irm

Fundamentals of Risk Management

Understanding, evaluating and implementing effective risk management

Paul Hopkin

KoganPage

3
Types of risks

Timescale of risk impact

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

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

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

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

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

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

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

Hazard, control and opportunity risks

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

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

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

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

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

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

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

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

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

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

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

Table 3.1 Categories of disruption

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

Hazard tolerance

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

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

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

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

Security standards

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

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

Management of hazard risks

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

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

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

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

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

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

Uncertainty acceptance

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

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

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

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

Opportunity investment

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

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

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

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

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

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

Heart disease risk factors

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

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

4

Development of risk management

Origins of risk management

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

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

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

Table 4.1 Definitions of risk management

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

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

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

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

Table 4.2 Importance of risk management

Managing the Organization

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

Changes in the Marketplace

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

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

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

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

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

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

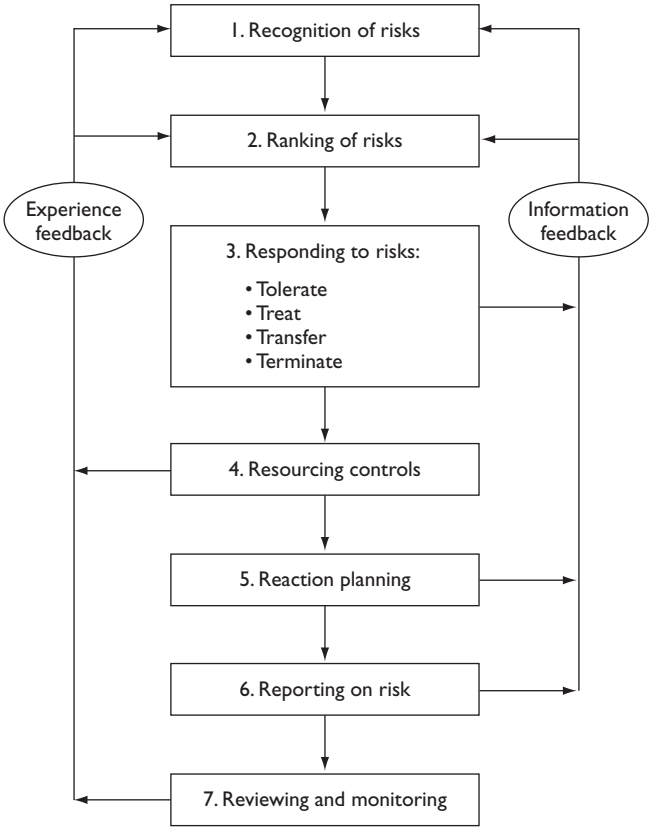

Figure 4.1 7Rs and 4Ts of (hazard) risk management

Insurance origins of risk management

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

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

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

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

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

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

Specialist areas of risk management

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

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

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

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

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

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

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

Enterprise risk management

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

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

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

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

Levels of risk management sophistication

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

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

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

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

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

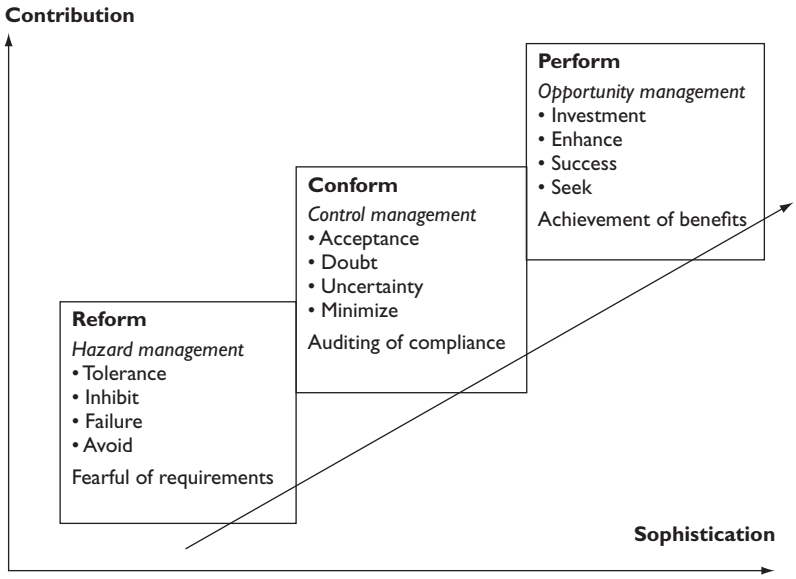

Figure 4.2 Risk management sophistication

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

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

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

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

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

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

Risk maturity models

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

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

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

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

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

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

5
Principles and aims of risk management

Principles of risk management

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

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

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

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

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

Table 5.1 Principles of risk management

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

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

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

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

Importance of risk management

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

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

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

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

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

Risk management activities

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

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

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

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

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

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

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

Efficient, effective and efficacious

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

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

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

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

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

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

Perspectives of risk management

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

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

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

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

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

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

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

Implementing risk management

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

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

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