Part I

Enterprise Risk Management in Context

1 Introduction

A pessimist sees the difficulty in every opportunity; an optimist sees the opportunity in every difficulty.
(Winston Churchill)

Risk management has taken centre stage. It is now the most compelling business issue of our time. Shareholders have repeatedly suffered from erratic business performance. Recent history has shown that risk exposure has not been fully understood and risk management practice has been inadequate. Looking back, while economists have cited many reasons for the Asian financial crisis of 1997–1998, clearly foreign exchange risk was a major contributor. After the New York World Trade Center and Pentagon terrorist attack on 11 September 2001, enterprise risk management was found to be wanting. Business continuity planning had been inadequate. In particular, it was found that greater emphasis needed to be placed on IT disaster recovery, human resource management and communication. After the bankruptcies of Enron in December 2001 and WorldCom in July 2002, inadequate corporate governance and the "soft underbelly" of risk management were exposed, arising primarily from the lack of integrity of financial reporting, a lack of compliance with regulations and operational failures. In late August 2005 Hurricane Katrina struck, reportedly the costliest natural disaster in US history. Oil production, importation and refining were interrupted.[1] Businesses were suddenly exposed to a surge in energy prices, continuity failures and shipping disruption. Costs of production rose and sales fell. More recently, failure to properly understand and manage risk has been cited as the root cause for the global financial crisis of 2007–2010. So severe was this financial tsunami that many economists have described it as the worst financial disaster since the Great Depression of the 1930s. Boards in the financial sector were accused of being greedy, reckless[2] and dysfunctional and in some cases "sheep", falling into the trap of "group think" due to an apparent absence of independent thinking. In addition, there had been a lack of appreciation of risk at both a business and a macro or industry level. Systemic risk in the financial industry had not been recognised, understood or addressed. Regulators on both sides of the Atlantic and the banks themselves failed to recognise the interconnectedness of banks and the potential domino effect of bank failure. If the financial crisis was not excitement enough, the media have had a field day with a number of high-profile and very damaging business ethics failures relating to bribery, insider trading, invasion of privacy and sexual harassment.

[1] As a result of Hurrricane Katrina, at least 20 offshore oil platforms went missing, sunk or adrift.

[2] In an economy where certain businesses are considered "too important to fail" and the taxpayer is called upon to underwrite the risks of banks in the private sector, banks were severely criticised for gambling with taxpayers' money. Banks in the UK had a pivotal role in the global financial crisis and caused economic instability and erosion of national prosperity. The need to nationalise the banks' losses resulted in unemployment particularly in the public sector and left those in employment facing a significant drop in their standard of living. The banks have responded by reinstating extravagant rewards and extraordinary bonuses.

1.1 RISK DIVERSITY

Providing strategic direction for a business means understanding what drives the creation of value and what destroys it. This in turn means that the pursuit of opportunities must entail comprehension of the risks to take and the risks to avoid. Hence, to grow any business entails risk judgement and risk acceptance. A business's ability to prosper in the face of risk, at the same time as responding to unplanned events, good or bad, is a prime indicator of its ability to compete. However, risk exposure continues to grow greater, more complex, diverse and dynamic. This has arisen in no small part from rapid changes in the globalisation of business, speed of communication, the rate of change within markets and technology. Businesses now operate in an entirely different environment compared with just three years ago. Recent experience has shown that as businesses strive for growth, internal risks generated by a business itself can be as large as (or greater than) external risks. The adoption of expansion strategies, such as investment in emerging markets, developing significant new products, acquisition, major organisational restructuring, outsourcing key processes and major capital investment projects can all increase a business's risk exposure.[3]

A review of risk management practices in 14 large global corporations revealed that by the end of the 1990s the range of risks that companies felt they needed to manage had vastly expanded, and was continuing to grow in number (Hunt 2001). There are widespread concerns over e-commerce, which has become accepted and embedded in society with startling speed. According to the Economist Intelligence Unit (2001):

> Many companies perceive a rise in the number and severity of the risks they face. Some industries confront unfamiliar risks stemming from deregulation. Others worry about increasing dependence on business-to-business information systems and just-in-time supply/inventory systems. And everyone is concerned about emerging risks of e-business – from online security to customer privacy.

As a consequence of the diversity of risk, risk management requires a broader approach. This sentiment was echoed by Rod Eddington, former chief executive officer (CEO) of British Airways, who remarked that businesses now require a broader perspective of risk management. He went to say that:

> If you talked to people in the airline industry in the recent past, they very quickly got on to operational risk. Of course, today we think of risk as the whole of business. We think about risk across the full spectrum of the things we do, not just operational things. We think of risk in the context of business risks, whether they are risks around the systems we use, whether they are risks around fuel hedging, whether they're risks around customer service values. If you ask any senior airline person today about risk, I would hope they would move to risk in the true, broader sense of the term. (McCarthy and Flynn 2004)

All stakeholders and regulators are pressing boards of directors to manage risk more comprehensively, rigorously and systematically. Companies that treat risk management as just a compliance issue expose themselves to nursing a damaged balance sheet.

[3] Conventional risk management focused on avoiding risks to the business strategy as opposed to managing the risks of the strategy itself, which is where a number of banks have had spectacular failings.

1.2 APPROACH TO RISK MANAGEMENT

This evolving nature of risk and expectations about its management have now put pressure on previous working practices. Historically, within both private and public organisations, risk management has traditionally been segmented and carried out in "silos". This has arisen for a number of reasons such as the way our mind works in problem solving, the structure of business organisations and the evolution of risk management practice. There is clearly the tendency to want to compartmentalise risks into distinct, mutually exclusive categories, and this would appear to be a result of the way we subdivide problems to manage them, the need to allocate tasks within an existing organisational structure and the underlying assumption that the consequences of an unforeseen event will more or less be confined to one given area. In actuality, the fallout from unforeseen events tends to affect multiple business areas and the interrelationships between risks under the categories of operational, financial and technical risk have been overlooked, often with adverse outcomes. Patricia Dunn, former CEO of Barclays Global Investors and former non-executive chairwoman of the board of Hewlett-Packard (HP),[4] has previously identified a failing in approach:

> I think what Boards tend to miss and what management tends to overlook is the need to address risk holistically. They overlook the areas that connect the dots because risk is defined so "atomistically" and we don't have the perspective and the instrument panel that allows us to see risk in a 360 degree way. (McCarthy and Flynn 2004)

Enterprise risk management (ERM) is a response to the sense of inadequacy in using a silo-based approach to manage increasingly interdependent risks. The discipline of ERM, sometimes referred to as strategic business risk management, is seen as a more robust method of managing risk and opportunity and an answer to these business pressures. ERM is designed to improve business performance. While not in its infancy, it is a slowly maturing approach, where risks are managed in a coordinated and integrated way across an entire business. The approach is less to do with any bold breakthrough in thinking, and more to do with the maturing, continuing growth and evolution of the profession of risk management and its application in a structured and disciplined way (McCarthy and Flynn 2004). ERM is about understanding the interdependencies between the risks, how the materialisation of a risk in one business area may increase the impact of risks in another business area. In consequence, it is also about how risk mitigation action can address multiple risks spanning multiple business sectors. It is the illustration of this integrated approach which is the focus of this book.

1.3 BUSINESS GROWTH THROUGH RISK TAKING

Risk is inescapable in business activity. As Peter Drucker explained as far back as the 1970s, economic activity by definition commits present resources to an uncertain future. The one thing that is certain about the future is its uncertainty, its risks. Hence, to take risks is the essence of economic activity. He considers that history has shown that businesses yield greater economic performance only through greater uncertainty – or in other words, through greater risk taking (Drucker 1979).

[4] Hewlett-Packard is referred to in Chapter 19 regarding their unethical behaviour and infringement of privacy.

Nearly all operational tasks and processes are now viewed through the prism of risk (Hunt 2001). Indeed, the term "risk" has become shorthand for any corporate activity. It is thought not possible to "create a business that doesn't take risks" (Boulton *et al*. 2000). The end result of successful strategic direction setting must be capacity to take a greater risk, for this is the only way to improve entrepreneurial performance. However, to extend this capacity, businesses must understand the risks that they take. While in many instances it is futile to try to eliminate risk, and commonly only possible to reduce it, it is essential that the risks taken are the right risks. Businesses must be able to choose rationally among risk-taking courses of action, rather than plunge into uncertainty, on the basis of a hunch, gut feeling, hearsay or experience, no matter how carefully quantified. Quite apart from the arguments for risk management being a good thing in its own right, it is becoming increasingly rare to find an organisation of any size whose stakeholders are not demanding that its management exhibit risk management awareness. This is now a firmly held view supported by the findings of the Economist Intelligence Unit's enterprise risk management survey, referred to earlier. It discovered that 84% of the executives who responded considered that ERM could improve their price/earnings ratio and cost of capital. Organisations that are more risk conscious have for a long time known that actively managing risk and opportunity provides them with a decisive competitive advantage. Taking and managing risk is the essence of business survival and growth.

1.4 RISK AND OPPORTUNITY

There should not be a preoccupation with downside risk. Risk management of both upside risks (opportunities) and downside risks (threats) is at the heart of business growth and wealth creation. Once a board has determined its vision, mission and values, it must set its corporate strategy, its method of delivering the business's vision. Strategy setting is about strategic thinking. Setting the strategy is about directing, showing the way ahead and giving leadership. It is being thoughtful and reflective. Whatever this strategy is, however, the board must decide what opportunities, present and future, it wants to pursue and what risks it is willing to take in developing the opportunities selected. Hence the discipline of risk management should support both the selection and setting of the strategy. However, risk and opportunity management must receive equal attention and it is important for boards to choose the right balance. This is succinctly expressed by the National Audit Office: "a business risk management approach offers the possibility for striking a judicious and systematically argued balance between risk and opportunity in the form of the contradictory pressures for greater entrepreneurialism on the one hand and limitation of downside risks on the other" (National Audit Office 2000). An overemphasis on downside risks and their management can be harmful to any business.

Knight and Petty (2001) stress that risk management is about seeking out the upside risks or opportunities, that getting rid of risk stifles the source of value creation and upside potential. Any behaviour that attempts to escape risk altogether will lead to the least rational decision of all, doing nothing. While risks are important, as all businesses face risk from inception, they are not grounds for inaction but restraints on action. Hence risk management is about controlling risk as far as possible to enable a business to maximise its opportunities. Development of a risk policy should be a creative initiative, exposing exciting opportunities for value growth and innovative handling of risk, not a depressing task, full of reticence, warning

and pessimism (Knight and Petty 2001). ERM, then, is about managing both opportunities and risks.

1.5 THE ROLE OF THE BOARD

Even before the global financial crisis, George "Jay" Keyworth, former member of Hewlett-Packard's board, stated that the most important lesson of the last few years is that board members can no longer claim impunity from a lack of knowledge about business risk. The message here is that when something goes wrong, as inevitably it does, board members will be held accountable. The solution is for board members to learn of the potential for adverse events and be sufficiently aware of the sources of risk within the area of business that they are operating in, to be afforded the opportunity to take pre-emptive action (McCarthy and Flynn 2004). The business of risk management is undergoing a fundamental sea change with the discipline of risk management converging at the top of the organisation and being more openly discussed in the same breath as strategy and protection of shareholders. Greater risk taking requires more control. Risk control is viewed as essential to maintaining stability and continuity in the running of businesses. However, in the aftermath of a series of unexpected risk management failures leading to company collapses and other corporate scandals in the UK, investors have expressed concerns about the low level of confidence in financial reporting, board oversight of corporate operations, the safeguards provided by external auditors and the degree of risk management control. These early concerns led to a cry for greater corporate governance, which led to a series of reports on governance and internal control culminating in the Combined Code of Corporate Governance (2003). The incremental development of corporate governance leading up to and beyond the 2003 Code is discussed in Chapter 2. Clearly risk exposure has been growing in an increasingly chaotic and turbulent world, and time has shown that this turbulence has not abated.

The lack of risk management control resides with the board. In 1995 in response to bad press about boards' poor performance and the lack of adequate corporate governance, the Institute of Directors (IoD) published *Standards for the Board*. It proved to be a catalyst for debate on the roles and tasks of a board and on the need to link training and assessed competence with membership of directors' professional bodies. The publication laid out four main objectives for directors. Within the IoD's 2010 factsheet entitled *The role of the board,* apart from one of the objectives being split into two, these objectives remain virtually unchanged as follows:

1. The board must simultaneously be entrepreneurial and drive the business forward while keeping it under prudent control.
2. The board is required to be sufficiently knowledgeable about the workings of the company and answerable for its actions, yet able to stand back from the day-to-day management of the company and retain an objective, longer-term view.
3. The board must be sensitive to the pressure of short-term issues and yet take account of broader, long-term trends.
4. The board must be knowledgeable about "local" issues and yet be aware of potential or actual wider competitive influences.
5. The board is expected to be focused on the commercial needs of the business, while acting responsibly towards its employees, business partners and society as a whole.

The task for boards of course is to ensure the effectiveness of their risk model. With this in mind, here are some action items for the strategic risk management agenda for boards and CEOs to consider:[5]

- Appoint a C-level risk leader empowered not only with the responsibility, but also with the authority to act on all risk management matters.
- Ensure that this leader is independent and can work objectively with the company's external advisers (external audit, legal, etc.) and the governing decision maker and oversight function (the CEO and board).
- Be satisfied as to the adequacy of the depth of current risk analysis actions, from an identification, assessment and mitigation standpoint.
- Be confident that the risk management information that board members receive is accurate, timely, clear and relevant.
- Actively require and participate in regular dialogue with key stakeholders to understand if their objectives have been captured, debated and aligned, are being met and whether stakeholders may derail current initiatives.
- Strive to build a culture where risk management and strategic planning are intertwined.
- Ensure that risk management remains focused on the most serious issues.
- Ensure that risk management is embedded throughout the organisation.

As illustrated in Figure 1.1, risk and opportunity impinge on the four main functions of boards: policy formulation, strategic thinking, supervisory management and accountability. Policy formulation involves setting the culture for the organisation, which should include risk management. Strategic thinking entails selecting markets to pursue and committing resources to those markets on the strength of the risk profile prepared. Supervisory management requires businesses to put in place oversight management and governance processes, including formal risk management. Accountability relates to ensuring that risk mitigation actions have clear owners who are charged with implementing pre-agreed actions to address the risks identified, report changes in risk profiles and engage in ongoing risk management.

1.6 PRIMARY BUSINESS OBJECTIVE (OR GOAL)

The primary objective of a business is to *maximise* the *wealth* of its *shareholders* (owners). In a market economy, the shareholders will provide funds to a business in the expectation that they will receive the maximum possible increase in wealth for the level of risk which must be faced. When evaluating competing investment opportunities, therefore, the shareholders will weigh the returns from each investment against the potential risks involved. The use of the term "wealth" here refers to the market value of the ordinary shares. The market value of the shares will in turn reflect the future returns the shareholders will expect to receive over time from the shares and the level of risk involved. Shareholders are typically not concerned with returns over the short term, but are concerned with achieving the highest possible returns over the long term. Profit maximisation is often suggested as an alternative objective for a business. Profit maximisation is different from wealth maximisation. Profit maximisation is usually seen as a short-term objective, whereas wealth maximisation is a long-term objective.

[5] These recommendations were made in the first edition of this text published in 2006, prior to the global financial crisis and the Walker Review of 2009 described in Chapter 2.

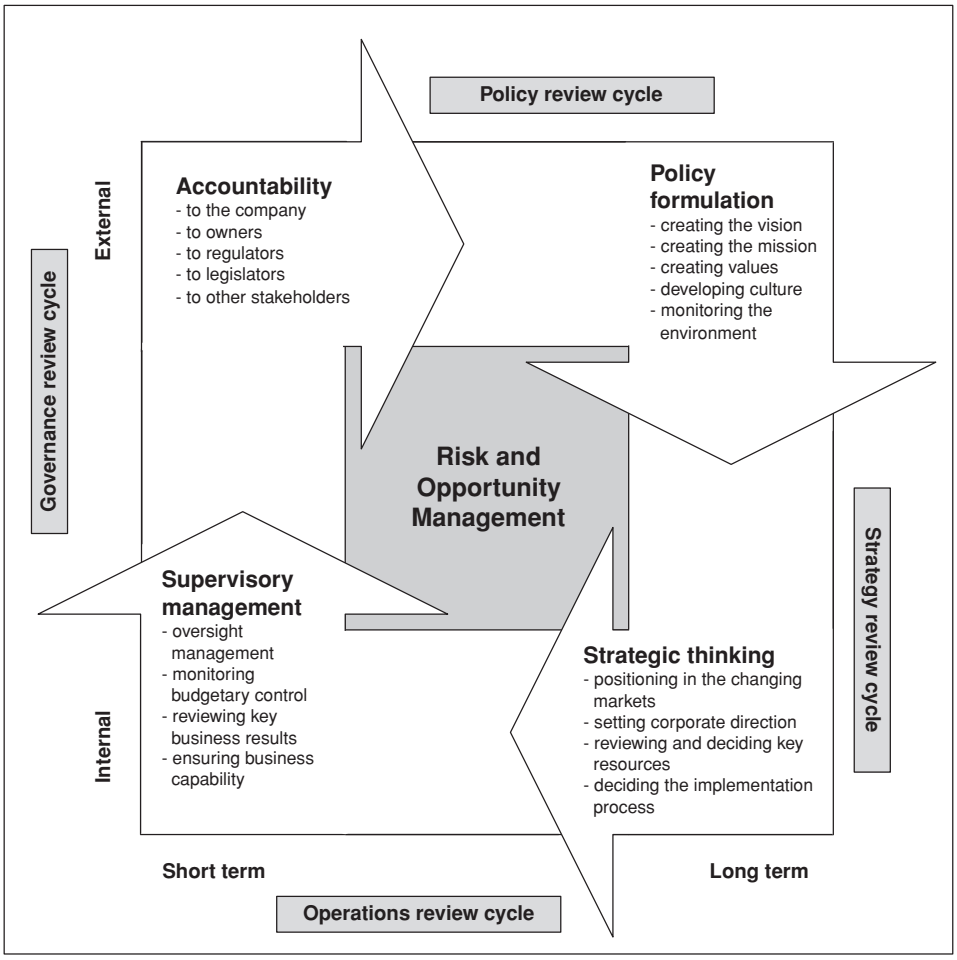

Figure 1.1 The role of the board and the integration of risk management (Garratt 2003). Reproduced with permission from *The Fish Rots from the Head*, B. Garratt, Profile Books Ltd.

Wealth maximisation takes account of risks to long-term growth, whereas profit maximisation does not.

1.7 WHAT IS ENTERPRISE RISK MANAGEMENT?

ERM has to satisfy a series of parameters. It must be embedded in a business's system of internal control, while at the same time it must respect, reflect and respond to the other internal controls. ERM is about protecting and enhancing share value to satisfy the primary business objective of shareholder wealth maximisation. It must be multifaceted, addressing all aspects of the business plan from the strategic plan through to the business controls:

- strategic plan
- marketing plan
- operations plan

- research and development
- management and organisation
- forecasts and financial data
- financing
- risk management processes
- business controls

Enterprises operating in today's environment are characterised by constant change and require a more integrated approach to manage their risk exposure. This has not always been the case, with risks being managed in "silos". Economic, legal, commercial and personnel risks were treated separately and often addressed by different individuals within a company without any cross-referencing of the risks or an understanding of the impact of management actions adopted for one subject group on another subject group. Risks are, by their very nature, dynamic, fluid and highly interdependent. As such they cannot be evaluated or managed independently.

Largely reflecting the COSO (2004) definition, ERM may be defined as:

> A systematic process embedded in a company's system of internal control (spanning all business activity), to satisfy policies effected by its board of directors, aimed at fulfilling its business objectives and safeguarding both the shareholder's investment and the company's assets. The purpose of this process is to manage and effectively control risk appropriately (without stifling entrepreneurial endeavour) within the company's overall risk appetite. The process reflects the nature of risk, which does not respect artificial departmental boundaries and manages the interdependencies between the risks. Additionally the process is accomplished through regular reviews, which are modified when necessary to reflect the continually evolving business environment.

Hence, in summary, ERM may be defined as "a comprehensive and integrated framework for managing company-wide risk in order to maximise a company's value".

1.8 BENEFITS OF ENTERPRISE RISK MANAGEMENT

No risk management process can create a risk-free environment. Rather, ERM enables management to operate more effectively in a business environment where an organisation's risk exposure profile is never static. Enterprise risk management provides enhanced capability to:

- *Increase the likelihood of a business realising its objectives*. ERM will equip organisations with techniques to identify, record and assess the opportunities they seek to proactively pursue and exploit. At the same time it will support the identification and conscious management of the risks associated with selected opportunities to ensure that bottom-line performance is enhanced rather than eroded. In this way it will enable organisations to mature and realise their stated objectives.
- *Build confidence in stakeholders and the investment community*. As a result of the global financial crisis institutional investors, rating agencies and regulators are more focused on and more eager to learn about an organisation's capabilities for understanding and managing risk. Investors in particular will wish to understand the degree of risk their investments will be exposed to and whether the returns will be adequate. Board members and managers may be called upon to explain the framework, policy and process they have in place for managing risk. ERM provides the rigour to establish, describe and demonstrate proactive risk management.

- *Comply with relevant legal and regulatory requirements*. ERM, through establishing (and subsequently monitoring) a risk management framework, requires an organisation to understand, record (and keep up to date) the business context including, but not limited to, the legal and regulatory requirements it has to comply with and, where appropriate, the implications of not doing so.
- *Align risk appetite and strategy*. Risk appetite is the degree of risk, on a broad-based level, that a business is willing to accept in pursuit of its objectives. ERM supports management's consideration of a business's risk appetite first in evaluating strategic alternatives, then in setting boundaries for downside risk.
- *Improve organisational resilience*. As the business environment continues to change and the pace of change accelerates, resilience is critical to business longevity. Organisational resilience is sometimes considered as the degree of flexibility (or capacity) of an organisation's culture to recover from and respond to change. ERM will support an organisation in understanding potential change and preparing for it through risk response planning or in deciding to be the change catalyst through opportunity exploitation.
- *Enhance corporate governance*. ERM and corporate governance augment each other. ERM strengthens governance through challenging potential excessive risk taking as occurred in the global financial crisis, encouraging board-level engagement in the high-level risk process and improving decision making on risk appetite and tolerance.
- *Embed the risk process throughout the organisation*. ERM, through the creation of a framework, policy, process, plans and training can embed risk management throughout the organisation from the board down to all elements of the organisational structure as risk exposure can emanate from any corner of the organisation (e.g. from a breach of ethics at board level to a breach of environmental legislation by production).
- *Minimise operational surprises and losses*. ERM supports businesses to enhance their capability to identify potential risk events, assess risks and establish responses, and thereby to reduce the occurrence of unpleasant surprises and associated costs or losses.
- *Enhance risk response decisions*. ERM provides the rigour to identify and select among alternative risk responses – risk removal, reduction, transfer or retention.
- *Optimise allocation of resources*. A clear understanding of the risks facing a business can enhance the effective direction and use of management time and the business's resources to manage risk.
- *Identify and manage cross-enterprise risks*. Every business faces a myriad of risks affecting different parts of the organisation. The benefits of enterprise risk management are only optimised when an enterprise-wide approach is adopted, integrating the disparate approaches to risk management within a company. Integration has to be effected in three ways: centralised risk reporting, the integration of risk transfer strategies and the integration of risk management into the business processes of a business. Rather than being purely a defensive mechanism, it can be used as a tool to maximise opportunities.
- *Link growth, risk and return*. Businesses accept risk as part of wealth creation and preservation and they expect returns commensurate with risk. ERM provides an enhanced ability to identify and assess risks and establish acceptable levels of risk relative to potential growth and achievement of objectives.
- *Rationalise capital*. More robust information on risk exposure allows management to more effectively assess overall capital needs and improve capital allocation.
- *Seize opportunities*. The very process of identifying risks can stimulate thinking and generate opportunities as well as threats. Reponses need to be developed to seize these

opportunities in the same way that responses are required to address identified threats to a business.
- *Improve organisational learning*. ERM can enhance organisational learning through the use of lessons learnt prior to embarking on new change projects and the maintenance of records of successful risk treatment plans that effectively removed risks prior to realisation.

There are three major benefits of ERM: improved business performance, increased organisational effectiveness and better risk reporting.

1.9 STRUCTURE

A structure for understanding ERM is included in Figure 1.2 and is composed of seven elements:

1. Corporate governance is required to ensure that the board of directors and management have established the appropriate organisational processes and corporate controls to measure and manage risk across the business.
2. The creation and maintenance of a sound system of internal control is required to safeguard shareholders' investment and the business's assets.
3. A specific resource must be identified to implement the internal controls with sufficient knowledge and experience to derive the maximum benefit from the process.
4. A risk management framework is required that will provide the foundations and arrangements for embedding risk management throughout the organisation at all levels.
5. A policy should be prepared describing the importance of risk management to the achievement of the organisation's corporate goals.
6. A clear risk management process is required which sets out the individual processes, their inputs, outputs, constraints and enablers.
7. The value of a risk management process is reduced without a clear understanding of the sources of risk and how they should be responded to. The framework breaks the source of risk down into two key elements labelled internal processes and the business operating environment.

1.9.1 Corporate Governance

Examination of recent developments in corporate governance reveals that they form catalysts for and contribute to the current pressures on ERM. It explains the expectations that shareholders have of boards of directors. It explains the approaches companies have adopted to risk management and the extent of disclosure of risk management practice. Corporate governance now forms an essential component of ERM because it provides the top-down monitoring and management of risk management. It places responsibility on the board for ensuring that appropriate systems and policies for risk management are in place. Good board practices and corporate governance are crucial for effective ERM. The section that follows addresses internal control, which is a subset of corporate governance (and risk management is a subset of internal control).

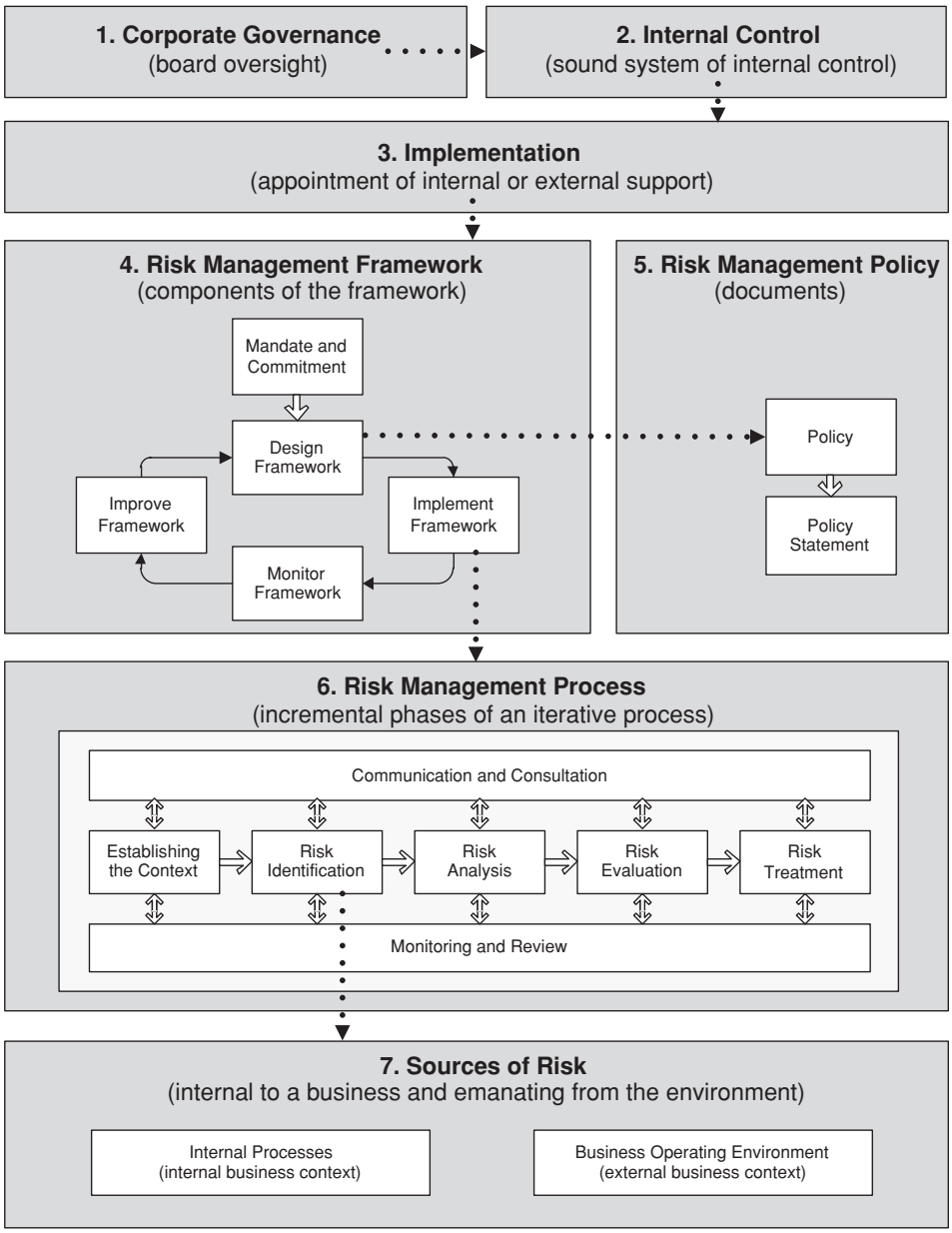

Figure 1.2 ERM structure

1.9.2 Internal Control

Examination of internal controls provides an understanding of what should be controlled and how. There is more of a focus on formal approaches. Internal controls are a subset of corporate governance. Risk management is a subset of internal controls. Risk management is aimed at facilitating the effective and efficient operation of a business, improving internal and external

reporting and assisting with compliance with laws and regulations. The aim is to accomplish this through the identification and assessment of risks facing the business and responding to them by either removing or reducing them or, where it is economic to do so, to transfer them to a third party.

1.9.3 Implementation

Implementation of risk management (forming part of a business's internal control processes) can be resourced from within a business or be supported by external consultants. Both are clearly acceptable approaches. Whichever route is selected, the parameters of any planned actions have to be mapped, communicated and agreed so that the timeframe, resources, costs, inputs and deliverables are understood.

1.9.4 Risk Management Framework

The purpose of the risk management framework is to assist an organisation in integrating risk management into its management processes so that it becomes a routine activity. The framework is aimed at ensuring that information about risk derived from the risk management process is adequately reported and is used as a basis for informed decision making. The framework is composed of five steps: mandate and commitment, design framework, implement framework, monitor framework and improve framework, as illustrated in Figure 1.2. The last four steps are cyclical in nature in that as lessons are learnt from the monitor step they are captured as enhancements in the improvement step which are fed back into the design step. Care needs to be taken to ensure the parent–child relationship between the framework and the policy is established (i.e. the policy is a subset of and subservient to the framework) and that the content of one document does not contradict or repeat the content of the other. Care should be taken to ensure that the framework is not verbose as there is a danger that the audience for whom it is intended may assign it to a shelf to collect dust.

The key aspects of each of the steps are as follows:

- *Mandate and commitment*. This step is critical in that risk management cannot be delivered from the bottom up within an organisation, but must come from the top down. Ongoing effectiveness of the risk management effort will be dependent on positive and sustained commitment by the organisation's management. Management have to be seen to be both implementing and driving risk management in recognition that risk management is one of the organisation's "vital organs" upon which the organisation's health depends. A board's commitment to risk management does not end in signing off the framework and policy. The risk management objectives must reflect and serve the organisation's objectives and performance indicators should be defined to measure the effectiveness of risk management over time. The relationship with internal audit should be established so that the organisation is ensuring legal and regulatory compliance. Management should agree and endorse the risk management policy.
- *Design framework*. The design of the framework entails understanding the organisation and its context, establishing the risk management policy, determining accountability for risk management, embedding risk management in all of the organisation's practices and processes, allocating appropriate experienced and competent risk resources, and establishing tailored internal and external communication and allied reporting.

- *Implement framework*. The timing of the implementation of the framework should be planned. Introduction into the organisation should be managed with training sessions held as required. Ensure as far as possible that decision making is based on the output of the risk management processes. Develop a risk management plan (or plans) for the delivery of the risk management process, which may vary depending on where in the organisation risk management is being implemented.
- *Monitor framework*. Periodically review with internal and external stakeholders whether the risk management framework, policy, plan and process require amendment as a result of changes in the organisation's internal or external context. Assess risk management performance against pre-agreed indicators.
- *Improve framework*. Based on the results of the monitor framework, decisions should be made on whether the risk management framework step, and the policy and process which support it, should be amended with the aim of improving the effectiveness of the organisation's risk management practices.

1.9.5 Risk Management Policy

In simple terms a policy should address *why* risk management will be undertaken, *who* within and outside the organisation will undertake it, *how* it will be undertaken by reference to the framework and process and internal functions, and *what* those who are responsible will be required to undertake. Specifically, the policy should state its purpose, objectives, scope (where it applies within the organisation), related and supporting policies, its degree of confidentiality (any limitations on disclosure), the frequency of its review and the date it was last updated. The organisation should declare within its policy the importance it attaches to active risk management to support the realisation of its purpose, vision, strategic and business objectives, and implementation strategy. The policy should address the interests of all stakeholders, including shareholders, customers, suppliers, regulators and employees. It should set out and describe the accountability for risk management within the organisation. This will include describing the specific responsibilities of the board – and (depending on the size of the organisation) internal audit, external audit, the risk committee, the corporate governance committee, the central risk function, employees and third-party contractors – in implementing risk management. Where appropriate, it should describe the relationship between risk and corporate governance and internal audit. The policy is not the place to describe the risk management process; however, it should describe the policy's relationship to the process and the framework. In addition, ideally any standalone policy statement prepared for display (alongside, say, the health and safety policy and the business continuity policy), should be short, concise and lucid (and is commonly more effective when confined to a single page).

1.9.6 Risk Management Process

A way of exploring the mechanisms for implementing a risk management process is to break it down into its component parts and examine what each part should contribute to the whole. It is proposed here that the risk management process is broken down into seven stages: context, identification, analysis, evaluation, treatment, monitoring/review and communication/consultation. While activities follow a largely sequential pattern, it may be a highly iterative process over time. For instance, as new risks are identified, the earlier processes of

identification and analysis are revisited and the subsequent processes are repeated through to the implementation of risk response actions.

1.9.7 Sources of Risk

A way of examining the sources of business risk is to consider that risk emanates from two primary areas: from within the business itself (relating to the actions it takes) and from the environment or context within which the business operates (and over which it has no control). In Figure 1.2 these sources are labelled "internal processes (internal business context)" and "business operating environment (external business context)", respectively, to show the relationship with the international risk standard, ISO 31000 (2009). They are a development of the traditional PEST analysis (an abbreviation for the external influences called political, economic, social and technological).

1.10 SUMMARY

All businesses in a free market are exposed to risk. This risk exposure exists from their inception. However, there would appear to be a swell of opinion that says risk is now more complex, diverse and dynamic. In particular, the source of risk is broader and the rate of change of the sources of risk has dramatically increased. The emergence of ERM has come about from the desire and need to move away from managing risk in silos and identifying and managing risk interdependencies. This is not some startling new intellectual breakthrough but rather a practical solution to a practical problem. It is clear from surveys and the press that board members believe that ERM is important to business growth. Whatever strategy boards adopt, they must decide what opportunities, present and future, they want to pursue and what risks they are willing to take in developing the opportunities selected. Hence, whatever the approach businesses adopt for risk management, they must strike a judicious balance between risk and opportunity in the form of the contradictory pressures for greater entrepreneurialism on the one hand and the limitation of downside risks on the other. In the aftermath of a series of unexpected risk management failures leading to company collapses and other corporate scandals in the UK and overseas, boards are under greater scrutiny and expectations of corporate governance have significantly increased. Board members cannot distance themselves from risk management or believe that they will not be held to account. Risk management needs to be integrated with the primary activities of the board. There are a series of clearly recognised benefits of implementing risk management practice, when applied in a systematic and methodical way. A structure was described for examining ERM to understand the pressures for its development, its composition, implementation, the overall process and the sources of risk.

1.11 REFERENCES

Boulton, R.E.S., Libert, B.D. and Samek, S.M. (2000) *Cracking the Value Code – How Successful Businesses are Creating Wealth in the New Economy*. Harper Business, New York.

Combined Code (2003) *Combined Code on Corporate Governance*. Financial Reporting Council, July.

COSO (2004) *Enterprise Risk Management – Integrated Framework*, September. Committee of Sponsoring Organisations of the Treadway Commission.

Drucker, P.F. (1979) *Management, an Abridged and Revised Version of Management: Tasks, Responsibilities, Practices*. Pan Books, London.

Economist Intelligence Unit (2001) *Enterprise Risk Management: Implementing New Solutions*. EIU, New York.

Garratt, R. (2003) *The Fish Rots from the Head. The Crisis in our Boardrooms: Developing the Crucial Skills of the Competent Director*, revised and updated edition. Profile Books, London.

Hunt, B. (2001) Issue of the moment: The rise and rise of risk management. In J. Pickford (ed.), *Mastering Risk Volume 1: Concepts*. Financial Times, Harlow.

ISO (2009) *ISO 31000:2009 Risk Management – Principles and Guidelines*. International Organization for Standardization, Geneva.

Knight, R.F. and Petty, D.J. (2001) Philosophies of risk, shareholder value and the CEO. In J. Pickford (ed.), *Mastering Risk Volume 1: Concepts*. Financial Times, Harlow.

McCarthy, M.P. and Flynn, T.P. (2004) *Risk from the CEO and Board Perspective*. McGraw-Hill, New York.

National Audit Office (2000) *Supporting Innovation: Managing Risk in Government Departments*. Report by the Comptroller and Auditor General, 17 August. The Stationery Office, London.