

Part I
Enterprise Risk Management in Context

1

Introduction

Providing strategic direction for a business means understanding what drives the creation of value and what destroys it. This in turn means 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 is becoming greater, more complex, diverse and dynamic. This has arisen in no small part from rapid changes in technology, speed of communication, globalisation of business and the rate of change within markets. Businesses now operate in an entirely different environment compared with just 10 years ago. The source of risk can also come from within, as businesses strive for growth. The adoption of expansion strategies, such as acquisition, investment in emerging markets, major organisational restructuring, outsourcing key processes, major capital investment projects and developing significant new products, can all increase a business's risk exposure. A recent 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. The Economist Intelligence Unit (EIU) survey "Enterprise Risk Management, implementing new solutions" highlighted:

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. (Economic Intelligence Unit 2001)

As a consequence of the diversity of risk, risk management requires a broader approach. This sentiment was echoed by Rod Eddington, former 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.

1.1 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 as 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. Pattie Dunn, vice chairman of Barclays Global Investors and a member of the board of Hewlett-Packard, says:

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. It is a relatively new approach, whereby 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, but 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). It 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 that is the focus of this book.

1.2 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. For 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 1977).

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 feel, 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 that responded considered ERM could improve their price/earnings ratio and cost of capital. Organisations which 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.

1.3 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. 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 who state: "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 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 (Knight and Petty 2001). 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 action 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.

1.4 THE ROLE OF THE BOARD

Jay Keyworth, chairman of the Progress and Freedom Foundation and a member of Hewlett-Packard's board, has 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

6 Simple Tools and Techniques for Enterprise Risk Management

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, in the safeguards provided by external auditors and in the degree of risk management control. These 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 is discussed in Chapter 2. Clearly risk exposure was growing from an increasingly chaotic and turbulent world. The lack of risk management control resided 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 published *Standards for the Board*. It is proving to be a catalyst for the 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 clearly lays out four main tasks for directors:

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, and yet to stand back from the day-to-day management and retain an objective, longer-term view.
3. The board must be sensitive to the short-term, local issues and yet be informed of the broader trends and competition, often of an international nature.
4. 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:

- Appoint a C-level risk leader empowered not only with the responsibility, but 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 board members receive is accurate, timely, clear and relevant.

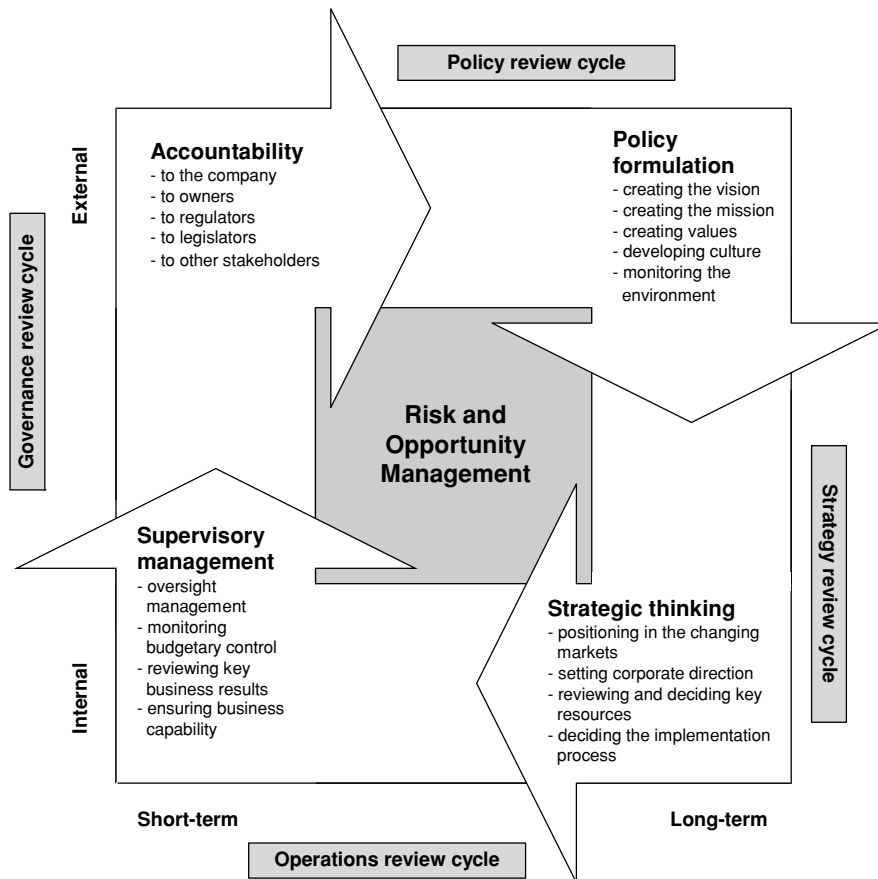


Figure 1.1 The role of the board and the integration of risk management. (Adapted from Garratt (2003)) Reproduced with permission from *The Fish Rots from the Head*, B. Garratt, Profile Books Ltd.

- 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 risk management remains focused on the most serious issues.
- Ensure risk management is embedded throughout the organisation.

As illustrated in Figure 1.1, risk and opportunity impinges 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 commit 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 processes. 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.

1.5 PRIMARY BUSINESS OBJECTIVE (OR GOAL)

The primary objective of a business is *shareholder wealth maximisation*, that 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 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. Wealth maximisation takes account of risks to long-term growth, whereas profit maximisation does not.

1.6 WHAT IS ENTERPRISE RISK MANAGEMENT (ERM)

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. Enterprise risk management 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, enterprise risk management 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, enterprise risk management may be defined as “a comprehensive and integrated framework for managing company-wide risk in order to maximise a company's value”.

1.7 BENEFITS OF ERM

No risk management process can create a risk-free environment. Rather enterprise risk management enables management to operate more effectively in a business environment filled with fluctuating risks.

Enterprise risk management provides enhanced capability to:

- *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. Management considers the business's risk appetite first in evaluating strategic alternatives, then in setting boundaries for downside risk.
- *Minimise operational surprises and losses*: Businesses have enhanced capability to identify potential risk events, assess risks and establish responses, thereby reducing 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 acceptance.
- *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*: Business's accept risk as part of wealth creation and preservation and they expect return 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. Responses need to be developed to seize these opportunities in the same way that responses are required to address identified threats to a business.

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

1.8 FRAMEWORK

A framework for understanding ERM is included in Figure 1.2 and is composed of five 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 shareholder’s investment and a 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 clear risk management process is required which sets out the individual processes, their inputs, outputs, constraints and enablers.
5. 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.

1.8.1 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 enterprise risk management because it provides the top-down monitoring and management of risk management. It places responsibility on the board

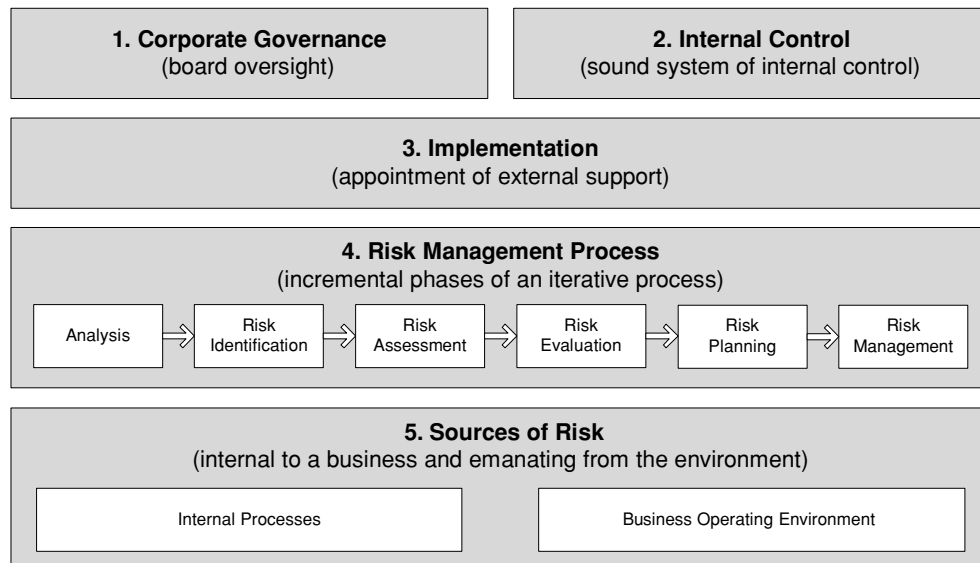


Figure 1.2 ERM framework

for ensuring that appropriate systems and policies for risk management are in place. Good board practices and corporate governance are crucial for effective ERM.

1.8.2 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 to either remove or reduce them or where appropriate transfer them to a third party where it is economic to do so.

1.8.3 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 study have to be mapped, communicated and agreed so that the timeframe, resources, costs, inputs and deliverables are understood.

1.8.4 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 six processes called analysis, identification, assessment, evaluation, planning and management. While activities follow a largely sequential pattern, it may be a highly iterative process over time. For as new risks are identified, the earlier process of identification and assessment are revisited, and the sequential process is repeated through to the implementation of risk response actions.

1.8.5 Sources of risk

A way of examining the sources of business risk is to consider that it emanates from two quarters, from within a business (relating to the actions it takes) and from the environment within which it operates over which it has no control. Within Figure 1.2 above, these sources have been labelled "internal processes" and "business operating environment". They are a development of the traditional PEST analysis (an abbreviation for the external influences called political, economic, social and technological).

1.9 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, 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 framework was described for examining ERM to understand the pressures for its development, its composition, implementation, the overall process and the sources of risk.

1.10 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 on Corporate Governance (July 2003), Financial Reporting Council, CCH.
- COSO (2004) *Enterprise Risk Management – Integrated Framework*, September, published by the Committee of Sponsoring Organisations of the Treadway Commission.
- Drucker, P.F. (1977) *Management, an Abridged and Revised Version of Management: Tasks, Responsibilities, Practices*, first published in Great Britain 1979 by Pan Books Ltd, London, 7th printing, 1983.
- Economist Intelligence Unit (2001) “Enterprise Risk Management, implementing new solutions”.
- Hunt, B. (2001) “Issue of the Moment: The Rise and Rise of Risk Management”, in *Mastering Risk Volume 1: Concepts*, editor James Pickford, Pearson Education Ltd, UK.
- Garratt, R. (2003) *The Fish Rots from the Head. The Crisis in our Boardrooms: Developing the Crucial Skills of the Competent Director*, first published in 1996 by HarperCollinsBusiness. This revised and updated edition was published by Profile Books Limited, London.
- Knight, R.F. and Petty, D.J. (2001) “Philosophies of risk, shareholder value and the CEO”, in *Mastering Risk Volume 1: Concepts*, editor James Pickford, Pearson Education Ltd, UK.
- 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, London, The Stationery Office.