an organisation, and the complexity of the linkages between these risks, what are the primary performance characteristics of an appropriate organisation-wide risk management system?

## 1.4 The Concept of Risk Classification

Risk classification is discussed in more detail as part of the general risk management process in Module 3.

Having established that decision makers consider risk and reward in terms of the range of outcomes that are acceptable, the next point to consider is how to classify risk. Organisations face a multitude of risks, and some risks are more dangerous than others and therefore merit greater care and attention. The idea of a risk classification system is that it allows risks to be appraised and described in some way that indicates their relative importance.

*Risk-dependent reward* can be classified simply in terms of its magnitude. The range of acceptable outcomes in decision making can be defined by the resources that are available to the decision maker and also by the strength or robustness of the system to take and absorb varying degrees of 'hits'. Risk is more complex as it depends on a number of variables. If a person is driving a car from A to B, he or she will be faced with a number of decisions that have to be made. One of these decisions might be whether or not to overtake a slow-moving vehicle on a windy road. In making the decision to overtake, a number of risks arise. One example is that an oncoming vehicle might suddenly appear travelling at high speed, giving the driver insufficient time to react and avoid an impact. This situation could result in a catastrophic collision. The likelihood of this occurring is a function of the driver's speed, the oncoming vehicle's speed, and the length of clear road that the driver can see before the next bend. The decision on whether to overtake will be influenced by all these factors, together with the driver's experience and his or her appetite for risk.

Given that the result of the risk occurring is very serious (a catastrophic collision), the driver will presumably accept this risk only if he or she can see well ahead and therefore be sure that there is sufficient time to complete the overtaking manoeuvre before the next bend. The same driver might be prepared to accept a lower probability of success if the consequences are less severe. An example of this is a puncture in a self-sealing tyre. A driver might be prepared to drive over road debris at a relatively high speed if he or she knows the automobile is fitted with self-sealing tyres. The driver knows that in the event of a puncture the tyre affected will seal itself, and there will be no risk of a 'blow-out'. The same driver would probably slow down if faced with the same road debris with non-self-sealing tyres fitted. In both cases the probability of suffering a puncture is the same. The impact of a puncture is quite different, depending on the self-sealing properties of the tyres.

Risk can therefore be measured or classified in terms of likelihood and consequence. In terms of classifying risk there is a functional relationship between likelihood and consequence. This relationship is sometimes referred to to as the *first-level equation for risk*:

- $\text{Risk} = f(\text{event}, \text{likelihood}, \text{impact})$

Two different events might therefore carry the same risk even though they feature quite different characteristics. For example, the likelihood of a radiation leak in a nuclear reactor cooling circuit resulting from a mechanical failure or leak might be very low because of all the monitoring and control systems that will inevitably be in place. However, the consequences or impact of such a leak could be very significant. The possibility of human error may be a great deal more likely, but the control systems will again make sure that the degree to which human operators can override the automatic control systems is limited. The overall risk of the mechanical failure and human error may be the same, although the likelihood of occurrence and maximum possible impact are very different.

Risk can be amplified in such situations. It may be possible for human operators to override more of the automatic monitoring and control systems than is safely acceptable. The probability of human error can then remain high while the impact also increases beyond the limit for what should be an acceptable outcome for the range of human-possible actions. This is exactly what happened at No 2 reactor at Chernobyl in the Ukraine in 1986. Human operators overrode important coolant circuit temperature control systems. They decided to shut down the primary cooling circuits and see how long the reactor could keep running. The result was a powerful explosion caused by rapid coolant steam expansion in the main reactor.

The first-level equation for risk relates the likelihood of an event occurring and the consequences of that event occurring. However, there could be some considerations where it is virtually impossible to identify a probability of an event occurring. At Chernobyl, the designers of the system had looked at all possible failure routes and designed their systems to be able to handle them (although one could argue that the absence of a reinforced concrete containment vessel around the reactor was somewhat risky!). Where the range of possible likelihood values cannot be accurately calculated, or even effectively considered, risk may be examined in terms of overall hazard rather than likelihood. This approach is common in weapons systems design, where it is virtually impossible to calculate the likelihood of a particular offensive weapon being used against the system.

The designer of a combat helicopter has to consider how much armour and how many duplicate systems to include in the design. The more armour that is included, the heavier the machine becomes and the lower the range, flight time and therefore effectiveness. The trade-off between armour and operational effectiveness depends on the extent to which the aircraft is likely to be hit while in combat. This assessment is almost impossible to make because it depends on so many variables. It is therefore sometimes prudent to consider risk in terms of the *second-level equation for risk*:

- $\text{Risk} = f(\text{event}, \text{hazard}, \text{safeguard})$

In this consideration, something or the lack of something causes a risky situation. The source of danger is a *hazard* and the mitigation or defence against the hazard is the *safeguard*. The risk of the helicopter being shot down is therefore a function of the hazard (such as loss of hydraulic power) and the safeguard (armour plate and duplicate hydraulic systems). The hazard-control equation is a measure of how dangerous something is in relation to the controls needed to control that item, or at least to reduce its impact to a level within the range of acceptable outcomes (the helicopter can stay in the air). When considered in this context, we describe the risk as residual to reflect the reduction in absolute risk that has been attained through the control. No matter what safeguards are put in place, there will always be an element of residual risk remaining. Generally, the lower the level of residual risk that is required, the higher will be the cost of achieving it.

The classification process identifies the importance of the risk. It highlights those risks that are critical and those that can perhaps be left alone for a while. This identification and rating can be based on likelihood and impact or on control and hazard. The classification and rating of risks can sometimes be done by the use of a simple risk assessment, as shown in Figure 1.5.

Figure 1.5 shows the likelihood of occurrence of a risk against the impact in terms of whatever success criteria (for example time or cost) apply for the project. Whether the

severity of impact of the risk or the likelihood of the risk occurring at all is high or low is a matter for the judgement of the risk takers, based upon their knowledge, experience and attitude to risk.

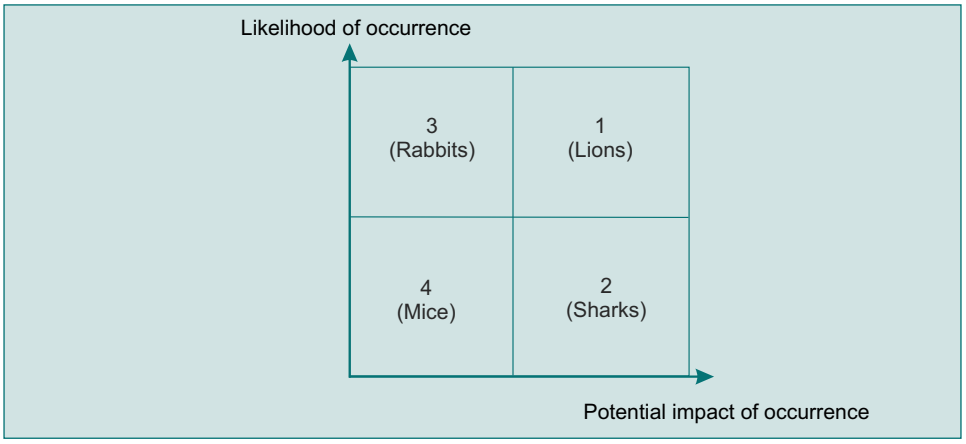



**Figure 1.5 Probability against impact of risk**

In simplistic terms, risks can categorised using analogies with the characteristics of various animals. Some animals (such as lions) are dangerous all the time if a person lives near to them. They are a clear and present danger. If someone walks near a lion there is a high probability (likelihood) that it will attack, and the consequences (impact) will be considerable. Lions are high impact because they can eat a human. They are also high likelihood because they also live on land (provided the risk taker lives in a country where lions also live). A 'lion' risk in a company context would be a key director in a recently acquired company. There is a significant probability (depending on circumstances) that he or she will leave the parent company within a short time of the acquisition. If he or she does so, there may be a considerable impact on the acquired sections. The acquiring company should take urgent measures to ensure that such an event is adequately covered. To ignore the risk involved is to invite disaster.

Sharks are *potentially* dangerous. They can cause much the same impact as lions, but they can attack only if a person is in their own environment (the sea). The impact of a shark attack is probably as great as that of a lion attack, but the probability of impact is lower as the shark lives in a different environment from people (unless of course a person chooses to go swimming in a shark-infested pool!) A 'shark' risk in a company context would be one of the key directors in the parent company leaving. Provided he or she is adequately catered for there is a low probability of this happening. However, if it does happen, the impact could be considerable. The parent company might consider appointing a deputy and/or taking out appropriate key-person insurance.

Rabbits are common but do not do much damage unless they are allowed to multiply uncontrolled. It is very likely that a person will see rabbits, but they are not likely to attack him or her. However, they might cause damage to crops if there are enough of them. In other words the impact of rabbits may increase if they are uncontrolled. A reasonable number of rabbits will maintain their classification risk of zone 3 in Figure 1.5. However, if they breed without control, the rabbit risk classification could increase to zone 2 or even zone 1. This is an example of risk classification migration, which is discussed in more detail

in subsequent chapters. A 'rabbit' in a company context would be something like IT facilities. There are likely to be constant minor IT problems such as viruses and the server going down. These events are common, but do not have much impact provided they are adequately managed and the appropriate procedures are in place.

Mice are less dangerous still and are unlikely to cause any real damage, although they are always present. Even with professional pest controllers, it is impossible to eradicate mice, and it is probably not desirable to do so anyway as they doubtless have a part to play. This view may be compromised when their residue is observed in a restaurant! A 'mouse' in a company context would be something like employee sick leave. People take sick leave all the time but, provided there are adequate overall staff resources, the consequences are generally minor. Most human resource departments allow for sick leave in setting staff levels. Sick leave can become a problem if it is not controlled.

The quadrant representation used in the illustration above is sometimes knows as a *risk map*. A simple two-way representation of likelihood against impact can be a very effective way of representing risk classification. A risk map is particularly useful where the various risks under consideration are dynamic. In practice most risks are dynamic in that they change over time. In the animals example, the risk map will be different depending on where the risk taker is. If the risk taker decides to go swimming off the east coast of Africa (for example), then the likelihood of the lion risk diminishes whereas the likelihood of the shark risk increases. In both cases the impact will probably remain the same.

In an organisation the likelihood of a mechanical failure in a production line will increase over time, presumably as a function of a number of independent variables including:

- age;
- maintenance;
- vandalism;
- fitness for use;
- reliability;
- sabotage.

The risk map is therefore used to show the migration of risk classification over time. It can provide a useful tracking mechanism for showing how risks migrate from one zone to another as dependent variables change over time. The main risks to look out for are obviously the high-likelihood ,high-impact ones (the lions). It is also important to watch other risks that migrate towards the lion quadrant over time. In risk mapping, mice really can grow into lions.

## 1.5 Exposure, Sensitivity and the Risk Profile

As discussed, risks are counter to opportunity, and risks are used to create value. As organisations evolve and as society generally becomes more complex, the ways in which risks are used to create value are changing. The risks that are acceptable for a given organisation at a given time can be defined in terms of a *risk profile*.

The use of risks to create value is changing. The profile of risk management and the risks defined by organisations in decision making are also changing. As organisations grow and become more complex, new risks come within the decision-making boundaries of the organisation. As a result, the risk management system has to become more sophisticated and

refined. The risk management system itself is generally calibrated to match the risk profile of the organisation. There are numerous ways of representing a risk profile. In its simplest form it is simply a listing of the various identified risks together with impact and occurrence probability estimates. The other extreme is represented by complex software profile modelling techniques based on probabilistic branching and conditional modelling.

*Exposure* is a measure of the extent to which an organisation has one or more of its functions open to risk. The organisation as a whole can be protected from risk in numerous ways. An organisation might have outsourced its cleaning functions to a supplier. In outsourcing the function, it has (theoretically) reduced its exposure to absenteeism or other workforce problems previously associated with that function. Theoretically, that risk has been transferred to the contractor, who presumably covers it with a premium. The extent to which organisations have outsourced specific functions affects their overall exposure to risk, but it is important to realise that outsourcing does not eliminate the risk; it simply transfers it. Risk transfer reduces the overall exposure of the organisation. As exposure reduces, the chances of 'taking a hit' are correspondingly reduced.

Some risks will affect the likelihood of a business attaining its *key performance indicators*. A firm is considered as having threats to its KPIs when a change in a given external variable will result in a measurable and corresponding change in one or more of the organisation's key performance indicators. In general terms the greater the possibility or potential for changes in KPI performance, the greater the degree of exposure of the organisation.

All organisations have some degree of exposure, but some are more exposed than others. The importance or significance of the degree of exposure in terms of the risk profile is largely determined by the *sensitivity* of the various functions. Risk sensitivity is a function of how much a particular 'hit' can hurt the organisation. In general, larger companies can absorb larger impacts than smaller ones. However, smaller companies with large reserves might be able to absorb larger hits than might at first appear to be the case.

A firm's sensitivity to risk is therefore a function of three variables:

- the significance or severity of the organisation's exposure to the occurrence of different risky events;
- the likelihood of these different events occurring in isolation or collectively within a given timescale;
- the organisation's ability to handle these different events, or combinations of events, should one or more of them occur within any give timescale.

A university, for example, might have a variety of income sources. These include tuition fees, research income, income from conferences and catering, rental income from a nearby research park, and so on. The university will have a certain sensitivity to changes in any of the variables that affect these various revenue streams. Tuition fees will be a function of student numbers, which in turn are a function of a complex variable set. Research income will be a function of general economic activity levels and government funding. Catering and conference income will again be affected by general levels of economic activity and perhaps by changes in local and regional competition. Changes in one single external variable such as government funding will affect some, but not all, of these key areas.

Some events could be linked. For example, government funding could be linked to general levels of economic activity. A slight downturn in the economy might affect a range of different key areas in different ways. The real danger comes when a series of unrelated or

partially related events occur that affect all of the key areas at the same time. The likelihood of their occurring simultaneously might be low but, if it is there, the university must be able to demonstrate that it has the necessary ability to cover this sensitivity. One way could be to use up reserves or borrow, although this will be limited by existing borrowing and overall borrowing capacity.

In considering exposure, sensitivity and the risk profile, the risk taker would consider the following questions:

- What specific possible outcomes do we face?
- Are these outcomes related?
- How sensitive are our strategies, cash flow, earnings etc. to the occurrence of future events?
- Is our achievement of critical objectives affected by future events?
- How capable are we of responding to whatever may happen in the future?
- How much potential reward is required before we are willing to accept the risks associated with the uncertainties that we face?
- If we decide to accept the exposures giving rise to our risks, do we have sufficient capital to absorb significant unforeseen losses, should they occur?

## 1.6 The Concept of Risky Conditions for Decision Making

Decision making under conditions of risk, certainty and uncertainty is considered in more detail in Module 2.

Risk is intrinsically linked to decision making. It is one of the three primary conditions under which decisions have to be made. The three primary conditions that apply in virtually all cases are:

- conditions of risk;
- conditions of certainty;
- conditions of uncertainty.

*Conditions of risk* apply where there is a reasonable likelihood that an event will occur and where some kind of assessment of impact can be made. The decision can then be made on the basis of these probability and impact assessments. These events cannot be projected with any degree of certainty, and they are therefore *unknown* events. To classify them to the next level, they are *known unknown* events. They cannot be predicted with great accuracy, but a reasonable assessment can be made by interpolating from past known events. This type of consideration is standard for insurance companies. When insuring an automobile driver, the insurance company considers individual age, past record, location and so on. The insurance company also considers general accident rates on a wider scale. The level of risk in the current assessment is evaluated largely from past data.

Another example would be a cricket captain considering the weather. In England it will definitely rain at some point, and probably soon. 'Soon' means different things in summer and winter, and also in different parts of the country. The captain therefore knows that it will rain (*known*), but he or she does not know when (unknown). This is therefore a risky event, and is a *known unknown*. Most insurance underwriters or even bookies (horse race betting) could give an assessment of the likelihood of the event based on past experience.

As an alternative to conditions of risk, decisions may have to be made under *conditions of certainty*. Conditions of certainty apply where the outcome is known. If a person throws a stone in the air it can be forecast with certainty that it will always fall back to earth. Theoretically, if somebody could throw the stone hard enough to achieve escape velocity it would go into orbit, but this eventuality is beyond consideration. It would therefore be reasonable to say that, if a person throws a stone out over a large glass roof, the stone will hit the glass at some point and damage will probably occur. This is therefore a *known* event. It does not have an *unknown* element.

The final possible conditions under which a decision might be made are conditions of uncertainty.

Uncertain conditions apply where it is not possible to identify any *known* events. Decision making under conditions of uncertainty is therefore concerned with wholly *unknown unknown* events. Considering the weather, this would apply to the likely occurrence and impact of a wholly unforeseeable and unparalleled storm, such as the great storm of 1987 in southern England. This freak weather system generated hurricane-strength winds; it was exceptional in every sense, and could not have been predicted with any accuracy using any existing meteorological data.

Decision making is intrinsically linked to risk conditions at all levels. This linkage is particularly important in deciding on future strategies. In selecting a strategy, a company is faced with making its most significant decisions under conditions of great uncertainty and risk. A risk-averse executive may hedge his or her bet by making a number of smaller investments or *partnering* with another organisation. Other organisations might favour investments in flexibility, which will allow the organisation to evolve as the future becomes more defined. However, the costs of a 'wait and see' strategy can be high, and waiting allows a *window* for competitors.

Making strategically sound decisions under conditions of uncertainty involves the identification of a range of outcomes or a discrete set of scenarios. Even the most uncertain business environments contain a lot of information, such as demographic trends, which describe changes in the characteristics of the population over time. There is also a range of other factors such as elasticities of demand, which are currently unknown but can be determined to a degree through research. After considering all these factors, and resolving as much uncertainty as possible, the uncertainty that remains is called *residual uncertainty*. Residual uncertainty is always present. In a strategic context it cannot be eradicated or transferred unless an alternative strategic risk response option is considered. The trick is to reduce it to such a level that it can be contained within the limits of the risk management system and that, if any uncertain events do impact, the system has sufficient reserves and responsive mechanisms to cope with them.

## 1.7 The Concept of Risk Management

Risk management is considered in more detail in Module 3.

The previous sections have highlighted the nature of risk and have given some insight into the range and type of risks that may be encountered and also the risk characteristics of the environment under which decisions are made. Having considered these factors, the next requirement is to establish an effective system for managing the risks to which an organisation is exposed.

Risk management is the process by which risks are managed alongside all other aspects of the business. It has already been established that risks are abundant and take numerous forms. Risks can be reduced and controlled up to a point, but they cannot be entirely eliminated, nor should organisations seek to do so. The organisation that is willing to take the risk may well be the one that succeeds overall. Risk management is the process that identifies risks and classifies them in some way so that they can be assessed and prioritised. It then controls and coordinates the chosen response of the organisation. Risk management is therefore a control mechanism for ensuring that overall risk magnitude stays within acceptable limits.

A typical risk management system first identifies all of the risks that are relevant. It analyses these risks and classifies them in some way, and then it gives consideration to the amount of risk that is acceptable in a particular application. Having established the level of risk that is acceptable, the risk management system makes an appropriate response. It then monitors and controls itself over a period of time.

A typical risk management system comprises:

- an identification process;
- an analysis and classification process;
- a controlled consideration of organisational attitude or strategy;
- a precaution or safeguard related to risk appetite;
- a response process;
- ongoing control and self-assurance.

Each stage is equally important.

*Risk identification* is the usual starting point. Risk identification is the process of looking at the organisation or project or process and identifying all of the risks that are relevant to the decision.

Identifying the risks does not necessarily mean that adequate response will be made.

It is very dangerous to overlook specific risks that have been identified, especially if they have catastrophic implications. An example is *HMS Hood*, which exploded and sank during combat with *Bismarck* in the Denmark Strait in 1941. *Hood* was a fast, heavily armed but lightly armoured battle cruiser. *Bismarck* was a slightly slower heavily armed and heavily armoured battleship. Hood had reasonable side armour but weak deck armour. This made the ship vulnerable to air attack and to plunging shells from high-trajectory (long-distance) salvos. The designers knew this, as did the Admiralty. They had seen ample evidence in the battle of Jutland in 1917, when three battle cruisers had been sunk under similar conditions. The risk was ignored, and a plunging shell from a *Bismarck* salvo hit the aft magazine and the ship exploded, leaving only three survivors.

It is crucial that all risks are identified and all high-impact, high-probability risks (lions) are properly classified and managed. They should never be ignored or underestimated.

Analysis and classification can take many forms. There are numerous established analysis tools and techniques ranging from simulation to bidding theory. The idea is to evaluate the risks in such a way that they can be compared with each other and assessed against the organisation as a whole.

Once the risks are analysed and classified, the organisation has to allow for its *risk appetite*. Risk is everywhere and has to be effectively managed. The extent to which large risks are

taken or the level to which identified risks are reduced are measures of the risk appetite of the organisation. Some organisations are naturally more risk averse than others. The appetite is the primary determinant of the subsequent risk response. In the *HMS Hood* example above, the British Admiralty knew from experience that the weak upper deck armour on this ship was a problem and constituted a real risk. However, they decided that the risk to the ship was not sufficiently great to prevent it from being used in action against a fully armoured battleship. More risk-averse decision makers might have decided to restrict the scope of action of *HMS Hood* and similar ships (a decision that was actually taken soon after the incident).

The risk management system also contains a requirement for a response. After analysing the risk and considering risk appetite the appropriate response is made. Typical examples are to try to:

- eradicate the risk;
- reduce the likelihood of the risk occurring;
- reduce the impact of the risk;
- transfer the risk to somebody else;
- accept the risk.

Finally, the risk management system needs a provision for ongoing monitoring and control. A risk management system can itself create new risk in that it can generate a false sense of security. There is always a danger that managers will assume that the risk management process will take care of everything, and operational vigilance can be reduced. In fact the risk 'universe' is very much dynamic, and the risk profile that faces an organisation can vary both significantly and quickly. The risk management system has to be monitored and adapted as necessary as the risks that it is attempting to manage change.

## Learning Summary

This module has covered:

- the concept of risk;
- the concept of risk and opportunity;
- the basic risk impact levels and types of risk;
- how risks can be classified;
- the idea of exposure, sensitivity and the risk profile;
- the concept of risk conditions and decision-making;
- the concept of risk management.

It should be apparent that risk is omnipresent and can be of many different types. The importance of individual or collective risks depends on the risk profile of the organisation together with the sensitivity and exposure of the organisation. The following section summarises some of the main learning outcomes from the various sections in Module 1.

## The Concept of Risk

- Risk is an inherent factor in virtually every human endeavour.
- The prevalence and complexity of risk tend to increase as a function of the development of society.
- Human beings naturally consider risk and reward as part of any decision-making process, and people make decisions constantly, whether major or minor, or whether directly or subconsciously.
- Risks can be evaluated 'scientifically' by identifying the various factors or variables that define the risk.
- Risks can also be evaluated 'intuitively', where an individual evaluates the risk in the light of past experience and consideration of the key elements of this particular case and makes a subjective appraisal.
- Between the two extremes of 'scientific' and 'intuitive' risk and reward consideration, the human reasoning and evaluation of any particular event is based on decision making within the limits of what are acceptable and non-acceptable outcomes.
- The maximum loss limit that is affordable defines the upper limit of the range of acceptable outcomes. Losses above this limit cannot be afforded and are therefore non-acceptable irrespective of the size of the potential reward.
- The consideration of risk and reward is the basis of risk analysis. Risk analysis can be considered as a basic function of the human cognitive process. People evaluate potential risks and rewards in terms of the range of acceptable outcomes when deciding on whether or not to do something.
- Risk is not a negative concept. Risk is necessary in order for opportunity to exist. It can be a deterrent to competition, leaving the risk taker to take advantage.

## The Basic Risk Types

- There are numerous types of risk. The number of possible sources and combinations of sources of risk is almost beyond classification. The primary classification typologies revolve around the origin of the risk and around the nature of the effect.
- Strategic risk relates to risk at the corporate level and affects the development and implementation of an organisation's strategy.
- Operational risk relates to the production process.
- Project risk operates at the programme or project levels.
- Change risk operates at the strategic, operational and project levels. Changes can be imposed by variations elsewhere either within or outside the organisation, or can be planned and engineered by the organisation as a way to achieve objectives.
- Unforeseeable risk also operates at the strategic, operational and project levels. Unforeseeable risk is the type of risk that cannot be accurately forecast before it occurs. It is generally allowed for by flexibility within the system with additional contingencies.
- Internal risks originate from within the organisation, whereas external risks originate from the environment.
- Speculative risk relates to risks where the net outcome can be positive or negative.
- Static risk relates to risks where the net outcome can only be negative.
- Risks at all levels and across all functions are interdependent. It is dangerous to consider any particular risk in isolation as risks at all levels and functions are linked. A change in any one can effect (i.e. bring about) changes in numerous others.

## The Concept of Risk Classification

- Risk can be measured or classified in terms of the probability and consequence of not achieving a specific goal or objective.
- Risk depends both on the *likelihood* (probability) of an event occurring and on the *consequences* (impact) of that event should it occur.
- Risk = *f* (event, uncertainty, consequences)
- Risk can also be classified in terms of the degree of hazard and the controls that are necessary to protect against that hazard.
- Risk = *f* (event, hazard, control).
- The classification process identifies the importance of the risk. It highlights those risks that are critical and those that can perhaps be left alone for a while. This identification and rating can be based on likelihood and impact or on control and hazard.
- Lions are high-impact, high-likelihood risks. They are very dangerous all of the time and have to be very carefully controlled.
- Sharks are high-impact, low-likelihood risks. They are just as dangerous (high impact) as lions but the likelihood of them being able to injure a human being is much less than a lion because sharks are only a threat in their own environment (the sea). As long as a person remains out of the water, sharks are no threat. People therefore have a degree of control over the threat offered by sharks.
- Rabbits are low-impact, high-likelihood risks. There are lots of rabbits but they do only limited damage so long as there are not too many of them around. It is generally safe to ignore rabbits so long as they are monitored in some way and some action is taken if their numbers begin to multiply to excessive levels.
- Mice are low-impact, low-likelihood risks. There are not many mice around any more and they cause relatively little damage. Mice can be disregarded unless a person has a business or other kind of activity that is not compatible with even a small number of mice.

## Exposure, Sensitivity and the Risk Profile

- The profile of risk management and the risks defined by organisations in decision making is a part of a dynamic process.
- Exposure is a measure of the extent to which an organisation has one or more of its functions open to risk.
- All organisations have some degree of exposure and some are more exposed than others. The importance or significance of the degree of exposure in terms of the risk profile is determined largely by the sensitivity of the various functions.
- Risk sensitivity is a function of how much a particular 'hit' can hurt the organisation.
- Sensitivity is a function of the significance or severity of the organisation's exposure to the occurrence of different events.
- Sensitivity is also a function of the likelihood of these different events occurring in isolation or collectively over any particular timescale.
- Sensitivity is also a function of the organisation's ability to handle these different events, or combinations of events, should one or more of them occur within any give timescale.

## The Concept of Risky Conditions for Decision Making

- Risk is intrinsically linked to decision making. It is one of the three primary conditions under which decisions have to be made.
- Conditions of risk apply where there is a reasonable likelihood that an event will occur and where some kind of assessment of its impact can be made. The decision can be made on the basis of likelihood and impact assessment.
- Conditions of certainty apply where the outcome is known.
- Uncertain conditions apply where it is not possible to identify any *known* events.

## The Concept of Risk Management

- Risk management is the process by which risks are managed and controlled to an extent that is acceptable to the organisation. A typical risk management system comprises:
  - an identification process;
  - an analysis and classification process;
  - a controlled consideration of organisational attitude or strategy;
  - a response.
- It is crucial that all risks are identified and all high-impact, high-likelihood risks (lions) are properly classified and managed. They should never be ignored or underestimated.
- Analysis and classification can take many forms. There are numerous established analysis tools and techniques, ranging from simulation to bidding theory.
- The end result of the risk management process is the response. This depends largely on the results of the classification and analysis and the attitude of the risk taker.
- The response can vary between refusing to accept the risk (don't overtake), reducing it (wait for straighter piece of road), avoiding it (go another way), or accepting it (accelerate and go for it).