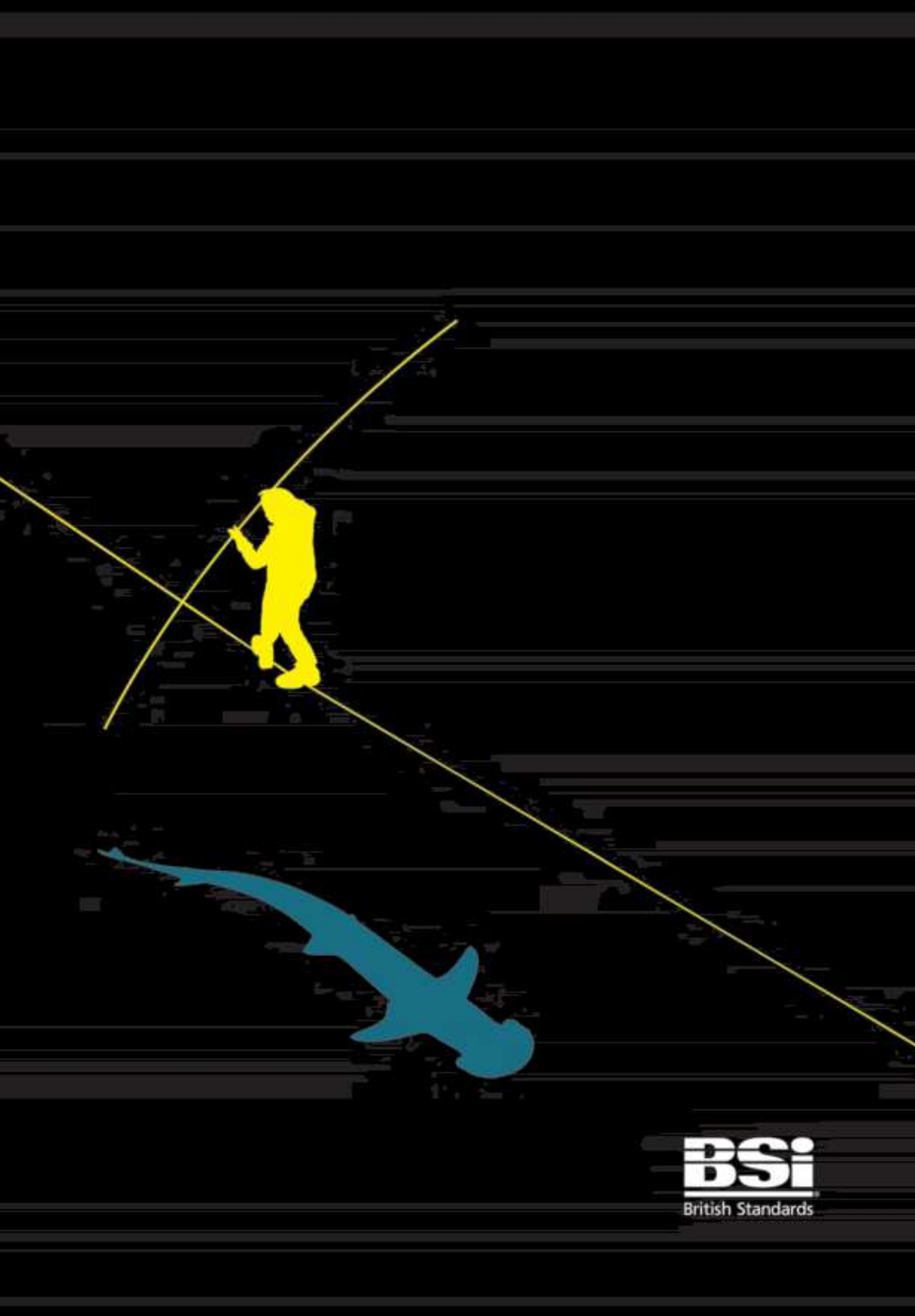


BSi
British Standards

Good Governance

A risk-based management systems approach to internal control

David Smith and Robert Politowski, iMS Risk Solutions Ltd

BSi®
British Standards

First published in the UK in 2000
Second edition published in the UK in 2008

by
BSI
389 Chiswick High Road
London W4 4AL

Typeset in Frutiger by Monolith – http://www.monolith.uk.com
Printed in Great Britain by The MFK Group, Stevenage

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN 978-0-580-64313-2

Contents

Foreword

This is a guide to how organizations can identify and manage their risks for good governance. Since the publication of PD 6668:2000, *Managing Risk for Corporate Governance*, upon which this book is based, there is a greater appreciation of the importance of risk management in organizations and society at large. All organizations take risks but as the 'credit crunch' of 2008 showed, these risks need to be balanced. They also need to recognize and manage those risks which, if realized, could prejudice the sustainability of the organization. The principles apply to organizations worldwide, in the private or public sectors, NGOs, as well as not-for-profit organizations. This book outlines a management framework for identifying the risks and opportunities, determining the extent of the risks, implementing and maintaining control measures and reporting on the organization's commitment to this process.

There have been a number of developments in the international and national management standards field since PD 6668 was published in 2000. These developments, including those on risk management (2008), occupational health and safety (2007), environmental management (2004) and sustainable development (2006), can help organizations with internal control for good governance. Although the principles in many of these documents are similar they do not use the same approach. This is unfortunate as there is an increasing demand for an integrated approach. An integrated approach that was developed in 2006 was PAS 99, *Specification of common management system requirements as a framework for integration*. The framework used in this book has elements in common with PAS 99 and helps support the holistic approach to risk management for internal control and good governance.

Acknowledgements

The authors would like to thank Chris Millidge for his help in drafting this document and Michael Faber for reviewing it for us and his helpful suggestions.

A risk-averse business culture is no business culture at all.

(Blair, 2005)

1. Introduction

This book provides guidance for organizations that wish to develop a framework for managing risk for good governance. Research by analysts demonstrates the positive link between good governance and organizational performance. In a recent study, the Association of British Insurers – major investors in public companies in the UK – found that 'well-governed companies will produce better returns for shareholders over time' (Association of British Insurers, 2008).

It is clear that well-managed organizations generally, whether in the public or private sector, are far more likely to satisfy stakeholders. The focus of this publication is about managing those risks for the sustainable operation of organizations using a management systems standard approach.

In this introductory chapter the background to governance and the organizations to which the approach is applicable are briefly reviewed. The chapter explains why the approach adopted is generally applicable and consistent with international management systems standards.

Background

The term 'corporate governance' came into general use following a number of major scandals and corporate failures in the late 1980s and early 1990s, and in the UK became enshrined in the report from the Committee on the Financial Aspects of Corporate Governance (the Cadbury Committee): 'Corporate governance is the system by which companies are directed and controlled' (Cadbury *et al*, 1992).

Such failures have occurred throughout the world and continue to occur, such as the crisis facing the global banking industry in 2008. The impact of these worldwide corporate failures had the potential to be of such a magnitude that there was the danger that the whole structure of the means of financing corporations might become threatened. The essence of the limited liability company is that external investors are willing to become shareholders, in the confidence that their interests will be safeguarded. Shareholders accept that not all investments will prove rewarding, but they are entitled to assume that there will be no mismanagement on the part of the directors and managers who are in day-to-day control of the corporation. If they cannot be confident that this is the case they will be unwilling to invest, and the basis of modern commercial activity will be under threat. Whilst an individual shareholder might have been willing to accept the risk, major investors such as insurance companies or pension funds began to demand that to safeguard the interests of their clients, there should be greater regulation of the behaviour of joint stock companies.

In 1999 the Organisation for Economic Co-operation and Development (OECD) produced a definition of corporate governance and a set of principles. These principles were revised in 2004 and at a high level comprise the following requirements of a corporate governance framework (Organisation for Economic Co-operation and Development, 2004a). It should:

1. *'…promote transparent and efficient markets, be consistent with the rule of law and clearly articulate the division of responsibilities among different supervisory, regulatory and enforcement authorities…';*
2. *'…protect and facilitate the exercise of shareholders' rights…';*
3. *'…ensure the equitable treatment of all shareholders, including minority and foreign shareholders. All shareholders should have the opportunity to obtain effective redress for violation of their rights…';*

4. *'…recognise the rights of stakeholders established by law or through mutual agreements and encourage active co-operation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises…';*
5. *'…ensure that timely and accurate disclosure is made on all material matters regarding the corporation, including the financial situation, performance, ownership, and governance of the company…';*
6. *'…ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's accountability to the company and the shareholders…'*

There are a number of sub-clauses to each of the main principles that cover specific areas.

There have been further definitions of governance and legislative powers in many countries around the world. These range from the voluntary code of practice approach as seen in the UK to the more prescriptive Sarbanes-Oxley Act (United States of America, 2002) – a response from legislators in the US to high-profile failures such as Enron and WorldCom.

Organization-wide risk management and internal control are important for the successful running of any business and should remain relevant over time in the continually evolving global business environment. The OECD principles specifically highlight board responsibility:

> *Ensuring the integrity of the corporation's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.*
> (OECD Principle VI.D.7)

This has led to the formal consideration of risk and the identification of it as a 'separate' aspect that can benefit from specific management arrangements. That is not to say that organizations have not previously recognized these risks, but simply that a formal and structured approach had not been a feature in many organizations.

The characteristics of many successful organizations tend to reflect an attitude and culture of identifying opportunities, recognizing the risks and managing them appropriately. There are upsides and downsides to the risks that come with every opportunity and it is necessary to select the right balance. Organizations that are risk averse are unlikely to thrive in the long term because of continual change in the market-place and social expectations.

Application of this approach

All organizations need to display good governance, whether they are corporate bodies, private entities, public bodies or charities.

In an increasingly complex world where stakeholders play an ever more important role there is the expectation of good governance and transparency. There are a variety of characteristics of good governance including promoting values in the organization, focusing on the purpose of the organization, effective performance, engagement with stakeholders and, most significantly from the perspective of this book, the management of risk.

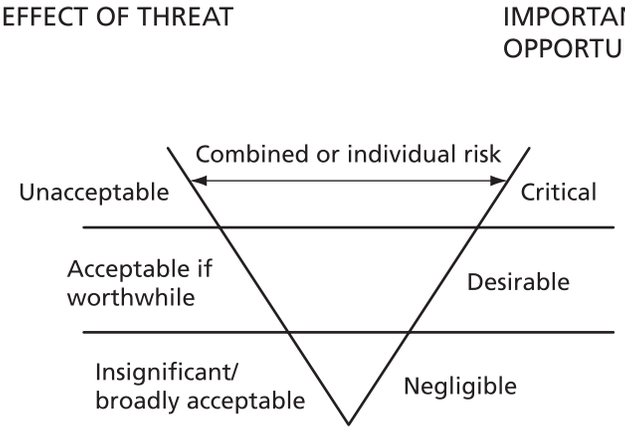
Many organizations need to manage a whole host of risks, for example:

— corporate organizations operate in an increasingly complex world with global impacts, international supply chains and informed public opinion expressing concern about social responsibility;
— public bodies have to determine the benefits of new technology against the risk of data loss;
— charitable bodies have to balance the risks of supporting international disasters against the risks faced by their workers and donors' concerns about misuse of aid;
— public bodies have similar accountabilities to their 'shareholders' – often taxpayers;
— charitable concerns need to assure their 'investors' that their donations are being applied to the purpose for which they were intended.

The principles of good governance equally apply to public bodies, charities, voluntary bodies, etc. There is a need for good governance of public bodies to reflect the need to ensure value for money, transparent decision making and reporting, proper codes of conduct, accountability and so on.

Despite the difference between the public and private sectors it is essential that people know for what they are responsible, and for what they are accountable.

There is also a drive for the public sector to be more creative and prepared to take more calculated business risks in order to deliver the best possible services to the public. The public and private sectors differ in this respect. The public sector needs good governance to enable it to take certain calculated risks, whilst the private sector needs good governance in order to manage the risks that are taken in everyday business. One way of expressing the relationship between threat and opportunity can be seen in Figure 1.1.



Source: BS 6079-3:2000

Figure 1.1 — Relationship between threat and opportunity

Public bodies need to direct and control their functions and nowhere can this be more clearly demonstrated than in local government. Local government bodies have a real need to relate to their communities in a similar manner to corporate bodies, and to demonstrate continuous improvement and value for money through outward-looking, accountable and responsive services.

Risk management and internal control should be included in all dimensions of public bodies such as:

— making public statements to stakeholders on the risk management strategy, process and framework, demonstrating accountability;
— the capability and capacity within the organization;
— mechanisms for monitoring and reviewing effectiveness against agreed standards;
— robust systems for identifying, profiling, controlling and monitoring all significant strategic, programme, project and operational risks;
— providing openness by involving all those associated with planning and delivering services, including partners.

All the above issues are equally applicable to charities, clubs, societies and associations. Large charitable concerns rely heavily on public donations to support their activities internationally.

There is clear recognition amongst boards of directors and investors – mostly those in the professional investment market – that there is a link between good corporate governance and organizational performance that is valued by stakeholders. There are a number of international ratings organizations that focus research on the development of scoring systems for ranking governance performance. This research is often used by professional investors to assist in making informed decisions to formulate an overall investment strategy, as a screening tool for analysts and portfolio managers and to adjust for governance risk when assessing credit risk, etc.

Additionally, companies themselves are beginning to use similar ranking research to help in their decision making, to reduce the chance of being targeted for shareholder action, to increase market trust in reported earnings, as a support in seeking lower borrowing costs, and in attracting highly qualified and experienced directors who can add value to the organization and achieve a higher market capitalization.

A management systems approach

Good risk management is an essential element of good governance and it is against this background that this publication focuses on a risk management framework to help organizations in applying the principles of risk management throughout the whole organization from the lowest operating levels to the board of directors.

It is clearly important that all aspects of corporate governance are managed in a holistic manner. This book focuses specifically on the important management of risk and the development of effective internal control mechanisms: Clause C.2 of *The Combined Code on Corporate Governance* (Financial Reporting Council, 2008) as expanded upon from *Internal Control – Revised Guidance for Directors on the Combined Code* (Financial Reporting Council, 2005).

Chapter **2** provides details of the scope and definitions used. A more detailed description of an approach to managing risks is given in Chapter **3**, which lays out a framework of the issues that should be addressed and follows a Plan, Do, Check, Act (PDCA) approach that is consistent with international management systems standards. This approach is based on the model given in PAS 99:2006 (The requirements included in section 4 of the PAS can be used as a specification against which organizations can be assessed by changing the word ‘should’ to ‘shall’.). Appendix B details the correspondence between this publication and the requirements of standards on quality, environment, health and safety and information security, by way of example.

Chapters **4** and **5** contain a practical guide to delivering business requirements with respect to risk management for good governance. Chapter **6** provides a questionnaire to enable organizations to carry out a self-assessment of their systems for governance.

A good management system will enable identification of risks, their management and help in any disclosure requirements for stakeholders. The aspect of disclosure is specifically highlighted in the OECD principles for governance, which additionally call for inclusion of material information on 'Foreseeable risk factors' (Principle V.A.6).

Figure 1.2 — Three key components for delivering effective corporate governance

Figure 1.2 shows a simple model of the interrelationship of the three main components of a risk management system for good governance. It is essential that the risks are identified and understood and decisions taken on how they will be managed.

A key feature of a management systems approach is identification of objectives and a programme for delivering the defined objectives. Many international management systems standards have differing approaches; PAS 99 provides a common approach for managing business risk requirements in an integrated manner. Many organizations already have management systems in place; meeting the requirements of these international standards and the approach builds upon these to ensure the benefits of existing systems can be utilized, eliminating redundancy and increasing efficiency.

However, good internal control and risk management systems will not succeed in delivering the organizational objectives unless the arrangements are embedded within the organization and individuals are committed to

Failure to identify risk of data loss

A government department was seeking to transfer personal data to another department in a short space of time. Effective procedures were in existence but the time and cost of removing the sensitive elements of the data was considered too great. As a result, when the data was lost in transit the personal details of many millions of people were lost.

The loss of this information has had many repercussions:

- *loss of confidence by the public in government departments handling confidential personal information;*
- *individuals whose details have been compromised;*
- *a possibility for fraudulent activity through the use of this information remains for many years to come.*

Charity and aid

Charity A was challenged by a government department that had made a grant for an aid project. The charity was asked to demonstrate that its governance procedures were effective in the delivery of aid as news media reports suggested that those supposedly receiving the aid had made claims that it was inappropriate for their needs and some had fallen into the wrong hands. This threatened to become a scandal and affect not only funding from government but also the many donations from members of the public who regularly made a significant contribution to overall funds. The need for an effective control framework and monitoring and auditing became obvious.

Financial turmoil

The turmoil in the financial markets in 2007 was a good example of the consequences of failing to recognize and manage risks. The failure of 'sub-prime' home loans in America led to failures in local banks. What would have been a local problem became international because large numbers of these sub-prime loans had been packaged up and sold to institutions around the world. The realization by investors that they had misjudged the risk of US mortgage borrowers led to a conclusion that risk had been underestimated in all kinds of debt markets, and banks were left with large amounts of unsellable debt. In the UK, mortgage lenders who were used to being able to borrow money when needed suddenly found that banks were no longer willing to provide the loans. A regional mortgage lender had grown substantially using wholesale money market borrowing which it was able to secure on very advantageous rates. The change in international money markets led to exposure to a shortfall in funding. Assessment of the risk and control of growth together with contingency arrangements should have prevented the collapse of the bank.

delivering their objectives – 'there has to be something in the lifeblood of the organization that persuades its people to do extraordinary things for it as well as for themselves' (Hillson, 2007).

2. Scope and definitions

Scope

The guidance given in this book outlines how an organization can implement effective arrangements for managing risk, to ensure that it meets its corporate governance needs. A PDCA framework is used, which is consistent with the approach in management systems standards produced by the International Organization for Standardization (ISO).

This guidance is applicable to any organization that wishes to:

— establish arrangements at top management level to identify, manage and mitigate risks;
— implement, maintain and continually improve its management of risks in a manner which is consistent with its policy;
— assure itself of conformance with this policy;
— make a self-determination and self-declaration of its performance on an annual basis.

There are a number of documents an organization may wish to refer to for further guidance within its particular country, sectors, etc; some are included in Appendix **B**.

Definitions

acceptable risk risk at a level that can be tolerated by the organization

audit systematic, independent process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

management system part of the overall management that includes organizational structure, planning activities, responsibilities, practices, procedures, processes and resources for developing, implementing, achieving, reviewing and maintaining the organization's policy

nonconformity non-fulfilment of a requirement

Note: a nonconformity can be any deviation from relevant work standards, practices, procedures, legal requirements, etc. (see BS EN ISO 9000:2005, 3.6.2 and BS EN ISO 14001:2004, 3.15).

organization company, corporation, firm, enterprise, authority or institution, or part or combination thereof, whether incorporated or not, public or private, that has its own functions and administration

Note: for organizations with more than one operating unit, a single operating unit may be defined as an organization (see BS EN ISO 14001:2004, 3.16).

risk effect of uncertainty on objectives

Note 1: an effect is a deviation from the expected – positive and/or negative.

Note 2: objectives can have different aspects, such as financial, health and safety, and environmental goals, and can apply at different levels, such as strategic, programme, project and operational.

Note 3: risk is often characterized by reference to potential events, consequences or a combination of these and how they can affect the achievement of objectives.

Note 4: risk is often expressed in terms of a combination of the consequences of an event or a change in circumstances, and the associated likelihood of occurrence (see BS 31100 (DPC) 2008).

top management person or group of people who directs and controls an organization at the highest level (see BS EN ISO 9000:2005, 3.2.7)

3. Risk management system

3.1 General requirements

An organization's top management should commit to establishing arrangements that will ensure that its risks are identified and effectively managed. It should establish a system that operates throughout the organization encompassing all the organization's activities.

Specifically the system should:

— have a defined scope;
— be documented, implemented, maintained, reviewed periodically for effectiveness and continually improved;
— ensure the availability of appropriate resources and communication of information to support it.

3.2 Policy

The top management in the organization should demonstrate commitment and develop a policy to focus on managing risk for corporate governance. This should lead to specific policies and arrangements to deal with specific risks. The corporate governance policy should reflect the commitment of the organization to its stakeholders. It should promote a positive culture within the organization for managing risk for good governance.

Specifically the policy should:

— reflect the nature and size of the organization, its activities, products and services, its position in the marketplace and the risks that it faces;
— commit to developing a culture to control risk;
— be communicated to all appropriate persons/organizations working for or on behalf of the organization;
— commit to comply with all relevant legal requirements, codes of practice and other requirements to which the organization subscribes;
— commit to ensuring that management competence is established to mitigate risks;
— commit to involving employees in identifying risks and their suggestions on the most effective methods of management;
— commit to internal control audits to verify the arrangements;
— commit to reviewing regularly the business risks faced by the organization to ensure that the arrangements are effective with a view to continual improvement;
— commit to reporting at least annually to stakeholders as appropriate.

3.3 Planning for risk management

Risk identification, assessment and control

The organization should establish a process for identifying those risks to the business that may impact upon organizational objectives, assessing their impact and applying controls where necessary.

Risk identification

The process should consider, amongst other things, the risks (including opportunities) that arise from:

— day-to-day operations;
— market developments;
— political changes;
— natural disasters;
— socio-economic changes;
— technical developments.

Risk analysis and evaluation

A process should be established for risk assessment that takes account of:

— exposure to the risk (on a scale of rare to continuous);
— probability, taking into account the management controls in place;
— impact, should the risk be realized.

Deciding how the risks are to be managed

Each identified risk should be considered and decisions made to:

— accept – no action;
— avoid – avoid activities that give rise to the risk;
— adopt – adopt measures for containment and/or mitigation;
— change – change the nature, magnitude or consequences;
— seek – search for ways of exploiting the risk;
— transfer – options such as 'sharing risk' with other parties/insurance.

Arrangements should be put in place for those risks that are not acceptable.

Although ultimate responsibility for risk management will lie with top management, those risks identified as requiring control, which may be included in the management programme, should be cascaded in the form of policies, objectives, targets and operating procedures as appropriate to the relevant level in the organization.

Note: some risks may need to be controlled at strategic level, and may not be included in the management programme.

Identification of compliance and stakeholder requirements

The organization should establish, implement and maintain arrangements to determine the legal requirements, codes of practice and stakeholder requirements that it has to satisfy with respect to its activities, products and services. International requirements to meet the demands of different markets should be considered in the assessment.

Contingency planning

The organization should establish and maintain arrangements for identifying and responding to any unplanned event, potential emergency or disaster. The arrangements should seek to prevent or mitigate the consequences of any such occurrence and maintain business continuity.

Objectives and management programme

The organization should establish measurable objectives taking into account:

— business objectives;
— brand value and reputation issues;
— legal requirements, codes of practice and stakeholder requirements;
— contingency and continuity plans;
— financial requirements;
— market opportunities;
— the supply chain.

The organization should establish, implement and maintain a programme to achieve these objectives at the appropriate function, location and level within the organization.

Organizational structure, roles, responsibility, accountability and authority

The ultimate responsibility and accountability for managing risks faced by the organization lies with top management. Top management should be accountable and should ensure that individual roles and responsibilities are defined and understood at each level where control needs to be exercised and that the necessary training has been provided. All those with management responsibility should demonstrate their commitment to the risk management control measures, fostering a positive culture for risk management throughout the organization.

The organization should ensure that those persons to whom responsibilities are assigned have the necessary authority to act when required, and that their roles and responsibilities are documented and communicated both up and down the organizational structure.

3.4 Implementation and operation

Operational control

The organization should identify the specific operational control arrangements that are necessary to meet the organization's risk management policy and objectives as well as compliance and stakeholder requirements.

To ensure that these control arrangements are effective, the organization should:

— stipulate the operating controls and conditions;
— establish and maintain documented procedures for use in situations where their absence could lead to deviations from the policy and objectives;
— maintain the systems and infrastructure to ensure effective operational control.

Managing resources

The organization should ensure that personnel are competent on the basis of appropriate training, skill and experience to undertake the duties and tasks assigned to them.

At every level within the organization managers should regularly evaluate the effectiveness of actions taken to ensure competence.

The organization should ensure that its personnel are aware of the relevance and importance of their activities and how they contribute to the achievement of the objectives.

The organization should ensure that adequate resources (including finance) are available. These are resources that affect the operation and maintenance of infrastructure, plant and facilities that have an impact on the organization's arrangements for control of its risks, and associated documentation.

Documentation

It is important that the organization has some way of documenting or recording its arrangements and of controlling documents. The organization should establish and maintain information in a suitable medium, which describes the core arrangements and gives direction on related documentation.

The documentation should include:

— a description of the system;
— a statement of policies and objectives;
— documents determined as necessary to ensure effective planning and operational control.

Records should be established, documented and maintained to provide evidence of conformity to requirements. Records should be maintained of:

— each risk identified and considered;
— the decisions taken on any control measures;
— the names of the personnel who identified and considered the risk and who authorized the decision on the appropriate management action;
— the name of the person assigned as the risk owner.

Communication

The organization should establish appropriate procedures and/or systems for ensuring that pertinent information is communicated and recorded:

— to and from employees;
— to and from other stakeholders.

The aim should be transparency, in line with current regulations recognizing that full disclosure may not always be possible because of the commercial sensitivity of the risk.

3.5 Performance assessment

Monitoring and measuring

To demonstrate that internal control arrangements are effective, the organization should implement a monitoring and measuring regime of relevant operational controls. The process should be proactive and should:

— determine the extent to which applicable requirements are being met;
— monitor the effectiveness of controls;
— include the recording of information to track performance;
— evaluate conformance with the organization's objectives.

Evaluation of compliance

The organization should carry out periodic evaluations of compliance with legal requirements, regulations, codes of practice and other requirements to which the organization subscribes.

Internal audit

The organization should establish and maintain an audit programme and procedures for periodic system audits to be carried out. The basis of the audit programme should be determined by the significance of the risk and the organization's performance in the management of its risks, in order to:

— determine whether or not the risk management system:
  – conforms to planned arrangements;
  – has been properly implemented and maintained; and
  – is effective in meeting the organization's policy and objectives;
— review the results of previous audits;
— provide information on performance to top management.

Audits should be undertaken by competent personnel and, wherever possible, conducted by personnel independent of those having direct responsibility for the activity being examined.

3.6 Improvement

General

Top management should strive continually to improve the management of risk in the organization. It should take into account:

— audit results;
— analysis of performance data;
— corrective and preventive actions;
— loss events and near misses;
— management review;
— lessons learnt.

Analysis and handling of nonconformities

The responsibilities for handling nonconformities and reporting should be defined by top management.

The organization should establish arrangements for:

— reviewing actual or potential nonconformities;
— determining the root cause;
— evaluating the need for appropriate action to be taken.

Any subsequent changes that could have a major impact should be reviewed by top management before implementation to ensure that they do not introduce a new risk or compromise existing internal control measures.

3.7 Review

Management review

The organization's top management should, at planned intervals, review the risk management system and arrangements to ensure their continuing suitability, adequacy and effectiveness. The management review process should ensure that the necessary information is collected to allow management to carry out this evaluation. Records of the management review should be retained.

Note: in some organizations the management team may report to an executive board, committee or individual.

Input

The input to the management review should include:

— results of audits;
— feedback from stakeholders;
— status of any remedial actions;
— follow-up actions from previous management reviews;
— changing circumstances, including developments in legal requirements, codes of practice and other requirements, related to the organization's risks;
— recommendations for improvement;
— data and information on the organization's performance;
— relevant changes in the external environment or market-place.

Output

The output from the management review should include any decisions and actions related to:

— improvement to the effectiveness of the risk management system;
— improvement related to stakeholder requirements;
— resource needs to enable improvement.

Reporting

Top management should report to shareholders and/or stakeholders. This should include assurance that it has taken measures, through internal control, to manage the risks faced by the organization. It may not be possible to divulge the nature of some risks and control measures for reasons of commercial sensitivity unless there is a regulatory requirement to do so.

4. Implementation of a risk management system

General

This chapter is provided to give guidance on implementing an effective risk management system for meeting corporate governance requirements. Guidance is given only in those areas where it is thought additional explanation is necessary and would be helpful to the reader.

Establishing a risk management strategy

Reference is often made to 'strategic' risks, implying that there is only one category of risks that could have a major impact on the organization and, by implication, that there are other classes of risk of less significance. This distinction is erroneous. There are numerous cases where operational errors at the lowest level have produced catastrophic consequences that threaten the whole organization. The management of risks at all levels is equally important. It is certainly true that a board of directors may take decisions which have associated risks that are certainly strategic. If, for example, the board decided to close all its UK operations and operate from offshore call centres, that would certainly be a strategic decision that involved risks, which may accordingly be categorized as strategic risks. If, on the other hand, a junior employee made a mistake at operating level which resulted in the whole plant being burned down, the consequences would clearly involve strategic decisions even though the original risk would not have been classified as strategic.

It is important to understand that, although different risks may be managed at different levels within the organization, there should be an overall strategy for risk management. This should be established by top management in the organization, whether it is in the private or public domain. The strategy for managing risk within the organization cannot be developed in isolation. It should be developed along with, and support, overall organizational strategy. Furthermore, the strategy should recognize that the organization does not exist in a vacuum and for the risk management strategy to be effective account should be taken of both internal and external forces and stakeholders. When formulating strategy, top management should ensure it is aware of stakeholder expectations and, where appropriate, should either include representation for the stakeholders or have access to their input.

Trading losses

A large multinational bank, Bank A, with a substantial investment banking arm allowed traders to make substantial trades over which there was ineffective control. The discovery of large losses that a trader had sought to hide led to some of the largest losses ever recorded with repercussions around the global financial markets. This situation had occurred before when the actions of a single trader led to the collapse of Bank B. Although Bank A was aware of the previous history it failed to implement adequate controls to prevent suffering a similar problem.

General system requirements

If an organization is to introduce a system of risk management successfully, the organization should be one that is ready to accept change. In this context, 'successfully' implies more than having a formal system in place. It also expresses a system that is working to the extent that the management and all stakeholders feel confident that:

— foreseen risks are being managed; and
— unforeseen risks are prepared for.

The successful management of change – and risk – in an organization depends upon the values and behaviour patterns that form the culture of the organization.

Policy

Top management should demonstrate the leadership and commitment necessary for the effective implementation of its governance and risk management arrangements, and their continuing operation and improvement. The development of a high-level policy should assist in achieving a consistent approach throughout the organization. A well-written policy can be communicated effectively to all levels of the organization and should reflect the nature and scale of the organization and its risks.

Although there needs to be a risk policy in line with that set out in Chapter 3 (see p. 9), there will almost certainly need to be policies and arrangements to deal with specific risks that arise through regulatory requirements or from stakeholders, e.g. listing rules, contractual requirements or occupational health and safety legislation. Consistency within the various policies is important.

As a general rule the risk policy will establish an overall sense of direction and principles for risk management within the organization. The policy should be 'owned' by a member of top management although the top management team bears collective responsibility for overall policy, and there may be individual responsibility for management of specific governance risks. Where appropriate the policy should be developed in conjunction with relevant stakeholders and reviewed at least annually.

Planning risk management for governance

A process is needed for identifying risks, assessing them and managing them; it should be appropriate to the board's policy and objectives. In simple terms the following need to be addressed:

— What could go wrong (or right; risks can be positive as well as negative)?
— How likely is this to happen?
— What would be the consequences if this did arise?
— Are these consequences sufficiently significant to call for action to reduce or exploit the risk?
— What action should be taken to reduce the risk to an acceptable level?
— Is there the authority to take this action, or does it need to be sought at a higher level?

In organizations that have not previously carried out a process of risk identification and management, this will be a new requirement involving training so that every manager regards it as part of the routine business of managing his or her department.

Process for assessing and responding to business risks

A process for risk management is shown in Figure 4.1.

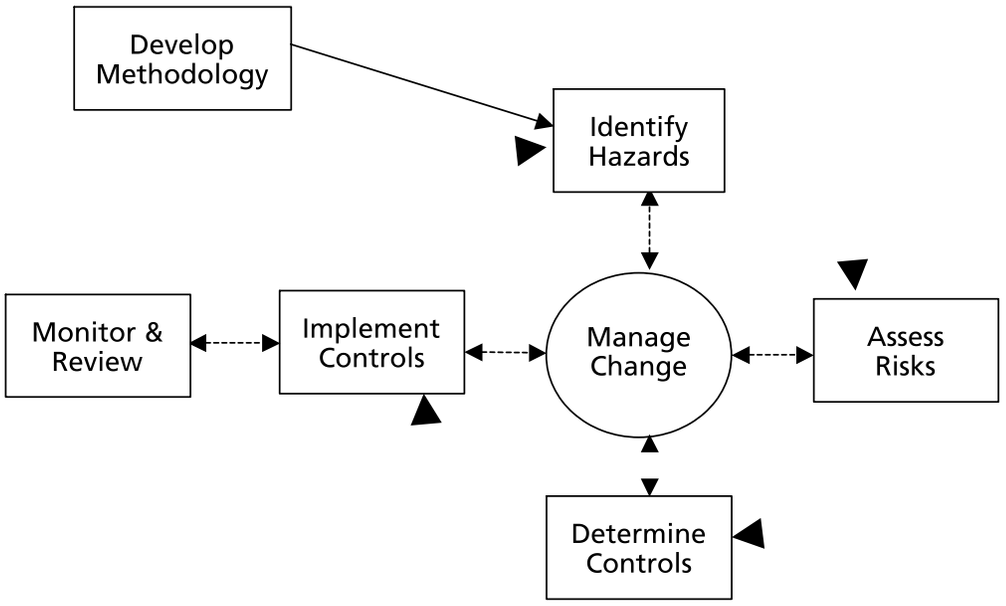


Figure 4.1 A process for risk management

The organization should establish a methodology for identifying risks to the organization that have the potential to affect the achievement of objectives. This process should ensure that these risks are fully understood, assessed, prioritized and controlled.

Develop methodology

There is no single methodology for identification of risks that will suit all organizations and it is important that organizations choose something that is appropriate to their nature and size and also meets expectations in terms of the detail of output, complexity, time and costs.

Identify the risks

Identification of risk can be extremely complex depending upon the nature and scale of the organization and its field of operation. Whatever methodology is chosen it is important to address both positive and negative aspects of risks and ensure that the validity of assumptions is fully tested. The process of risk identification is of paramount importance to the organization for identifying opportunities.

In order to identify risks pertinent to the organization a variety of techniques may be employed. A list of such approaches is given in BS 31100 – see Appendix A of this book.

Sources of information can include:

— professional/trade bodies;
— government;
— regulators;
— insurers;
— public information/media on problems experienced by similar organizations.

There are many activities that can give rise to significant risk. Some examples are given below; the list is not intended to be exhaustive.

— fraud;
— unethical dealings;
— product and/or service failure;
— public perception;
— lack of business focus;
— exploitation of workers and/or suppliers;
— environmental mismanagement;
— occupational health and safety mismanagement and/or liability;
— regulatory action;
— civil action;
— failure to respond to market changes;
— failure to control industrial espionage;
— failure to take account of widespread disease or illness amongst the workforce;
— failure to compete;
— failure to adopt new technology;
— failure to invest;
— failure to control IT effectively;
— failure to establish a positive culture;
— vulnerability of resources (material and human);
— failure to establish effective contingency arrangements in the event of a product and/or service failure;
— failure to establish effective continuity arrangements in the event of a disaster;
— inadequate insurance provision.

Any one of the above can damage an organization's reputation. Loss of reputation is one of the greatest potential impacts faced by an organization. It can have catastrophic effects in the short-term, and long-term consequences.

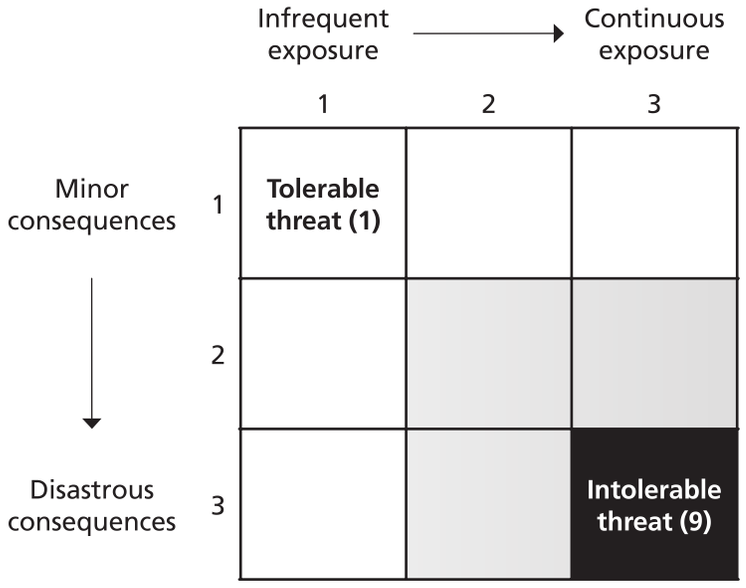
It is important to remember that where an organization operates in many different countries and cultures the identification process should take on board any relevant requirements that are specific to the location.

Analyse and evaluate the risks

A process should be established to identify the likelihood of the risk being realized and the consequence of such an event, so that the risks can be prioritized. The process of identifying threats may give rise to a long list of possibilities. Clearly it is not sensible to tackle all these at one time even if they could be realized as risks. The organization should establish what the consequence would be if the risk was realized. If the outcome is minor then the evaluation process should be deferred in favour of those threats with more potentially disastrous outcomes.

Having identified the possible outcome, the risk should be evaluated as to its frequency. Those risks that have continuous exposure should be viewed as having a higher priority than those with infrequent exposure. There are many processes for identifying risk, but one way of ranking these two dimensions is to use a simple matrix as shown in Table 4.1. Those risks that are considered unacceptable should be prioritized for further evaluation.

Table 4.1 Matrix for threat assessment



This method prioritizes risks that would give rise to significant problems in the organization if they were to occur. It does not identify whether the risk is likely to be realized.

The organization should identify the likelihood of the risk being realized, bearing in mind the internal controls in place and the appetite and culture of the organization with regard to the management of risks.

The organization should evaluate its prioritized risks and the likelihood of their being realized in two ways:

1. with the necessary management and internal controls embedded in the culture of the organization; and
2. in the absence of internal controls embedded in the organization.

The risks can be evaluated as shown in Table 4.2.

Risks identified as unacceptable and which may have a significant impact upon stakeholder expectations should be dealt with as a matter of priority in order to demonstrate good governance.

Table 4.2 Matrix for risk assessment

	Excellent control measures embedded in culture → Negligible control measures		
Minor consequences and infrequent exposure etc. ↓ Disastrous consequences and continual exposure			
1 - 3	Tolerable		
4 - 6			
9			Intolerable risk

Decide how the risks are to be managed

The strategic risks that top management includes in the risk management programme should be cascaded in the form of policies, objectives and targets, as appropriate, to the relevant level within the organization. A management system model may be a mirror (daughter) of the overall strategic model, as shown in Figure 4.2.

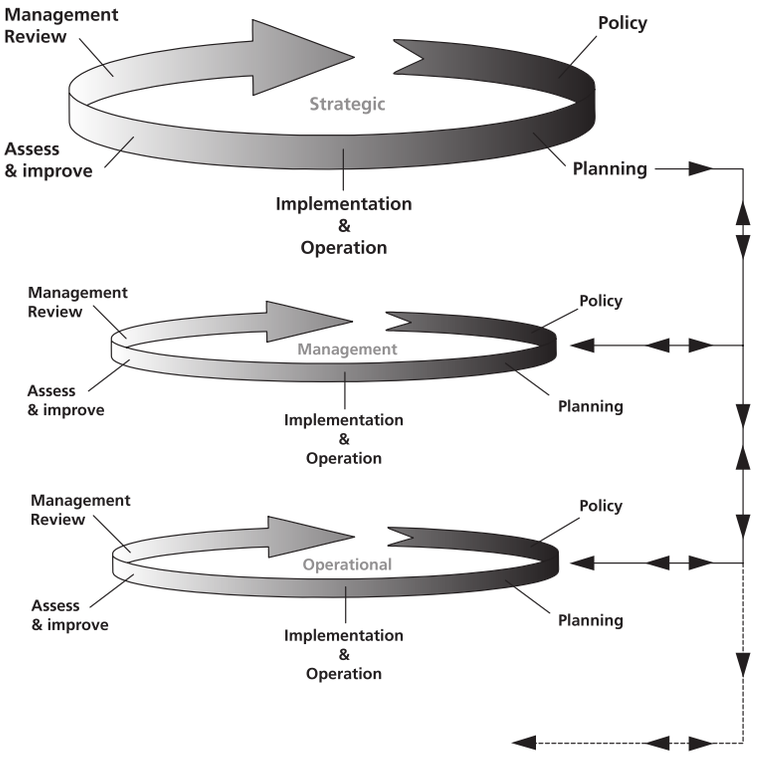


Figure 4.2 Management system model with daughters

Plan for the management of individual risks

Each identified unacceptable risk should have arrangements in place for dealing with the risk as identified in the previous chapter (see p. 9). In order to do this the organization should ensure that it has a plan that is consistent with its policy(ies), objectives and targets. This can be achieved using a mirror management system as shown in Figure 4.2. Alternatively, an integrated system or other arrangements that are considered satisfactory by the organization should be used. The arrangements should be documented to allow audit.

Compliance and stakeholder requirements

Many countries have now introduced a variety of regulations and/or guidance outlining the requirements for corporate governance within their jurisdiction. All organizations will have to take into account any relevant territory-based requirements when developing arrangements for controlling risk, in addition to possible sector-based regulations or expectations. This is an area that is of even greater importance to an organization that has operations in more than one country as there may be specific control arrangements for a particular country or, in some cases, particular stakeholders.

There needs to be a process in place for identifying what requirements, legal, guidance or otherwise, apply in the sphere of operation of the organization as well as any new or forthcoming requirements.

Contingency planning

An organization should make arrangements to deal with any foreseeable emergency and implement contingency arrangements for prevention or minimization of the consequences. Emergency situations can arise from both the organization's own activities and from external events over which the organization has little or no control or influence.

The organization should consider its range of activities, including products or services, to determine if there are situations, no matter how unlikely, that it should plan to mitigate in the event of an emergency. Aspects that should be considered are:

- Has a list of potential emergency situations been compiled?
- Has a contingency response team been established?
- Has there been consultation with all senior managers to contribute to this list?
- When considering each emergency situation have the consequences been documented, and the likelihood of occurrence (i.e. the risk) assessed and categorized?
- Have plans been developed for business continuity with procedures issued and tested regularly?

In order to mitigate the effects on all stakeholders it is essential that the board sets in place procedures and plans that anticipate that things can go wrong so that it can take planned and rehearsed steps to protect the business.

A guide on business continuity has been published by BSI: BS 25999-1:2006, *Business continuity management – Part 1: Code of practice*.

Objectives and management programme

Top management has a responsibility to shareholders, investors, staff, etc. to define and rank effective and measurable objectives for the organization. These objectives should be determined from the risk identification process, contingency plans, stakeholder requirements and the overall business planning. Objectives selected should take into account resources available; a simple but well-recognized methodology is the SMART process: objectives that are specific, measurable, achievable, realistic and time-orientated.

The organization should develop a strategic plan for managing those risks that have been identified as needing control. The programmes developed for achieving the objectives needs to be established with appropriate personnel who have the necessary accountabilities, responsibilities and resources.

Organizational structure, roles, responsibility, accountability and authority

Establishing the appropriate structure and accountability is essential if the policy and objectives are to be achieved and a climate for good governance created. The organization should establish the owners of particular risks and have a structure in place for managing those risks it has identified as needing control.

Organizational structure

Structure is closely related to leadership and decision making. The extent to which the organization is decentralized and managers are held accountable and rewarded for success (and sanctioned for failure) affects the culture. The willingness to take risks is an example. The organization should recognize this and ensure that the structure and the accountabilities, the freedom to act and resources are appropriate for effective operation, and develop policies, guidance and frameworks that support this.

The structure should reflect how individual risks are managed within the operation of the organization; see Figure 4.3.

Source: Hillson, 2007

Figure 4.3 Corporate governance organogram

Although a certain part of the organization (divisions, functions, etc.) may be assigned ownership of a risk it may well be necessary for other parts of the organization to be involved for a pan-organizational risk governance system to be effective.

There may be a need for specific arrangements for dealing with certain areas/disciplines of risk, e.g. health and safety and information security. One way of managing this requirement is to have supportive management systems to the overall risk management framework. Despite the fact that the organization has sought input from experts in these individual areas the board should recognize that it has overall accountability for the management of the specific risk area. Where necessary, additional training/guidance should be provided at board level to ensure the management of the risk is effective and meets organizational accountability and policy objectives. Where risks are managed by specialists in an independent manner, it is important that the board recognizes the danger that there is the possibility that a coherent organizational strategy for dealing with risk will be undermined.

Establishing ownership of risk

The management of risks should be cascaded as appropriate within the organization. Some risks should be discussed, prioritized and actioned exclusively at top management level. The internal controls and any actions may be treated in secrecy because, for example, of the sensitivity of the risk or for security reasons. The risk classification process and more specifically the controls required should help in determining where risk is best managed. Although top management may identify the risk, it may be that it is managed at middle management and/or at operational level; see Table 4.3.

Table 4.3 — Cascade of risk management system

Operational level	**Responsibility**		
	Top management	Middle management	Operational
Strategic	✓		
Strategic/management	✓	✓	
Strategic/management/operational	✓	✓	✓
Management		✓	
Management/operational		✓	✓
Operational			✓

For example, the organization may have determined that not maintaining security of its site during non-operational hours is a significant risk. The control is the employment of a subcontracted security company. Top management has identified this risk and allocated accountability within the organization, but day-to-day responsibility will have been assigned at a more junior level, where control of the outsourced function is managed.

In contrast, health and safety management will have to be controlled throughout the organization. Some market risks will be handled at a senior level and will not be cascaded.

Implementation and operation

General

The control measures necessary for meeting the policy and objectives should be implemented, ensuring that the necessary arrangements, documents and resources are in place.

There is also a need to instigate the monitoring procedure to verify and validate that what should be happening really is happening.

Building capability for effective risk management requires a strategy that takes into account the organization's present position and appetite for risk, and the relation to organizational objectives. It is, unfortunately, commonplace to find that these strategies focus upon risk as having a possible adverse effect on organizational performance, and a 'source of risk' as a threat to ongoing and planned activities.

It is essential to view risk in the widest possible interpretation and the outcomes are not always a threat. An appropriate understanding might be:

> *Risk is something that might happen which could have either negative (threats) or positive (opportunities) effects on the achievement of objectives.*

When risk management within an organization becomes primarily a threat-focused activity it tends to foster the development of specialists who focus on specific classes of threat (for example, health and safety, security, legal and treasury staff). This in turn can lead to the creation of organizational silos in which the specialist develops a position totally disproportionate to their importance, separated from line management decision making, rather than one that is fully integrated into all management decision processes.

It is important to remember that resources for the management of risk are always limited and every organization has to be wise in the manner in which it deploys its resources to maximum effect. Cost-effective approaches to creating risk management capability within the organization can often be achieved by focused, incremental developments, targeting the specific areas where effective management of risk matters most and where the improvement in the decisions taken by management can have the greatest impact.

It will be impossible for any organization to develop effective capability in risk management without involving the workforce and convincing it of the value of what is being put in place. There have been many instances where poor operational control has led to catastrophic failures. In many cases the risks had been identified and control measures implemented; the failures were due, at least in part, to a poor culture within the organization.

The role of culture in the strategic management of organizations is important because:

- the prevailing culture is a major influence on current strategies and future changes; and
- any decisions to make major strategic changes may require a change in the culture.

Culture is, therefore, a vital element in both strategy creation and strategy implementation. The model in Figure 4.4 demonstrates the influence that culture and values have within organizations.

When creating a climate for a culture that values people for the contribution they can make to the business, it is necessary to ensure that effective mechanisms exist for involvement of the workforce. In many areas of 'risk management' there is much evidence

to suggest that the involvement of the workforce in a meaningful way can have a positive impact upon risk even at the lowest levels in an organization. Each organization is different and there can be no single model for effective involvement of the workforce. However, some general principles that can be adopted are outlined below.

— *Leadership* – demonstrating commitment, and setting organizational vision, objectives and goals.
— *Provision of information* – sharing information with employees. The provision and exchange of information and instructions enables the organization to function efficiently and employees to be properly informed about developments and training.
— *Consultation* – management and workers or their representatives jointly consider issues of mutual concern with a view to identifying risks and seeking acceptable solutions to problems through a genuine exchange of views and information.
— *Involvement and participation of the workforce in joint problem solving* – effective worker involvement is more than provision of information and consultation and can lead to joint problem solving, which offers employers and workers an even greater level of involvement.

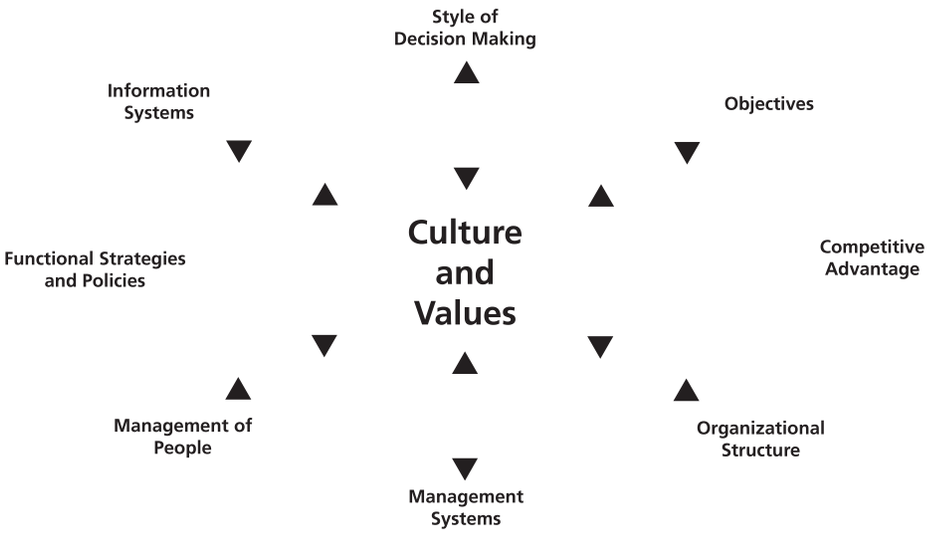


Figure 4.4 The influence that culture and values have within organizations

Consultation with the workforce will enable the organization to consider some areas in which risk should be more appropriately managed and, working with the workforce, embed a positive attitude towards risk management in the organization by incorporating it into each individual's job description. This will enable individuals at all levels within the organization to understand the risks that relate to their role and activities and how the management of them can contribute both individual and organizational goals and objectives. It will further the development of an appropriate risk management culture within the organization and foster an understanding of how individuals can contribute to continuous improvement of risk management. Provision should be made for protecting those who raise issues of concern where the individual feels the organization is not taking adequate precautions to mitigate the risk.

Contractor problems

Small- and medium-sized enterprises (SMEs) have an equal need to apply governance principles to their organization, particularly when this is a requirement or expectation of contract tendering.

A local contractor working in a school failed to control the activities of an apprentice working under inadequate supervision. Whilst unsupervised the apprentice was able to access the school IT network and used it to access the internet, communicating with indiscrete outside parties. When the matter came to light the contractor was suspended from the approved contractors' list and the member of staff responsible dismissed.

However, the involvement of the workforce at all levels in the organization can in no way diminish the accountability of top management for the management of risk. In addition to using the 'eyes' of the workforce in improving risk management throughout the organization, management should ensure that there are strong and effective processes for internal control and the management of risk. These controls need to be embedded within the organization.

Managing resources

Identifying resources

The organization should clearly identify and commit the resources necessary to deliver the policies, objectives and targets it has established, including:

— people;
— infrastructure, machinery, plant, etc;
— finance, investment, etc.

The organization should commit those resources that are essential to the implementation, control and improvement of the risk management arrangements.

There will always be financial limitations and possibly human resource factors (numbers, time and skill sets) that have to be taken into consideration. These may affect the priority in which tasks are tackled.

People

The organization should establish whether people are committed and capable of managing the risks that have been identified and where individual personnel are expected to enforce controls.

However, it should be recognized that an organization may be vulnerable to the inappropriate actions of an individual employee who can do untold damage – consider the collapse of Barings Bank. For this reason, there needs to be recognition of the importance of individuals and the vulnerability of the organization to those individuals.

Establishing appropriate competencies and behaviours

Commonly, organizations arrange training without fully establishing the needs of the organization or the individual. Failure can occur through one individual either being incompetent or failing to demonstrate the

appropriate behaviour. Organizations should ensure that those responsible for establishing, implementing and managing governance have knowledge and understanding of:

— strategic planning;
— legal requirements;
— agreements and contracts;
— organization;
— communication techniques and/or information management;
— involvement and motivation;
— education and continual professional development;
— continuous improvement and/or analytical techniques;
— evaluation and monitoring;
— delegation and/or equal opportunities;
— resource management.

Organizations should provide detailed specifications of the performance that employees are expected to achieve, based on the knowledge and understanding required to deliver positive task outcomes.

Organizations should also establish behavioural standards to underpin their competency framework. An example of management competency is shown in Table 4.4.

Table 4.4 An example of management competency

Competency	Behavioural characteristic(s)
1. Acting in an ethical manner	Shows integrity and fairness in decision making
2. Analysing information and taking decisions	Defines processes by task and activity Takes realistic decisions for a given situation Demonstrates an ability to identify patterns from events and data where there is no obvious relationship

Performance – towards a culture of good governance

Achieving success in an ever more complex and competitive global market-place is becoming increasingly challenging. The speed of change is accelerating, there is a consequent lack of organizational history as a reference point and the boundaries between organizations are

Safety and environmental incidents

A multinational oil exploration and refining organization, which typically performed well on the financial market and attracted ethical investors, experienced major failures with both safety and environmental incidents. These incidents received global media exposure and adverse comment about the board and its commitment to the management of these operational risks. Investigators pointed to a lack of internal control and poor cultural issues as having a large part to play in the incidents and, at a time of escalating oil prices, its stock market performance was poor.

becoming progressively more blurred. It is important that organizations develop a culture of performance and this is equally applicable to a commercial organization, a hospital or a charity, and the backbone in achieving the desired performance is the workforce.

Clearly, if members of the workforce are to be enthused about their responsibilities for managing risk within their roles and linking their activities directly to the overall performance of the organization, there has to be some sort of mechanism for providing appropriate reward. This is often achieved through a performance management process that links individual reward to achievement of individual objectives that support overall organizational objectives.

Performance management is a process, or set of processes, which should enable organizations to achieve their objectives. It should first establish shared understanding between managers and their staff about what is to be achieved. Then it should encourage management and development that increases the probability of achieving short- and long-term goals.

Outputs from effective performance management should be the communication and reinforcement of organizational strategies, values and norms. Most importantly, it enables the integration of individual and corporate objectives. It can also be a conduit to enable expression of individuals' views about achieving current goals for their team or department.

Features of good performance management are:

— that it is a continuous process, not an annual event;
— the communication of vision, objectives and strategy;
— that it is subjected to regular evaluation;
— that use is made of existing processes for objective setting and work planning;
— top management commitment;
— line management understanding and commitment;
— cultural commitment.

Managing other resources

A whole range of resources is required for the effective running of a business. Some considerations might be:

— *buildings, workspace and associated utilities*
The provision of infrastructure to meet needs is an obvious requirement but it is sometimes forgotten that buildings, work areas and support facilities need regular maintenance, replacement, cleaning, etc. You need to provide for reviewing the infrastructure in the broadest sense, bearing in mind technological changes, workplace expectations, changes in workload, and reliability, consistency and other quality aspects.
— *process equipment (both hardware and software)*
The point about infrastructure is particularly important in respect of hardware and software, which date very quickly. Reliance on computers increases the risk of accidental loss of data, which is a serious danger.
— *supporting services (such as transport or communication hardware)*
Transport services are also sometimes not seen as a core issue. However, they can impact on the environment through poor environmental specification

and there are occupational health and safety issues related to transport: driver hours, carriage of dangerous loads, training, the type of vehicles used or poor maintenance.

Documentation

It is important that the organization has some way of documenting or recording its arrangements and controlling its documents. The organization should establish and maintain information in a suitable medium, which describes the care arrangements and gives direction on related documentation.

Any documentation or electronic media should be so managed that:

— it can be located;
— it is periodically reviewed, revised as necessary and approved for adequacy by authorized personnel;
— current versions of relevant documents and data are available at all locations where operations essential to the effective functioning of the system are performed;
— obsolete documents and data are promptly removed from all points of issue and points of use or otherwise assured against unintended use; and
— archival documents and data retained for legal purposes or knowledge preservation, or both, are suitably identified.

Communication

Communication from stakeholders can give an early warning of possible problems that could adversely affect the reputation of the organization. Reputations are built upon trust, the trust that stakeholders, particularly customers, have in the organization. Proactive communication with stakeholders can do much to develop trust and provide feedback on areas of concern.

External communication to and from stakeholders should be integrated in the organization's framework. This includes marketing and communication with national bodies, investors, the media and any other appropriate areas. It may be necessary to have an appointed person who is tasked with coordinating and dealing with media enquiries.

Organizations should consider the following.

— Is internal communication seen as essential to the organization's strategic success?
— Is the organization willing to change things when this is necessary to improve internal communication?
— Is the organization prepared to invest in resources for internal communication, for example, in training people in the use of new technology?
— Does the organization make sure that those responsible for internal communication have access to all the right information, at the right time, to enable them to play their part in implementing the business strategy?
— Does the organization value and show that it values the views and ideas of people at all levels throughout the organization?
— Is the organization's collective commitment to positive communication self-generated such that personnel act on it consistently even when unprompted?

Performance assessment

Monitoring and measuring

Internal control is a requirement of corporate governance. Audit is one powerful tool for assessing the organization's performance against the arrangements it has specified, which is described below. In addition, there are other ways of assessing performance that are extremely valuable and may be required for a number of reasons. There are many activities undertaken within an organization on a daily basis that are essential to ensuring the organization manages its operational risks, e.g. visitors, site security, delivery of correct supplies and safety. The aim should be to monitor, check, inspect and measure those activities or parameters that could have a significant impact should they fail in some way.

The requirement to monitor what is happening in an organization, either at an individual operating unit or across the organization, together with effective systems for measuring results and reporting these at the appropriate level, is particularly important. Everyone will be familiar with the regular reporting on financial matters (fundamental in the ongoing sustainability of any organization) but, equally, monitoring activities that relate to other specific organizational objectives is important in effective internal control.

For example, local government may have best-value performance indicators in the following areas:

— corporate health;
— education;
— Social Services;
— housing and homelessness;
— Housing Benefit and Council Tax;
— waste;
— transport;
— planning;
— environment/environmental health and trading standards;
— cultural services/libraries and museums;
— community service and well-being;
— fire;
— quality of services.

In a commercial organization these could reflect differing objectives and might include:

— return to shareholders;
— dividend per share and dividend cover;
— operating profit before tax;
— customer satisfaction;
— waste management;
— emissions and pollution;
— transport;
— health and safety performance;
— employee satisfaction;
— quality.

The selection of indicators will depend entirely upon the organization, its sector and its stakeholders, and both of the above lists comprise high-level strategic objectives for the organizations that will require monitoring. There will also be many lower-level monitoring activities that feed into the organizational objectives. These might include the following:

— Managers demonstrating genuine interest in 'shop floor' activities will encourage buy-in by employees and help encourage feedback on potential problems and opportunities for improvement.
— Regular checks to ensure waste is disposed of appropriately.
— Evaluating the efficiency and cost of dealing with planning applications.
— Monitoring the satisfaction of householders with council services.

In any event, the methods used should be proactive, that is, seeking information on what is happening and identifying areas of possible concern before they become an issue.

Evaluation of compliance

At various times the organization needs to determine whether it is compliant with any regulatory controls or requirements that apply to its operations. This evaluation may need to be against the requirements specified in other countries if the organization provides goods or services to other parts of the world. The frequency of this evaluation can vary depending on the risk and the controls that are applied.

A similar process is also appropriate for evaluating customer or stakeholder requirements.

Internal audit

Many people are familiar with the concept of auditing for financial purposes. The function of financial auditors is quite different from that of a systems auditor. In the case of risk management for corporate governance, the internal audit should be focused on the risk management systems and their ability to deliver the organization's policies and objectives. The auditor has a responsibility to make sure that the defined system is in fact being followed.

Audit considerations at a high level should include:

— board policy objectives and priorities;
— stakeholder requirements;
— statutory and regulatory requirements;
— risks to the organization;
— systems and operational arrangements.

The audit should establish that the following requirements have been met:

— plans prepared, documented and communicated;
— responsibilities designated;
— time-scales set to achieve objectives;
— plans reviewed at planned regular intervals;
— documentation of roles, responsibilities, and authorities;
— a management representative has been appointed as a risk owner;
— resources (including human resources, specialized skills, technology and financial resources);
— roles, responsibilities and authorities defined and documented;
— effective procedures for ensuring the competence of personnel to carry out their designated functions.

All internal audit activities should result in a formal report dealing with the specific areas that have been audited. This report should be confidential and, whilst aspects of the

findings may have been discussed with appropriate levels of management, it should be provided directly to the top management responsible for risk management.

Personnel chosen to undertake the internal audit should be selected on the basis of competence and independence from the area being assessed.

Improvement

General

No system should be static as the expectations of stakeholders continually change over time. Moreover, the ability to manage risk may well improve, and the system needs to take account of emerging risks.

The processes of monitoring, measurement and audit provide valuable information on where improvements to the system are necessary or can be made.

Analysis of nonconformity

If the system is failing in some way, this is often termed as a nonconformity and arrangements need to be established for analysing and correcting this. The root cause for the nonconformity shall be determined and the failing addressed.

The level at which responsibility and authority for any specific action to deal with preventing nonconformance will obviously depend upon the nature of the risk. This should be dealt with at a sufficiently senior level to demonstrate commitment to the process. There needs to be some process instigated to check that action has been taken and that it has been effective in dealing with the root cause of the nonconformance. Any new arrangements put in place should be evaluated before implementation to determine that no new unacceptable risks will be created.

Management review

Reviewing risk management governance systems is a fundamental requirement in any organization. The review ensures that internal controls are being applied effectively, as intended, and deliver organizational objectives. Most importantly, reviews provide the mechanism to drive the continual improvement required of any management system.

There are specific inputs to the management review and what is expected in the form of outputs. This reinforces the vital role of these reviews in driving the continual improvement cycle.

- ***Results of audits***
  The audit process should be embraced as an essential activity and top management should view the outputs in a positive manner, whether the results are positive or negative. The results are one of the most important inputs to the review process. They should help to identify whether the existing arrangements are sufficient for delivering the policy and objectives.
- ***Feedback from stakeholders***
  Any emerging trends, stakeholder requirements or information from external sources should be dealt with as they arise throughout the year. The management review needs to consider whether there is a need for new strategies or arrangements.

For the system to be effective there is a need to involve the workforce and encourage its contribution. Its concerns should be considered with a view to identifying opportunities for continuing and/or improved commitment to the organization in its management of the risks for good governance.

— ***Status of remedial actions***
The organization should review any actions it has taken or is taking following any incidents.

— ***Follow-up actions from previous management reviews***
The follow-up actions should be presented and an indication given where possible of the timeliness of the implementation of new measures and their effectiveness.

— ***Changing circumstances, including developments in legal and other requirements***
This includes both internal and external factors, such as takeovers or mergers, reorganizations, new technology, new projects and any new legal or regulatory impacts.

— ***Data and information on organizational performance***
This is where the overall performance of the organization is reviewed to see how well it has been managing its risks for governance and whether the objectives have been delivered within the defined schedule.

— ***Recommendations for improvement***
A frequent misconception is that the management review should just be carried out annually. In reality, the frequency should be determined by circumstances. To be truly effective, the management review of the organization's processes should be structured around areas of delivery where uncertainty and risk matter most.

The management review differs from the audit in that it is more strategic in its focus. For example, the audit may conclude that everything is in place to meet the policy and objectives, but the management review may show, for example, that internal or external considerations justify a change.

As well as seeking to remedy deficiencies, the management review offers the opportunity for a more proactive approach: to consider where the organization wishes to be in the governance of its risks and how it can maximize the resulting benefits.

5. Other management processes

There are many international and national management system processes that can help an organization in the implementation, operation and maintenance of internal control arrangements. There may be individual arrangements to deal with specific risks that are very sound in themselves, which are externally assessed and certified. These individual arrangements may be useful as a framework for developing overall internal control and risk management arrangements. In any event, the use of external parties to undertake independent audit should give assurance to the board that arrangements are sound and can meet reporting requirements expected under corporate governance frameworks. Additionally, the use of such certified systems can assist in embedding within the organization arrangements for risk assessment and internal control, enabling an organization to demonstrate compliance to interested stakeholders.

The list below includes standards that relate to some areas that might be considered:

BS 25999–1:2006, *Business continuity management — Part 1: Code of practice*

BS 25999–2:2007, *Business continuity management — Part 2: Specification*

BS 31100 (DPC) (2008) *Code of practice for risk management*

BS EN ISO 14001:2004, *Environmental management systems — Requirements with guidance for use*

BS EN ISO 22000:2005, *Food safety management systems — Requirements for any organization in the food chain*

BS ISO/IEC 27001:2005; BS 7799-2:2005, *Information technology — Security techniques — Information security management systems — Requirements*

BS OHSAS 18001:2007, *Occupational health and safety management systems — Requirements*

SA8000:2001, *Social Accountability*

Please see Appendix B for correspondence of the requirements between various management systems for quality, environment, health and safety and information security.

6. Self-assessment questionnaire

The simple questions set out below will enable you to establish where your organization is positioned with respect to the basic elements it needs for controlling its risks.

Each question attracts a score between 0 and 2. Score 0 where the issue has not been addressed, 1 for partial compliance and 2 if your organization fully satisfies the question.

	0	1	2
Is top management committed to effective risk management for good governance?			
Is the risk management system based on the best available information?			
Is risk management part of the process of decision making in your operations?			
Are your risk management systems and policies appropriate for the size, complexity and nature of your organization?			
Are your risk management system and policies appropriate for the nature of the risks your organization faces, reflecting best practice in your sector?			
Does the organization have a process for identification of risks?			
Have you identified the risks to the organization?			
Have you assessed the likelihood and consequences of the significant risks being realized?			
Is the risk management system systematic and structured?			
Does the risk identification process take into account organizational culture, human factors and behaviour?			
Is your risk management system dynamic and responsive to change?			
Have you assessed the risks that could damage your organization's reputation?			
Have you assessed the risks that could result in production loss or service failing?			

	0	1	2
Have you assessed the risk that could adversely affect your market position?			
Do you have a mechanism to identify and assess risks on an ongoing basis?			
Have you established internal control arrangements to deal with the identified risks?			
Is top management up to date with developments in regulatory frameworks, technological issues and political issues, which may affect the organization's market?			
Is there a process in place to identify legal and other requirements that the organization needs to address?			
Have you identified your organization's stakeholders and their expectations?			
Have you established a contingency plan and evaluated its effectiveness?			
Have you established continuity arrangements in the event of a disaster or emergency?			
Does top management have clear objectives for the organization that have been communicated to employees as appropriate?			
Does management demonstrate the necessary competence and integrity to create a climate of trust?			
Are the arrangements embedded in the culture of the organization?			
Are management control arrangements implemented effectively throughout the organization?			
Does management ensure that people are adequately trained to manage the risks they are assigned to control?			
Do the people in the organization have the knowledge, skills, tools and resources to support the achievement of the company's objectives?			
Are arrangements in place for documenting arrangements and records kept where necessary?			

	0	1	2
Is there effective communication between top management and the management team, other employees and others to ensure that all parties understand the company's appetite for risk?			
Are there established channels of communication for individuals to report suspected breaches of law, regulations, etc. – a 'whistle-blower's charter'?			
Are operational controls monitored on a regular basis to ensure continued effectiveness?			
Do you regularly review arrangements for complying with customer, stakeholder and regulatory requirements?			
Do you regularly audit the risk management control arrangements?			
Do you regularly seek to improve your arrangements?			
Do the results of audits, incidents and performance reports regularly form part of the review process?			
Do you report regularly upon your risk management processes?			

If your total score is:

less than 30: your organization has hardly made a start on the effective management of its risks for good governance and needs to move forward quickly

31 to 60: your organization has made a start but needs to do more

more than 60: provided you do not score less than 1 in any area, the organization should be well on the way to effective control.

Appendix A. Summary of risk management tools

Table A.1 Summary of risk management tools

Tool	Identification	Assessment	Response
Risk questionnaires	✓		
Risk checklists/Prompt lists	✓		
Risk identification workshop	✓	✓	
Nominal group technique	✓	✓	
Risk breakdown structure	✓	✓	
Delphi technique	✓	✓	
Process mapping	✓	✓	
Cause-and-Effect diagrams	✓	✓	
Risk mapping/Risk profiling	✓	✓	
Risk Indicators	✓		
Brainstorming/ 'thought shower' events	✓		
Interviews and focus groups	✓		
'What if?' workshops	✓		
Scenario analysis/scenario planning/horizon scanning	✓	✓	✓
Hazard and operability study (HAZOPs)	✓	✓	
PEST (Political, Economic, Sociological, Technological) analysis	✓	✓	
SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis	✓	✓	
Stakeholder engagement/Matrices	✓		
Risk register/Database	✓	✓	✓
Project profile model (PPM)	✓		
Risk taxonomy	✓		
Gap analysis: Pareto analysis	✓	✓	

Tool	Identification	Assessment	Response
Probability and consequence grid/Diagrams (PIDs)/Boston grid	✓	✓	
CRAMM	✓	✓	✓
Probability trees		✓	
Expected value method		✓	
Risk modelling/Risk simulation (Monte Carlo/Latin Hypercube):		✓	
Flow charts, process maps and documentation		✓	
Fault and event tree modelling: Failure Mode Effects Analysis (FMEA)		✓	
Stress testing	✓	✓	
Critical path analysis (CPA) or Critical path method (CPM)		✓	
Sensitivity analysis		✓	
Cash flow analysis		✓	
Portfolio analysis		✓	
Cost-Benefit analysis		✓	✓
Utility theory		✓	
Visualization techniques Heat maps, RAG status reports, Waterfall charts, Profile graphs, 3D Graphs, Radar charts, Scatter diagrams		✓	✓

Source: Table A.1 is taken from DC BS 31100

Appendix B. Comparative table – common elements of quality, environmental and OH&S Systems with PAS 99

Table B.1 Comparative table illustrating the common elements of quality, environmental and OH&S Systems with PAS99: specification of common management systems requirements as a framework for integration

Good Governance – Risk Management System	ISO 9001	ISO 14001	ISO 18001	ISO/IEC 27001	Requirements of PAS 99
3.1 General requirements	4.1 5.5	4.1	4.1	4.1 4.2	4.1
3.2 Policy	5.1 5.3	4.2	4.2	5.1	4.2
3.3 Planning for risk management	5.4	4.3	4.3	4.2	4.3
3.3 Risk identification, assessment and control	5.2 5.4.2 7.2	4.3.1	4.3.1	4.2	4.3.1
3.3 Identification of stakeholder requirements	5.3 7.2.1 7.2.1	4.3.2	4.3.2	4.2.1(b2)	4.3.2
3.3 Contingency planning	5.4 8.3	4.4.7	4.4.7		4.3.3
3.3 Objectives and management programme	5.4.1 5.4.2 8.5.1	4.3.3	4.3.3	4.2.2	4.3.4
3.3 Organizational structure, roles, responsibilities, accountability and authority	5.1 5.5	4.4.1	4.4.1	4.2.2	4.3.5
3.4 Implementation and operation	7	4.4	4.4		4.4
3.4 Operational Control	7	4.4.6	4.4.6	4.2.2	4.4.1
3.4 Managing resources	5.1 5.5.1 6	4.4.1 4.4.2	4.4.1 4.4.2	5.2.1 5.2.2	4.4.2

Good Governance – Risk Management System	**ISO 9001**	**ISO 14001**	**ISO 18001**	**ISO/IEC 27001**	**Requirements of PAS 99**
3.4 Documentation	4.2	4.4.4 4.4.5 4.5.4	4.4.4 4.4.5 4.5.4	4.3	4.4.3
3.4 Communication	5.3 5.5.1 5.5.3 7.2.3	4.4.3	4.4.3	4.2.4(c)	4.4.4
3.5 Performance assessment	8	4.5	4.5		4.5
3.5 Monitoring and measuring	8 7.6	4.5.1	4.5.1	4.2.3	4.5.1
3.5 Evaluation of compliance	8.2	4.5.2	4.5.1 4.5.2	4.2.3	4.5.2
3.5 Internal Audit	8.2.2	4.5.5	4.5.5	6	4.5.3
3.6 Improvement	8.5	4.5.3 4.6	4.6.	8	4.6.1
3.6 General	8.5	4.5.3 4.6	4.6	4.2.4 8.1	4.6.1
3.6 Analysis and handling of nonconformities	8.3 8.4 8.5	4.5.3	4.5.3	4.2.4 8.2 8.3	4.5.4 4.6.2
3.7 Review	5.6	4.6.	4.6.	7	4.7
3.7 Management review – general	5.6.1	4.6		7.1	4.7.1
3.7 Input	5.6.2	4.6		7.2	4.7.2
3.7 Output	5.6.3	4.6		7.3	4.7.3
3.7 Reporting		4.4.3			

Note: this Table should be taken as a guide only, since correspondence between the clauses could be imprecise

Appendix C. References and further reading

Corporate governance codes from around the world:
http://www.ecgi.org/codes/all_codes.php

Association of British Insurers (ABI) (2008) *ABI Research Paper 7 – Governance and Performance in Corporate Britain*, London: ABI

The Association of Insurance and Risk Managers (AIRMIC), The National Forum for Risk Management in the Public Sector (ALARM) and The Institute of Risk Management (IRM) (2002) *A Risk Management Standard*, London: AIRMIC/ALARM/IRM

Basel Committee on Banking Supervision (1999) *Enhancing Corporate Governance for Banking Organisations*, Basel: Basel Committee on Banking Supervision. See:
http://www.bis.org/bcbs/

Blair, A (2005) 'Risk and the State' speech delivered by Rt Hon A Blair at University College London, 26 May 2005

BS 6079-3:2000, *Project management — Part 3: Guide to the management of business related project risk*, London: British Standards Institution

BS 25999-1:2006, *Business continuity management – Part 1: Code of practice*, London:

BS 25999-2:2007, *Business continuity management — Part 2: Specification*, London: British Standards Institution

BS 31100 (DPC) (2008) *Code of practice for risk management*, London: British Standards Institution

BS EN ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*, London: British Standards Institution

BS EN ISO 9001:2000, *Quality management systems — Requirements*, London: British Standards Institution

BS EN ISO 14001:2004, *Environmental management systems — Requirements with guidance for use*, London: British Standards Institution

BS EN ISO 22000:2005, *Food safety management systems — Requirements for any organization in the food chain*, London: British Standards Institution

BS ISO/IEC 27001:2005; BS 7799-2:2005, *Information technology — Security techniques — Information security management systems — Requirements*, London: British Standards Institution

BS OHSAS 18001:2007, *Occupational health and safety management systems — Requirements*, London: British Standards Institution

Cadbury, A et al. (1992) *Report of the Committee on the Financial Aspects of Corporate Governance*, London: Gee and Co Ltd

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004) *Enterprise Risk Management — Integrated Framework*, Washington, DC: COSO

The Federal Reserve Board (2004) 'Trends in Risk Management and Corporate Governance' ('Remarks by Governor Susan Schmidt Bies At the Financial Managers Society Finance and Accounting Forum for Financial Institutions, Washington, D.C., June 22, 2004'). See:
http://www.federalreserve.gov

Financial Reporting Council (FRC) (2005) *Internal Control – Revised Guidance for Directors on the Combined Code*, London: FRC

Financial Reporting Council (FRC) (2008) *The Combined Code on Corporate Governance*, London: FRC

Hillson, D (2007) *The Risk Management Universe: A guided tour* (2nd edition) (BIP 2036), London: British Standards Institution

IMS Risk Solutions (2003a) *IMS: Continual Improvement through Auditing* (BIP 2011:2003), London: British Standards Institution

IMS Risk Solutions (2003b) *IMS: Risk Management for Good Governance* (BIP 2012:2003), London: British Standards Institution

The Independent Commission on Good Governance in Public Services (2004) *The Good Governance Standard for Public Services*, London: Office for Public Management Ltd and The Chartered Institute of Public Finance and Accountancy

International Corporate Governance Network (ICGN) (1999) *ICGN Statement on Global Corporate Governance Principles*, London: ICGN. See: http://www.icgn.org/documents/globalcorpgov.htm

Kelly, J M (2004) *IMS: The Excellence Model* (BIP 2010:2004), London: British Standards Institution

MORI (2003) *Focus on the Future of Corporate Governance*, London: MORI

Murray, R P (2003) *IMS: Information Security* (BIP 2008:2003), London: British Standards Institution

Nowacki, G (2003) *IMS: Customer Satisfaction* (BIP 2005:2003), London: British Standards Institution

Office for Public Management Ltd (OPM) (2007) *Going Forward with Good Governance*, London: OPM

Office of Government Commerce, *Management of Risk*. See: http://www.ogc.gov.uk/guidance_management_of_risk.asp

Organisation for Economic Co-operation and Development (OECD) (2004a) *OECD Principles of Corporate Governance*, Paris: OECD. See: http://www.oecd.org

Organisation for Economic Co-operation and Development (OECD) (2004b) *Guidelines on Corporate Governance of State-owned Enterprises – Draft Text*, Paris: OECD. See: http://www.oecd.org/dataoecd/46/51/34803211.pdf.

Organisation for Economic Co-operation and Development (OECD) (2004c) *Comments from Public Consultation on the Draft for Guidelines on Corporate Governance in State Owned Enterprises*, Paris: OECD. See: http://www.oecd.org

PAS 99:2006, *Specification of common management system requirements as a framework for integration*, London: British Standards Institution

Robbins, M and Smith, D (2000) *Managing Risk for Corporate Governance* (PD 6668), London: British Standards Institution

SA8000:2001, *Social Accountability*, New York: Social Accountability International

Smith, D and Politowski, R (2007a) *IMS: A Framework for integrated management systems. Background to PAS 99 and its application* (BIP 2119:2007), London: British Standards Institution

Smith, D and Politowski, R (2007b) *IMS: Implementing and operating using PAS 99* (BIP 2138:2007), London: British Standards Institution

Turnbull, N *et al*. (1999) *Internal Control – Guidance for Directors on the Combined Code*, London: The Institute of Chartered Accountants in England & Wales. Available at: http://www.icaew.com

United States of America (2002) Sarbanes-Oxley Act of 2002. Available at: http://www.sec.gov/about/laws/soa2002.pdf. See also: http://www.sec.gov/spotlight/sarbanes-oxley.htm

Escalating energy costs
Huge order for your new product
2008 'credit crunch'

Such events can put your organization at risk. The adverse effects of poor risk management are evident everyday in the news, affecting the lives and welfare of organizations, individuals and society as a whole. Robust management systems will assist resilience and sustain an organization through challenging change. Furthermore, stakeholders in all types of organizations, public or private sector, have increasing expectations of the manner in which organizations are managed. Those responsible for ensuring the successful and sustainable operation of their organizations must be able to demonstrate that their grasp of risk areas within their control is sufficient and that strong internal controls are in place.

Since its first publication in 2000 under the title *PD 6668:2000, Managing Risk for Corporate Governance* there have been many developments in international and national management systems standards all of which focus upon specific areas of risk for organizations. *Good Governance – a risk-based management systems approach to internal control* outlines the framework of a risk management system and provides guidance on implementation, other management processes and a self-assessment questionnaire. This framework uses as its foundation the Plan, Do, Check, Act approach found in PAS 99:2006, which facilitates an integrated approach across all risk management areas where organizations are seeking the business benefits of such an approach.

About the Authors

David Smith and Robert Politowski are directors of iMS Risk Solutions Ltd, facilitating risk management results for organizations who care, in a wide range of risk areas relevant to modern-day businesses including Health & Safety, Environment and Governance.

In addition to this publication, they had a leading role in the drafting of PAS 99 and the Integrated Management Systems series published by BSi. Additionally, David Smith represents the UK on a variety of international standards committees and is Chair of the BSi committee on Health and Safety management systems standards.

BSI
Group Headquarters
389 Chiswick High Road
London
W4 4AL
www.bsigroup.com

The British Standards Institution is incorporated by Royal Charter
BSI order ref: BIP 2154

ISBN 978-0-580-64313-2
9 780580 643132