

BS 31100:2008



BSI Standards Publication

Risk management — Code of practice

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© BSI 2008

ISBN 978 0 580 64908 0

ICS 03.100.01

The following BSI references relate to the work on this standard:

Committee reference RM/1

Draft for comment 08/30174620 DC

Publication history

First published October 2008

Amendments issued since publication

Amd. No.	Date	Text affected
----------	------	---------------

Contents

Foreword *ii*

Introduction 1

1 Scope 3

2 Risk management principles 3

3 Risk management framework 5

4 Risk management process 16

5 Developing risk management activities 22

Annexes

Annex A (informative) Risk categories 26

Annex B (informative) Risk management tools 27

Annex C (informative) Effects of controls 29

Annex D (informative) Risk maturity models 31

Annex E (normative) Incorporating potentially positive consequences of risk 32

Glossary 33

Bibliography 40

List of figures

Figure 1 – Risk management perspectives 2

Figure 2 – Risk management model 2

Figure 3 – Risk management framework 5

Figure 4 – The risk management process 16

List of tables

Table B.1 – Examples of risk management tools (including techniques) 28

Summary of pages

This document comprises a front cover, an inside front cover, pages i to ii, pages 1 to 40 and a back cover.



Documents

Document Sharing Hub

© BSI 2008 • 1

Foreword

Publishing information

This British Standard was published by BSI and came into effect on 31 October 2008. It was prepared by Technical Committee RM/1, *Risk management*. A list of organizations represented on this committee can be obtained on request to its secretary.

This British Standard has been developed by practitioners throughout the risk management community, drawing upon their considerable academic, technical and practical experiences of risk management.

Relationship with other documents

This British Standard has been drafted to be consistent with the general guidance on risk management that will be given by ISO 31000 (in preparation), but is also developed recognizing the knowledge contained in HM Treasury's Orange Book [1], the Office of Government Commerce publication, *"Management of risk: Guidance for practitioners"* [2], *"Enterprise Risk Management — Integrated Framework"* and application techniques published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) [3], and the Risk Management Standard developed by The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) and ALARM [4].

Use of this document

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The word "should" is used to express the recommendations of this standard, with which the user has to comply in order to comply with the standard. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

Introduction

Organizations of all types and sizes face a range of risks affecting the achievement of their objectives. While “risk” is commonly regarded as negative, risk management is as much about exploiting potential opportunities as preventing potential problems. It is important to bear this in mind whenever managing risk, and in reading this Code of Practice. Risk management is an essential part of good management.

Effective risk management can assist the organization to achieve its objectives by, for example:

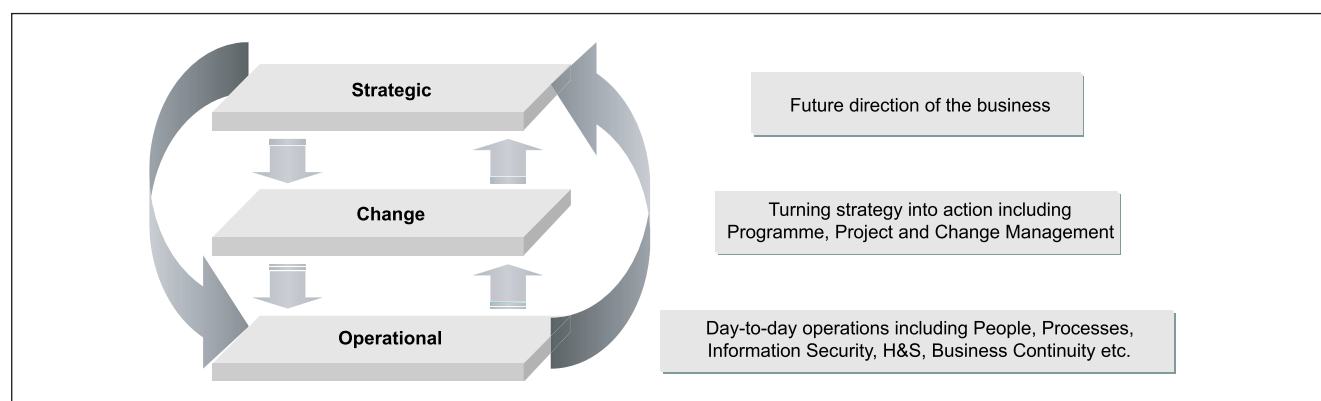
- a) reducing the likelihood of events that would have a negative consequence overall and reducing the negative consequences of such events;
- b) increasing the likelihood of events that would have a positive consequence overall and increasing the positive consequences of such events;
- c) identifying opportunities where taking risks might benefit the organization;
- d) improving accountability, decision making, transparency and visibility;
- e) identifying, understanding and managing multiple and cross-organization risks;
- f) executing change more effectively and efficiently and improving project management;
- g) providing better understanding of, and compliance with, relevant governance, legal and regulatory requirements, and corporate social responsibility and ethical requirements;
- h) protecting revenue and enhancing value for money;
- i) protecting reputation and stakeholder confidence;
- j) proactively managing the organization’s operations;
- k) targeting control expenditure and delivering a cost-optimal control environment;
- l) retaining and developing customers through reducing risks to service delivery and enhancing service provision; and
- m) making the organization more flexible and responsive to market fluctuations so that it is better able to satisfy customers’ ever-changing needs in a continually evolving business environment.

The benefits of good risk management (and the consequences of poor risk management) will be felt by an organization’s management, staff, shareholders, customers and other stakeholders.

Risk management has to continuously, systematically and proportionally address the risks surrounding an organization’s activities. It cannot be separated from the culture of the organization.

Risk management comprises a framework and process that enable an organization to manage uncertainty in a systemic, effective, efficient and systematic way from strategic, programme, project and operational perspectives, as well as supporting continual improvement. Risk management applies at all levels of an organization and to all activities (see Figure 1).

Figure 1 Risk management perspectives



This standard provides a guide to risk management principles, models, framework and processes. Its purpose is to assist organizations to achieve their objectives through effective risk management.

The risk management model presented in this standard provides at the core a framework and process on which to manage risks. The outer rings of Figure 2 contain the context in which the organization operates, the organization itself and the culture, with communication required at all levels.

Figure 2 Risk management model



1 Scope

This British Standard provides a basis for understanding, developing, implementing and maintaining proportionate and effective **risk management** throughout an organization, in order to enhance the organization's **likelihood** of achieving its objectives. This British Standard establishes the principles and terminology for risk management, and gives recommendations for the model, framework, process and implementation of risk management which are derived from experience and good practice.

NOTE 1 A glossary gives the definitions of the risk management terms most commonly used in this Standard, with the first instance of each term being highlighted in bold to indicate that it is included in the glossary. With some exceptions, the definitions in the glossary are consistent with those given in Working Draft 2 of ISO Guide 73 (1 April 2008).

The basic risk management principles (see Clause 2) are applicable to any organization, but the way they are implemented will vary according to an organization's nature, including size and complexity, and **context**.

This Standard is intended for use by anyone with responsibility for any of the following:

- ensuring an organization achieves its objectives;
- ensuring **risks** are proactively managed in specific areas or activities;
- overseeing risk management in an organization;
- providing assurance on the effectiveness of an organization's risk management; and/or
- reporting to **stakeholders**, e.g. through disclosures in annual financial statements, corporate governance reports and corporate social responsibility reports.

NOTE 2 Annex A gives guidance on risk categories, Annex B gives examples of risk management tools, Annex C discusses the effects of controls, Annex D explains the use of risk maturity models and Annex E specifies the incorporation of the potentially positive consequences of risk into risk management.

2 Risk management principles

Risk management should be part of the organization's overall approach or framework for governance. The organization should base its risk management practices on the following principles.

i) Risk management should be tailored

The organization should have an approach to risk management which is proportionate and scaled to address the context.

ii) Risk management should take into account organizational culture, human factors and behaviour

The organization's risk management processes should take into account the capabilities, perceptions and intentions of the people in the organization and other relevant stakeholders who might facilitate or hinder attainment of the organization's objectives.

iii) Risk management should be systematic and structured

The approach to risk management should be consistently applied within the organization. This helps ensure that the outputs of the **risk management process** are both reliable and comparable, and gives managers increased confidence to make effective decisions.

iv) Risk management should operate under a common language

The organization should apply a common language when identifying, assessing and responding to risks, and maintaining its risk management framework.

v) Risk management should be based on the best available information

The inputs to the risk management process should be based on relevant information sources, such as reported experience, subject knowledge, expert judgment and projected forecasts. Managers should be aware of any limitations to the data or divergence of opinion among experts.

vi) Risk management should explicitly address uncertainty

The organization should use risk management to help clarify the nature of uncertainty, how this might affect decisions and how it might be treated.

vii) Risk management should be part of decision making

Risk management should support informed decision making by helping to understand risks. This aids the organization in making a decision concerning its **risk appetite** and ability to manage the risks effectively.

viii) Risk management should protect everything of value

Risk management should contribute to the achievement of objectives and maximize benefits through integration with management processes, taking account of legislative, regulatory and compliance requirements.

ix) Risk management should be transparent and inclusive

The organization's managers should ensure that all stakeholders are identified, informed and appropriately involved in **risk identification**, assessment and response.

x) Risk management should be dynamic, iterative and responsive to change

The organization should ensure its risk management continually identifies and responds to changes affecting its operating environment (context).

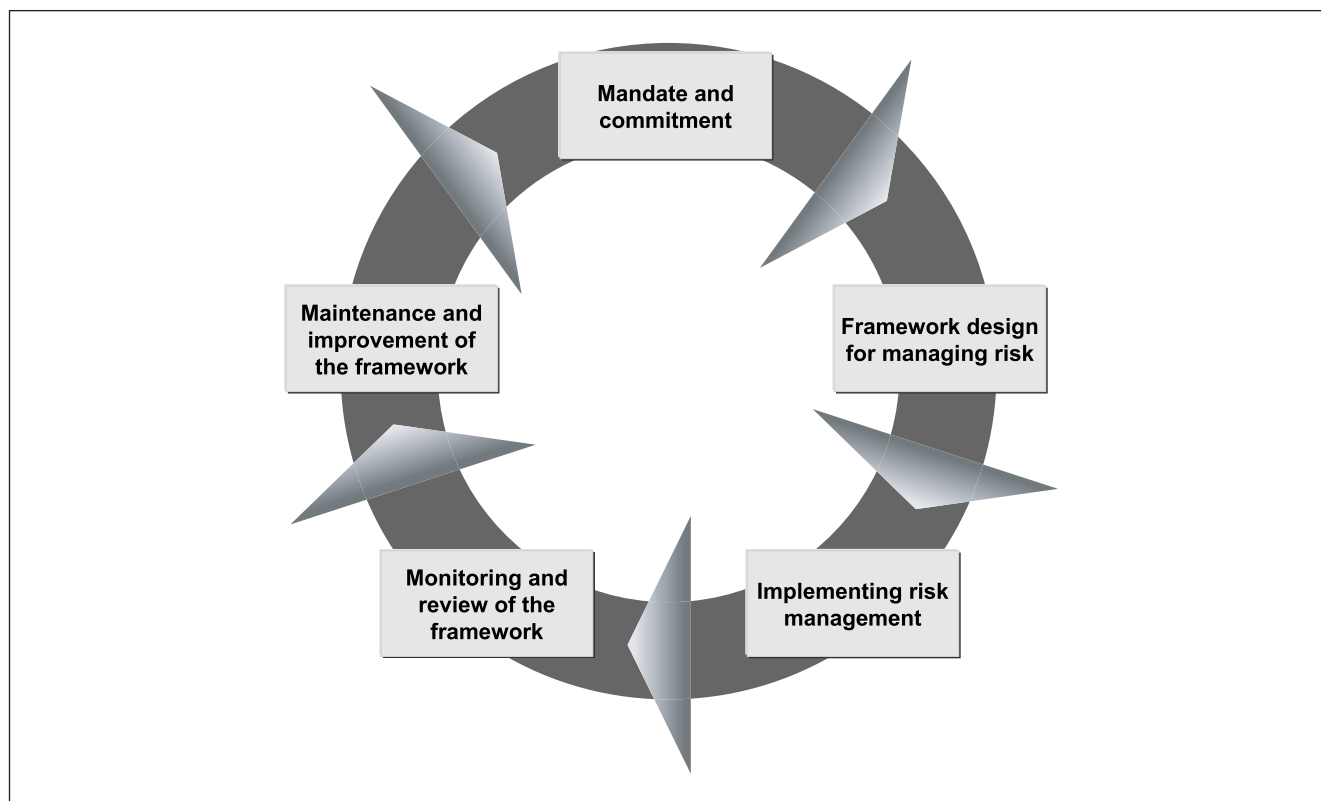
xi) Review of the principles

The way in which the risk management principles are applied should be subject to regular review to reflect changes in the organization's nature and context.

3 Risk management framework

NOTE The risk management framework provides an infrastructure for delivering, maintaining and governing risk management throughout the organization. The risk management framework comprises a system of interrelated components, as indicated in Figure 3.

Figure 3 Risk management framework



Area	Framework components
Mandate and commitment	Governance (3.1)
Framework design for managing risk	Risk management strategy (3.2) Risk management policy (3.3) Risk management culture (3.4) Building capability and competence (3.5) Roles, responsibilities and authorities (3.6) Risk management tools (3.7) Risk appetite and risk profile (3.8) Risk and consequence categorization and measurement (3.9) Risk criteria (3.10)
Implementing risk management	Risk communication (3.11) Risk management process (Clause 4) Developing risk management activities (Clause 5)
Monitoring and review of the framework	Risk reporting (3.12) Risk management implementation and maintenance (5.3) Risk management monitoring, review and continual improvement (5.4)
Maintenance and improvement of the framework	Risk management implementation and maintenance (5.3) Risk management monitoring, review and continual improvement (5.4)

3.1 Governance

Risk management is an important element of how a **board (or equivalent)** discharges its responsibilities to stakeholders in the governance of the organization; the organization's **risk management framework** should have the following features:

- risk management as part of the organization's overall approach or framework for governance;
- risk being recognized as a Board (or equivalent) matter, with the Board ultimately accountable for risk management;
- risk management objectives designed to support and achieve the organization's risk appetite and the approach to recognizing risk in decisions, providing achievable goals for risk management;
- ownership and accountability for managing and reporting on risk throughout the organization;
- roles, accountabilities and responsibilities for managing risk, which are communicated and understood, and a clear distinction between those who have:
 - a) direct responsibility for the management of risk, e.g. management and staff working within each organizational unit;
 - b) responsibility for development, implementation, maintenance and oversight of the effectiveness of the risk management framework, e.g. a risk committee;
 - c) responsibility for providing independent assurance, e.g. internal audit; and
 - d) ultimate responsibility for obtaining assurance and thereafter driving improvement.
- a defined, effectively communicated and understood policy, which sets out the requirements for managing risk;
- defined processes and procedures for managing the organization's risks (see Clause 4) and for managing the development of risk management across the organization (see Clause 5);
- a method of assessing, leading and monitoring the organization's risk management culture;
- defined parameters around the **level of risk** that is acceptable to the organization, and thresholds which trigger escalation, review and approval by an authorized person/body;
- a defined approach to recognizing risk in decisions;
- an appropriate flow of risk information around the organization; and
- a commonly defined and agreed terminology for describing **key risk management** concepts and practices.

The risk management framework should include objectives for risk management, plans for developing risk management across the organization, and designs for elements such as processes and tools. These should be contained in a risk management strategy and a risk management policy.

3.2 Risk management strategy

A risk management strategy should be prepared that:

- sets the direction, scope and priorities of risk management;
- indicates how risk management supports the strategy, aims and objectives of the organization;
- takes into consideration the context, key stakeholders and the organization's existing risk management capability and maturity;
- is documented and is approved by senior management; and
- is communicated effectively.

The risk management strategy may also include:

- the objectives of risk management;
- the risk management activities to be undertaken within an appropriate timeframe to help the organization achieve its objectives;
- the resources required, including people, knowledge and budget;
- the target level of risk management capability and specific activities to be taken to develop and embed risk management in the organization within a given timeframe; and
- how progress against the risk management strategy will be monitored, reviewed and reported.

3.3 Risk management policy

3.3.1 General

The risk management policy should provide a clear and concise outline of the organization's requirements for risk management as an integral part of the organization's overall approach to governance.

To achieve consistency of risk management activities across the organization, with appropriate variations in detail, the policy should contain a high level overview and description of the risk management process.

The risk management policy should be:

- owned by a manager, preferably at Board (or equivalent) level;
- developed in consultation with key stakeholders;
- developed with consideration of how the organization will monitor adherence to the policy and reference any relevant standards, regulations and policies that have to be included or taken into account; and
- subject to quality assurance practices, e.g. document, change and version control.

3.3.2 Content of the risk management policy

The organization's risk management policy may include:

- **governance**, outlining how risk management is governed;
- **policy scope**, describing the purpose of the policy and who it is aimed at; describing the high level principles and the benefits of implementing risk management; setting out the objectives

including legal and regulatory requirements, and what it intends to achieve; and providing an explanation of the relationship with other policies;

- **policy applicability**, setting out to whom and to what the policy applies;
- **risk management process**, providing a high level overview and description of the risk management process adopted by the organization;
- **risk appetite**, outlining the organization's risk appetite, thresholds and escalation procedure;
- **reporting**, describing the purpose, frequency and scope of reporting;
- **roles, accountabilities and responsibilities**, describing the high level roles, accountabilities and responsibilities in respect of risk management; and
- **variations and dispensations**, stating whether variations or dispensations from the policy are allowed and, if they are allowed, describing the process for requests for this.

3.4 Risk management culture

Developing an effective risk management culture is a critical part of the risk management framework and results in the willingness and motivation of people to:

- give attention and resources to risk management;
- comply with the intent and details of risk management policies and procedures;
- solve practical difficulties in implementing risk management policies and procedures, and do so in a way that is consistent with good risk management principles;
- manage risk beyond compliance with formal policies and procedures; and
- communicate about risk openly and appropriately.

The organization should monitor and develop its risk management culture through, for example:

- demonstrating effective risk management leadership at senior levels as an example to others;
- monitoring and communicating the value added by risk management;
- providing education and training in risk management, including practical examples;
- including risk management within individual objectives and performance appraisals;
- monitoring attitudes to risk management;
- ensuring that formal risk management policies and procedures extend into all organizational processes, including strategic planning, operational processes, and programme, project and change management; and
- commitment to continually maintaining and improving risk management.

3.5 Building capability and competence

To build capability, which is essential for embedding risk management throughout the organization and developing risk management maturity, the organization should provide relevant people with appropriate experience, skills and knowledge on:

- current corporate governance requirements and their source;
- the legislative and compliance context of risk management;
- the organization's risk policy;
- the organization's risk appetite and escalation rules;
- statements on **controls**;
- the risk management process;
- how to identify, assess and manage risks;
- risk tools and techniques and how and where they are applied;
- risk reporting requirements;
- where the organization's risk management capability stands (its risk management maturity);
- roles, accountabilities and responsibilities, including the responsibility of the Board (or equivalent), audit committee, risk management oversight body and senior management; and
- an assessment of performance as part of the organization's overall appraisal system.

The organization should ensure that any person under its control performing tasks that can impact on the risks are competent on the basis of appropriate education, training or experience.

3.6 Roles, responsibilities and authorities

3.6.1 Identification

The organization should clearly identify, define, document and communicate the roles, accountabilities and authorities that are required to deliver the risk management strategy and policy.

NOTE These roles do not have to be full-time appointments or assigned to different people.

3.6.2 Senior management responsibilities

The responsibilities of the senior management of the organization in respect of risk management should include:

- ensuring that there is a fit-for-purpose and up-to-date risk management framework and process in place and that risk management is adequately resourced and funded;
- providing strategic direction on the appropriate recognition of risk in decisions and setting risk appetite and associated authority;
- approving the risk management policy and setting the "tone" and culture for managing risk and embedding risk management;
- ensuring the key risks facing the organization are properly assessed and managed;

- evaluating the risk implications of change;
- planning for how the organization will respond to risks that could arise, including the management of a crisis;
- providing direction and receiving assurance on the effectiveness of risk management and compliance with the risk management policy; and
- reporting on risk management to stakeholders and signing off public disclosures.

3.6.3 The role of individuals

The organization should embed risk management by incorporating it into each individual's responsibilities. People should understand:

- the risks that relate to their roles and their activities;
- how the management of risk relates to the success of the organization;
- how the management of risk helps them to achieve their own goals and objectives;
- their accountability for particular risks and how they can manage them;
- how they can contribute to continuous improvement of risk management;
- that risk management is a key part of the organization's culture; and
- the need to report in a systematic and timely way to senior management any perceived new or emerging risks, **near misses** or failures of existing control measures within the parameters agreed.

3.6.4 The roles of the risk owners and risk response owners

Where the risk management process identifies any risks that need to be actively managed, each risk and each response should be assigned an owner who is responsible and accountable for:

- in the case of a risk, owning the organization's assessment of the risk, monitoring it, and reporting its status; and/or
- in the case of a **risk response**, responding to the risk, contributing to the development and maintenance of an appropriate control environment, and reporting on the status of the response.

Risks and their responses may be owned by the same person.

3.6.5 Additional roles, responsibilities and authorities

Depending on the size, purpose, nature and context of the organization, the following may also be involved in risk management.

a) Risk management oversight body

The role of a risk management oversight body may be performed by a risk committee or a committee of the Board (or equivalent). In a smaller organization, the role of the risk management oversight body may be undertaken by the Board (or equivalent).