Risk management — Code of practice
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

<table>
<thead>
<tr>
<th>Amd. No.</th>
<th>Date</th>
<th>Text affected</th>
</tr>
</thead>
</table>


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.
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).
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.
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

<table>
<thead>
<tr>
<th>Area</th>
<th>Framework components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandate and commitment</td>
<td>Governance (3.1)</td>
</tr>
<tr>
<td>Framework design for managing risk</td>
<td>Risk management strategy (3.2)</td>
</tr>
<tr>
<td></td>
<td>Risk management policy (3.3)</td>
</tr>
<tr>
<td></td>
<td>Risk management culture (3.4)</td>
</tr>
<tr>
<td></td>
<td>Building capability and competence (3.5)</td>
</tr>
<tr>
<td></td>
<td>Roles, responsibilities and authorities (3.6)</td>
</tr>
<tr>
<td></td>
<td>Risk management tools (3.7)</td>
</tr>
<tr>
<td></td>
<td>Risk appetite and risk profile (3.8)</td>
</tr>
<tr>
<td></td>
<td>Risk and consequence categorization and measurement (3.9)</td>
</tr>
<tr>
<td></td>
<td>Risk criteria (3.10)</td>
</tr>
<tr>
<td>Implementing risk management</td>
<td>Risk communication (3.11)</td>
</tr>
<tr>
<td></td>
<td>Risk management process (Clause 4)</td>
</tr>
<tr>
<td></td>
<td>Developing risk management activities (Clause 5)</td>
</tr>
<tr>
<td>Monitoring and review of the framework</td>
<td>Risk reporting (3.12)</td>
</tr>
<tr>
<td></td>
<td>Risk management implementation and maintenance (5.3)</td>
</tr>
<tr>
<td></td>
<td>Risk management monitoring, review and continual improvement (5.4)</td>
</tr>
<tr>
<td>Maintenance and improvement of the framework</td>
<td>Risk management implementation and maintenance (5.3)</td>
</tr>
<tr>
<td></td>
<td>Risk management monitoring, review and continual improvement (5.4)</td>
</tr>
</tbody>
</table>
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).
The size, purpose, nature, complexity and maturity of an organization’s risk management framework might require a risk management oversight body with the following responsibilities:

- supporting senior management in establishing the risk appetite;
- monitoring compliance with the organization’s risk policy;
- monitoring the adequacy of controls;
- monitoring changes to the organization’s risk profile and formally reporting any material changes to the senior management;
- assisting the organization to understand its key risks;
- periodically reviewing the effectiveness and appropriateness of the risk management and reporting process;
- periodically reviewing the adequacy of the risk management resources;
- challenging risk management issues and practices; and
- escalating and reporting material risk issues to the Board (or equivalent) for consideration.

b) Risk management function and the risk manager

The organization should, depending on its size and complexity, have a risk champion/manager or a dedicated risk management department working under the guidance of a risk management oversight body, if one exists. A risk manager assists in identifying, evaluating, controlling, monitoring and reporting risks. In addition, the organization should identify the requirements of specialist functions or individuals managing specific aspects of risk, such as compliance risk, operational risk, health and safety, information security, and business continuity management. The role of the risk manager and risk management function should include:

- promoting the consistent use of risk management and ownership of risk at all levels within the organization;
- building a risk aware culture within the organization, including appropriate education and training;
- developing, implementing and reviewing the risk management framework and risk management processes;
- developing competence and maturity in risk management;
- coordinating the other functions that advise on specific aspects of risk management;
- coordinating responses where risks impact more than one area;
- understanding the relationship between key stakeholders, e.g. the Board (or equivalent) and risk management oversight body (if one exists);
- providing assurance to senior management/the Board (or equivalent) and/or the oversight body regarding risk management within the organization;
- managing quality within risk management; and
- reporting, escalating and communicating risk management issues to key stakeholders.
c) Organization units
Where there are organization units, departments and divisions, their managers should have the primary responsibility for managing risks on an operational basis, and for promoting risk awareness. In particular, each unit of the organization should:

- establish risk management objectives;
- clarify the organizational risk management strategy, risk appetite, assessment scales and management accountability framework at the unit level;
- ensure they have access to competent advice, as appropriate, to manage risks;
- implement the risk management process;
- take into account the risks that fall within their areas of responsibility, the possible implications of these on other parts of the organization, and the consequences other areas might have on them;
- ensure that risks are managed in a cost-effective way;
- formulate risk management indicators, so that progress toward risk management objectives can be measured;
- ensure that risks are evaluated as a regular meeting item to allow consideration of exposures and to re-prioritize activities in the light of risk analysis;
- monitor risk management action programmes;
- report in a systematic and timely way to senior management any perceived new, or changes to existing, risks or failures of existing control measures; and
- provide suitable arrangements for the exchange of relevant risk management information.

d) Internal audit
If the organization has an internal audit function, this may be accountable for providing the senior management with independent assurance on:

- risk management processes, both their design and how well they are working;
- management of key risks, including the effectiveness of the controls and other responses to these; and
- reliable and appropriate assessment of risk and reporting of risk and control status.

The organization’s risk and internal audit functions may operate independently. They should share information and coordinate their activities. The information shared may include:

- each function’s annual activity plans;
- methods of managing risks effectively;
- key risks;
- key control issues;
- output from risk management process activity and audits; and
- reporting and management information.
3.7 Risk management tools

The organization should have a suite of tools (a toolkit), which may include practices, techniques, templates, documents, systems and advice, that:

a) helps to develop and implement risk management in practice;
b) is aligned to the organization’s risk management framework, process and maturity;
c) is in keeping with the organization’s nature, scale, complexity and culture; and
d) assists in the development and distribution of risk management knowledge and expertise.

The organization should communicate information on the toolkit to those required to undertake risk management activities, together with guidance on where they can obtain an appropriate tool and who to contact for further assistance.

*NOTE* Annex B provides examples of risk management tools, and the part(s) of the risk management process to which they relate, and gives guidance on the selection of tools.

3.8 Risk appetite and risk profile

Considering and setting a risk appetite enables an organization to increase its rewards by optimizing risk taking and accepting calculated risks within an appropriate level of authority.

The organization’s risk appetite should be established and/or approved by the Board (or equivalent) and effectively communicated throughout the organization.

The organization should prepare a risk appetite statement, which may:

- provide direction and boundaries on the risk that can be accepted at various levels of the organization, how the risk and any associated reward is to be balanced, and the likely response;
- consider the context and the organization’s understanding of value, cost-effectiveness of management, rigour of controls and assurance process;
- recognize that the organization might be prepared to accept a higher than usual proportion of risk in one area if the overall balance of risk is acceptable;
- define the control, permissions and sanctions environment, including the delegation of authority in relation to approving the organization’s risk acceptance, highlighting of escalation points, and identifying the escalation process for risk outside the acceptance criteria, capability or capacity;
- be reflected in the organization’s risk management policy and reported upon as part of the organization’s internal risk reporting system;
- include qualitative statements outlining specific risks the organization is or is not prepared to accept; and
- include quantitative statements, described as limits, thresholds or key risk indicators, which set out how certain risks and their rewards are to be judged and/or how the aggregate consequences of risks are to be assessed and monitored.
The risk profile provides an overall picture of risk across an organization, within an organizational unit or for a defined area. The risk profile should convey the nature and level of risks the organization faces, the impact and likelihood of risk incidents on the organization and its stakeholders, and the effectiveness of controls in place to manage the risks. This may present an overview or a summary of the detailed risk documentation or show the full detail, whichever is most appropriate.

Both the risk appetite and risk profile should be monitored by the Board (or equivalent) and formally reviewed as part of the organization’s strategy and planning processes. This should consider whether the organization’s risk appetite remains appropriate to deliver the organization’s objectives in light of internal and external drivers and constraints.

3.9 Risk and consequence categorization and measurement

3.9.1 General
The organization should set and document its risk and risk consequence categories and risk criteria, and integrate these into the risk management framework.

3.9.2 Risk categories
The organization should develop risk categories that suit its size, purpose, nature, complexity and context, while taking into account the maturity of its risk management.

NOTE An explanation of risk categories is given in Annex A.

The risk categories, including those from stakeholders, should be communicated through the organization in order for all to share a common understanding.

3.9.3 Risk consequence categories
To allow consistent assessment, profiling and reporting of the consequences of actual and potential events, and to facilitate comparison across the organization, the organization should develop risk consequence categories that suit its size, purpose, nature, complexity and context, while taking into account the maturity of its risk management capability.

The risk consequence categories should be communicated through the organization in order for all to share a common understanding.

3.10 Risk criteria
To enable risks to be consistently assessed, the organization should develop risk criteria that suit its size, purpose, nature, complexity, management level and context, while taking into account the maturity of its risk management. A basic approach is to consider likelihood and consequence, and the time period over which consequences are assessed.
The organization's risk criteria should take into account its risk appetite and allow for all risks to be measured, including those that do not naturally lend themselves to numerical analysis.

The criteria should be communicated through the organization in order for all to share a common understanding of how risk is measured.

3.11 Risk communication

Senior management should ensure that appropriate communication processes are established and that information about risks and risk responses is communicated to stakeholders.

3.12 Risk reporting

The organization's risk reporting should be:

• based upon an understanding of the stakeholders’ needs, priorities and time scales, and aligned to their responsibilities;
• timely, concise, specific and reliable;
• sufficiently detailed that the stakeholders can gain an appropriate understanding of the key issues;
• integrated with other reporting processes where practical and appropriate;
• delivered in sufficient time to allow recipients to adequately review the content; and
• independently reviewed periodically to validate its quality and ensure it is aligned to its stakeholders.

The organization should tailor what it reports and how often to:

• provide assurance that the risk management process is operating effectively and risks are being managed; and
• enable risks and issues to be aggregated, prioritized and addressed appropriately.

The organization’s internal reporting should be aligned with its governance structure and allow the flow of risk information through the organization. The organization should identify the specific risk information, and its level of detail and frequency, that allows the components of the governance structure, management and individual risk owners to fulfil their roles. The structure and process for internal reporting should be documented, and a timetable developed detailing responsibilities and timescales.

The organization’s internal reporting system should enable it to:

• monitor:
  – the identification of new and emerging risks;
  – whether risks are being managed in accordance with the risk appetite;
  – the overall risk profile of the organization and key risks, including how they change over time;
  – the progress of actions to respond to key risks, and operation of key controls;
the effectiveness of the overall risk management framework and process, and adherence to the risk policy or policies; and
actual losses, lost opportunities and near misses;
- escalate and prioritize risks and resources;
- intervene and take action where necessary;
- identify significant internal and external changes, issues and events that might impact on the risk profile of the organization and require action;
- identify new and emerging opportunities for improvement; and
- highlight common problem areas/knowledge gaps and ensure wherever relevant that a common solution is developed, duplication is avoided, and knowledge is effectively transferred throughout the organization.

4 Risk management process

4.1 General

The risk management process should provide a systematic, effective and efficient way by which risks can be managed at different levels throughout the organization. It should be a continuous undertaking by the organization and its units as an integral part of their decision making, be and operated in accordance with the parameters that are set out by the risk management framework (see Figure 4).

Figure 4  The risk management process
The organization’s risk management process should, as a minimum, comprise the following steps:

- Risk context;
- Risk identification;
- Risk assessment;
- Risk response;
- Risk reporting;
- Risk review.

*NOTE* There are many tools for presenting and communicating the results of risk management; examples can be found in Annex B.

### 4.2 Risk context

Those managing risk should identify, monitor and take into account:

a) the context; and
b) the internal factors which influence the management of risks and the risks over which the organization can exercise some degree of control or response.

They should:

- define the scope and ground rules for the risk management process;
- review the relevant elements of the risk management framework;
- select appropriate procedures, tools and techniques, and a schedule for the risk management process;
- involve appropriate people at each stage; and
- establish relevant documentation.

### 4.3 Risk identification

#### 4.3.1 General

Risk identification should be approached methodically to ensure that, wherever possible:

- all significant *risk sources* potentially affecting the achievement of objectives are identified and recorded;
- risks are clearly defined, do not overlap, and there are no unintended gaps;
- threats and opportunities are addressed as appropriate;
- each risk’s cause is examined;
- the validity of assumptions is challenged;
- interaction/conflict between stakeholders and objectives, which can be a significant source of risk, is identified;
- the risks are owned; and
- existing risk responses perceived to be addressing the risks, and their owners, are identified.

Risks should be recorded consistently and explicitly to allow review and development of effective responses.
4.3.2 **Methods for identifying risks**

The process of identifying risks should be iterative and one of refining the output until it is appropriate and adequately reflects the risks. Reviews should be undertaken as the identification process progresses to ensure that it remains relevant and that risks are adequately recorded.

4.4 **Risk assessment**

4.4.1 **General**

The risk assessment stage should involve:

- analysis of individual risks;
- analysis (and quantification where relevant) of potential risk aggregation; and
- evaluation and prioritization.

Risk assessment should determine the level of and exposure to risk and provide input to decisions on where responses to reduce or exploit risk are necessary or likely to be worthwhile.

4.4.2 **Risk analysis**

A risk might have a number of consequences, some positive and some negative. Managing the risk and its consequences could change a consequence, potentially from negative to positive.

Risk analysis may be undertaken with varying degrees of detail depending upon the risk, the purpose of the analysis, and the information, data and resources available. Analysis may be qualitative or quantitative, or a combination of these.

Each risk should be analysed to an appropriate extent, considering its consequences, and summarized in terms of the consequences arising and their likelihood.

Risk analysis should be an iterative process, being repeated as more data become available. It may take into account the inherent risk, the controls in place and how well these mitigate the risk, and be undertaken in accordance with the risk criteria.

**NOTE** Resources in an organization are finite and an understanding of inherent risk might help to ensure that the response is proportionate to the overall exposure. It can help to identify and guard against over-control. It might also help the organization to understand what its full exposure could be if controls fail, and therefore recognize the contribution of certain controls to overall risk mitigation.

4.4.3 **Analysis of inter-related risk**

The initial set of risks should be reviewed and revised to take account of instances where links between risks or common risk responses suggest that risks could be split or aggregated, or considered in groups. Risks that are interlinked may be aggregated or considered together, while risks that contain independent elements may be split up. Also, risks that are addressed by a common response may be aggregated or grouped, while risks that have elements addressed by separate responses may be split.
4.4.4 Risk evaluation and prioritization

Those managing risk should prioritize the analysed risks whilst also taking into account how soon the risks might occur (proximity) and manageability.

The risk evaluation process should compile/calculate risk profiles by appropriately combining/aggregating analysed risks, and compare levels of risk with the risk appetite.

Evaluation and prioritization of risks should take account of the context of the risks and include consideration of the possible acceptance or rejection of the risks by stakeholders (see Annex E).

This information should be used to inform and facilitate decisions about whether to respond to risks and how to set priorities.

4.5 Responding to risks

4.5.1 Understanding existing risk responses

Existing risk responses, including controls and retained residual risk, should be ascertained, documented and understood. Controls should be mapped to the risks to clarify the residual risk currently being retained. Residual risk reflects inherent risk and the effect of all relevant controls, but residual risk levels may be estimated directly from evidence of past risk occurrence.

4.5.2 Developing ideas for changes to risk responses

At each iteration of the risk management process, ideas for possible improvements (changes) to controls relevant to the risks under consideration should be developed in sufficient detail to inform decision making about what changes to implement. These changes may include implementing additional controls, removing controls and using different controls, or a decision may be taken to continue with no controls at all. Controls may be actions that are repeated, either regularly or in response to events, or they may be one-off actions or decisions. A control may be implemented to:

- avoid risk;
- seek risk (take opportunity);
- modify risk;
- transfer risk; or
- retain risk.

NOTE 1 It is often worth gathering more information about risks.

NOTE 2 Further information on possible controls is given in Annex C.

Consideration should be given to the work needed to develop and implement the possible control changes, as well as to operate the controls.

Controls may be considered individually, but controls considered as an integrated system are likely to be more effective and efficient.
4.5.3 Deciding which control changes to make
When deciding which control changes to implement, those managing risk should assess:

a) the possible net benefits compared with the cost of implementing and operating the controls, taking into account the effects on all risks modified by each control;

b) the relative cost-benefit of different control changes considered;

c) any legal or regulatory requirements or social responsibility factors that might override a cost-benefit analysis and necessitate a specific control change; and

d) any additional risks that might be introduced by a particular control change.

NOTE Analysis of costs and benefits need not be measured purely in financial terms or be fully quantified.

Control change decisions should take into account the perceptions and concerns of stakeholders.

Changes to controls should be chosen that will provide reasonable assurance of keeping risk within the risk appetite.

All changes to controls and the resulting retained residual risk should be appropriately authorized by the organization.

4.5.4 Managing changes to controls
Those managing risk should prioritize changes to controls, taking into account the impact on other activities and the availability of resources.

The control changes selected should be allocated to risk response owners and a schedule for their implementation should be prepared. Progress towards implementation of control changes should be monitored.

The controls implemented should be documented.

4.5.5 Monitoring performance of controls
After control changes have been implemented and it becomes possible to gather data on the actual residual risk, the level of residual risk should be assessed. The same decision process should be used to decide whether to retain the residual risk or whether pursuing further control changes is worthwhile.

The process should be repeated until the level of residual risk is within the risk appetite and pursuing further control changes does not seem worthwhile.

The organization should monitor and test its controls to ensure:

- they have a named owner;
- they are defined, communicated and understood;
- their implementation did not introduce any unacceptable additional risks;
- they are operating as designed, each is worthwhile, and collectively they managed the risk to an acceptable agreed level;
- they remain cost-effective; and
that where deficiencies in the implementation or operation of controls are identified:

- the implications of control deficiencies not being remedied are established and options for resolution are identified;
- they are reported so that the consequence for the risk profile can be assessed; and
- the resolution of control deficiencies is planned and carried out.

NOTE Assurance as to the effectiveness of controls may take a variety of forms and range from self-assessment and internal audit to detailed reviews by independent external experts. Relevant evidence on controls’ effectiveness is usually available from routine monitoring of activities.

4.6 Risk management process reporting

The key outputs from the risk management process should be communicated to the relevant stakeholders.

Individual risk management process level reporting should provide an appropriate level of detail, and be specific, relevant, timely and reliable. This may include:

- the status of key risks identified by the process, highlighting:
  - any material changes that alter their likelihood of occurring and/or their consequences, particularly if these are likely to affect what responses are worthwhile; and
  - any risk(s) greater than the risk appetite (risk tolerance or limit);
- the status of risk responses for key risks, for example where progress is behind agreed target or is significantly threatened;
- any significant emerging risks that need to be assessed and monitored;
- the underlying causes/sources of risk(s), e.g. a particular activity or process;
- a description of the uncertainty related to a particular activity, process or event;
- the possible consequence(s) of risks, described in terms of the effect on a business, activity or project, rather than just the specific consequence, e.g. financial loss/gain;
- the timing of risks;
- the dates risks were raised, in order to monitor ageing of risks with respect to the progress of mitigation;
- the likelihood of a risk occurring (see 4.4.2);
- the link between an identified source(s) of risk and the relevant performance objectives;
- the link to other risks;
- existing risk responses;
- proposed actions to improve responses; and
- the risk owner(s) and risk response owner(s) (see 3.6.4).
4.7 Risk review

Those managing risk should regularly review the output from the risk management process to ensure it remains valid, reflects changes in the context (see also 4.2) and supports better informed and, therefore, better decisions. Specifically, they should:

- consider:
  - the risk profile and key risks identified by the process and how they are changing over time;
  - the progress of actions to treat key risks and the operation of key controls;
  - whether controls remain aligned to risks, according to the organization's method of recognizing risk in decisions;
  - whether key risks are being managed within the risk appetite;
  - whether risks are closed where the point at which they might have occurred has passed or where they have been fully mitigated;
- reprioritize resources; and
- escalate risk management issues.

5 Developing risk management activities

5.1 General

The risk management development activities should provide a systematic, effective and efficient way by which risk management can be embedded and maintained throughout the organization. These activities should, as a minimum, comprise the following steps:

- planning;
- implementation and maintenance;
- monitoring, reviewing and continual improvement; and
- reporting.

5.2 Risk management development planning

5.2.1 Preliminaries

The organization should:

- utilize the risk management framework to identify key competency requirements;
- consult with its stakeholders to understand their capability and expectations;
- recognize the constraints and the organization’s capacity to deliver;
- consider its existing processes and understanding of risk management;
- devise and implement a strategy for meeting a desired level of capability in a way that is efficient for the organization; and
• leverage existing capabilities, resources, processes and systems of the organization.

5.2.2 Establishing context
The organization should establish the external and internal context of risk management development to ensure that the risk management framework is appropriate.

5.2.3 Identifying obstacles to implementation
The organization should identify weaknesses in its existing risk management framework, including weaknesses in elements that might hinder development of other elements, such as:
• limited commitment and resources from the Board (or equivalent);
• lack of clear delineation of responsibility, accountability and/or ownership;
• failure to embed risk management in the culture; and
• the person charged with implementing risk management having a limited/ambiguous/no mandate or limited skills.

5.2.4 Developing objectives and plans
The organization should develop objectives for risk management, plans for embedding and maintaining risk management throughout the organization, and plans for all other elements of the risk management framework. This should include establishing or revising:
• the risk management strategy; and
• the risk management policy, including plans for risk management processes.

5.3 Risk management implementation and maintenance
The actions planned to embed and maintain risk management throughout the organization should be allocated owners, and a schedule for their implementation should be prepared. The actions should be taken and progress in implementing the changes should be monitored.

5.4 Risk management monitoring, review and continual improvement

5.4.1 Continual improvement
The organization should continue to improve the effectiveness of its risk management framework through, for example:
• learning from risk events and the application of controls (see Annex C);
• internal audit (if an internal audit function is present); and
• a review process (see 5.4.2),
5.4.2 Monitoring and review

The organization should ensure that changes to the context, or changes to other factors affecting the suitability or cost of risk management, are identified and addressed.

A review process should be undertaken, as a minimum annually, to determine whether:

- the framework and processes are fit-for-purpose and aligned to the objectives and priorities of the organization;
- the framework and processes adopted resulted in what was intended;
- relevant stakeholders are receiving adequate reporting to enable them to discharge their roles and responsibilities in the governance structure;
- people across the organization have sufficient risk management skills, knowledge and competence, in line with the risk role/risk element of a role they are required to perform on a daily basis;
- the risk management resources are adequate;
- lessons have been learned from actual losses, near misses and opportunities that were identified in advance, occurred, and yet were not acted on; and
- overall, current risk management maturity and capability achieve the objectives set out in its risk management strategy.

NOTE 1 Further information on assessing risk management maturity is given in Annex D.

NOTE 2 The review may take a variety of forms and range from self-assessment and internal audit to detailed reviews by independent external experts.

5.4.3 Learning from risk events

A key mechanism for improving risk management awareness, knowledge, capability and future performance is to ensure that the organization learns from risk events.

The organization should review risk occurrences in a timely fashion to identify emerging trends that might need to be addressed. This may involve the use of a loss event database.

The organization should consider actively reviewing risk occurrences and ensuring that, where appropriate, these are adequately reported and recorded. The following may be considered during a review:

- what happened;
- how and why the risk occurrence came about;
- what action has been taken (if any) subsequent to the risk occurrence;
- the likelihood of the risk occurrence happening again;
- any additional responses or steps to be taken; and
- key learning points and who they need to be communicated to.

The organization should also consider readily available information about the risk occurrences of relevant external organizations, e.g. industry/sector peers, to determine whether there is a significant
likelihood of the organization experiencing a similar occurrence, and whether action should be taken.

5.5 **Risk management development reporting**

The organization might be required, or may decide, to report to applicable stakeholders, setting out its risk management policy and framework, and their effectiveness. The organization should understand specific external risk reporting obligations, time scales and requirements, which may include:

- the organization’s risk management framework, including management responsibilities for risk management;
- the key risks and the primary control systems in place to manage these;
- the monitoring and review of control systems in place; and
- any major deficiencies uncovered and the steps taken to deal with them.
Annex A (informative) **Risk categories**

Risks arise in all areas of the organization and derive from a variety of different sources. Identifying, analysing, evaluating and responding to different kinds of risks that could influence the organization’s ability to achieve its objectives often require specific skills, competences, knowledge and perspectives.

Grouping similar kinds of risks together into appropriate risk categories helps to:

- define the scope of risk management in an organization;
- provide a structure and framework for risk identification;
- identify areas of strength or weakness within an organization;
- aggregate and map similar kinds of risks across units or the organization as a whole;
- allocate management responsibilities for the response to and management of risk;
- identify, build and obtain sufficient internal/external skills, knowledge and expertise to manage risks throughout the organization;
- provide a platform to build more advanced measurement methodologies as risk tools and practices mature, which is necessary for the allocation of funds to risk;
- overcome potential organizational silos; and
- allocate accountability.

The number and type of risk categories employed, and the level of granularity within categories, should suit the organization’s size, purpose, nature, complexity and context, and reflect the maturity of its risk management. While risk categories differ between organizations, risk categories in common usage include:

- **strategic risk**;
- **programme risk**;
- **project risk**;
- **financial risk**; and
- **operational risk**.

Risk categories can be influenced by legal and regulatory requirements or sector practice.
Risk management tools

Tools enable those engaging in risk management to capture information in a consistent way, engage with stakeholders, provide more thorough and reliable analysis results, make explicit the risks associated with different options, prioritize actions, improve communication and produce a reliable audit trail. Although tools are not an end themselves, they can be powerful aids to support effective risk management.

There is a considerable range of tools to choose from. Each is suitable for a specific task and not all will be needed at the same time. While the tool(s) to be used is sometimes immediately apparent, the choice of others is not always straightforward.

Table B.1 illustrates some of the more commonly used tools for stages of the risk management process.

The organization's tool selection is based upon:

- the intended user or function and the desired output;
- the purpose or goal of undertaking the risk management activity, such as calculating a contingency or selecting an option;
- the stage of the activity being undertaken;
- the intended user's competence and experience with the tool's application;
- the amount of time available for the risk study;
- the level of detail that the sponsor requires;
- the use to which the risk management outputs will be put;
- the familiarity of the participants with the tool(s);
- the degree to which risk management is embedded in the organization;
- the willingness of the participants to use the tools;
- the availability of information or data on the use of the tools in a productive way;
- the ability of the intended user to understand the benefits of using the tools; and
- the ease of use, suitability, cost and applicability of the tools.
### Table B.1  Examples of risk management tools (including techniques)

<table>
<thead>
<tr>
<th>Tool</th>
<th>Identification</th>
<th>Assessment</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk questionnaires</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk checklists/prompt lists</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management workshop</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Nominal group technique</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk breakdown structure</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Delphi technique</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Process mapping</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Cause-and-effect diagrams</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk mapping/Risk profiling</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Risk Indicators</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Brainstorming/“thought shower” events</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Interviews and focus groups</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>“What if?” workshops</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Scenario analysis/scenario planning/horizon scanning</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Hazard and operability study (HAZOPs)</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Failure mode effects analysis (FMEA)</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>PESTLE (political, economic, sociological, technological, legislation and environment) analysis</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SWOT (strengths, weaknesses, opportunities and threats) analysis</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Stakeholder engagement/matrices</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Risk register/database</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Project profile model (PPM)</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Risk taxonomy</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Gap analysis: Pareto analysis</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Probability and consequence grid/diagrams (PIDs)/Boston grid</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Probability trees</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Expected value method</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Risk modelling/risk simulation (Monte Carlo/Latin Hypercube)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flow charts, process maps and documentation</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Fault and event tree modelling</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Stress Testing</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Critical path analysis (CPA) or critical path method (CPM)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sensitivity analysis</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Cash flow analysis</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Portfolio analysis</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Cost-Benefit analysis</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Utility theory</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Visualization techniques:</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Heat maps, RAG status reports, Waterfall charts, Profile graphs, 3D Graphs, Radar chart, Scatter diagram.</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Annex C (informative)  Effects of controls

C.1 Avoid risk

Where risks cannot be influenced by the organization and/or cannot be managed to an acceptable level, the only option might be to not proceed with an activity or to withdraw from it. Risk avoidance may also be justified as a cost-effective way to manage a risk.

The option of avoiding an activity could be severely limited in the public sector, compared to the private sector, due to the obligation to provide certain services.

Withdrawing from an activity can be an important option in project management if it becomes clear that the costs of achieving the project objectives are too high, or that the objectives might not be realized irrespective of cost. In such a case, the response may be to terminate the project.

Avoiding risk can occur inappropriately if an organization or individual is unnecessarily risk averse. In these circumstances avoiding a risk might increase the importance of other risks or result in failure to make the most of opportunities.

C.2 Seek risk

Risks with desirable potential consequences can make an activity more attractive and lead an organization to seek that activity, just as risks with undesirable potential consequences can motivate avoidance.

There are more potential opportunities than is sometimes appreciated but appropriate focus, procedures and language can allow them to be identified and included in decision making.

C.3 Modify risk

The majority of risks are managed in this way. The purpose of modification is to optimize potential opportunities and minimize threats. Risk modification may involve changing:

- the likelihood of a risk, to increase it if the risk’s overall consequence would be positive and decrease it if the risk’s overall consequence would be negative;
- the consequences if the risk occurs, shifting these in a positive direction; and
- both the likelihood and consequences.

A number of measures to modify a risk may be considered and implemented, either individually or in combination.

C.4 Transfer risk

For some risks the most appropriate response may be to transfer them (often referred to as “risk sharing”). This might be done by conventional insurance, by contractual arrangements, or through arrangements such as partnerships and joint ventures where exposures and liabilities are shared, as well as the potential for gain.

It is important to recognize the limitations of risk transfer. Where risks are transferred, in whole or in part, the organization transferring
the risk acquires a new risk: the organization to which the risk is transferred might not manage the risk effectively. Many risks can never be transferred completely; for example:

- insurance might provide the funds to rebuild a production plant which has been destroyed by fire, but it does not solve the problem of how to maintain the business in the interim;
- outsourcing the operation of IT systems to a specialist service provider does not eliminate the risk of IT systems failure or remove the need to have contingency plans if the systems fail; and
- contracting other organizations to manufacture products or supply services on the organization’s behalf does not remove the risk to the organization’s reputation; in many cases, it is of no concern to a customer that the failure was with a contractor.

In practice, risk transfer is used in combination with one or more of the other risk response options.

C.5 Retain risk

Retaining a residual risk means planning no further action to respond to it, for the time being. This might be done because no further worthwhile actions can be devised and the risk is within the risk appetite, or it might be because the only remaining responses are unacceptable for some reason. Risk retention has to be a conscious decision based on the results of the risk analysis and evaluation process, but might need to be reviewed in future if circumstances change. Retention of risks by default because of a failure to identify or appropriately manage them ought not to be tolerated.
Annex D (informative)  Risk maturity models

Maturity models provide a well-structured and detailed guide to facilitate the progressive incremental improvement of risk management capability. With the aid of a maturity model, the organization can set a realistic long term strategy for the organization’s approach to risk management.

Maturity models enable the organization to document, communicate and implement process improvement. They contain the essential elements of effective processes and describe an evolutionary improvement path from ad hoc, immature processes to disciplined, mature processes providing greater benefit.

Maturity models are typically composed of four or five levels of maturity and the quality of the processes within each level is described by the use of assessment criteria. Though there is no limit on the number of criteria that might be adopted, models commonly contain fewer than ten to avoid becoming unwieldy.

The current level of maturity attained can be determined by asking a series of initial questions, including the following.

- Has risk management been made mandatory by the Board (or equivalent)/senior management?
- Are the risk management roles and responsibilities identified and established?
- Has a risk management policy been prepared?
- Has the risk management policy been communicated?
- Has a risk management process been defined?
- Is there a plan for embedding risk management?
- Have reporting requirements been made explicit?
- Are appropriate tools being used to support risk management?
- Is risk management information captured in a consistent way?
- Is the frequency at which risk management is carried out appropriate to the organization’s business cycle?
- Do the appropriate organizational activities include risk management?
- Is risk management being used to support the pursuit of opportunities?
- Has risk management increased Board (or equivalent) confidence in pursuing new opportunities?
- Is there a process of continual improvement?
Annex E (normative)

Incorporating potentially positive consequences of risk

E.1 Potentially positive consequences

The definition of “risk” used by this Code of Practice and ISO Guide 73 reflects the modern approach to risk management that includes good events as well as bad.

Incorporating potentially desirable consequences requires the approach to risk management to have appropriate features.

E.2 Language

Where an organization chooses to include potentially positive consequences in its risk management process it should ensure that the words it uses do not introduce bias. In particular, since most people identify the word “risk” with undesirable potential events only, the technical view of risk should be explained effectively or alternative language used, e.g. referring to risks as “potential problems and potential opportunities”, “upside and downside risks”, or as “uncertainties”. When identifying risks, circumstances that drive risk can be described as “threats and opportunities”.

E.3 Characterizing risks

When risks are characterized in terms of consequences and likelihoods the methods used should be appropriate for the intended types of risk. It should be possible to characterize and communicate those risks whose consequence is predominantly desirable, as well as those whose consequence is predominantly undesirable.

Where the consequence of a risk, if it occurs, could be anywhere within a range it might be that this range includes desirable and undesirable consequence levels. Summarizing this range of consequences using a measure such as its average could be misleading because desirable and undesirable possibilities could balance, leaving the risk level apparently as zero even though important uncertainty exists. Alternatives include presenting the range in some way and using a measure of spread. In quantitative risk assessments the standard deviation is often used as a measure of spread.

E.4 Incorporating risks in decisions

The organization should have clearly defined approaches to incorporating risk in decisions. These should ensure that decision making involves consideration of all potential consequences, including those better and those worse than expected or planned. If a course of action carries a risk whose potential consequence is positive then this will make the course of action more attractive. Further, if that potential consequence is increased and still positive then this will make the course of action even more attractive. This is why consideration of costs and net benefits of risk treatments is necessary in addition to any comparison with a risk appetite.
Glossary

For the purposes of this British Standard, the following definitions apply.

**Board (or equivalent)**
organization’s governing body

*NOTE* This includes a board of directors, head of a legislative body or agency, supervisory board, or the board of trustees or governors of a not-for-profit organization

**business continuity management**
holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities

[BS 25999, modified]

**consequence**
outcome of an incident that will have an effect on an organization’s objectives

*NOTE 1* There can be a range of consequences from one incident.

*NOTE 2* A consequence can be certain or uncertain and can have positive or negative impact on objectives.

**context**
environment in which the organization seeks to achieve its objectives

[ISO Guide 73, modified]

**control**
measure to modify risk

*NOTE 1* Controls are the result of risk treatment.

*NOTE 2* Controls include any process, policy, device, practice, or other actions designed to modify risk.

[ISO Guide 73]

**enterprise risk management**
approach to managing all of an organization’s key business risks and opportunities with the intent of maximizing stakeholder value

[Risk and Insurance Management Society]

**event**
occurrence or change of a particular set of circumstances

*NOTE 1* Nature, likelihood and consequence of an event cannot be fully knowable.
NOTE 2  An event can be one or more occurrences, and can have several causes.

NOTE 3  Likelihood associated with the event can be determined.

NOTE 4  An event can consist of a non-occurrence of one or more circumstances.

NOTE 5  An event with a consequence is sometimes referred to as an “incident”.

NOTE 6  An event where no loss occurs may also be referred to as a “near-miss”, “near-hit”, “close call” or “dangerous occurrence”.

ISO Guide 73
exposure
extent to which an organization is subject to an event
ISO Guide 73
incident
event in which a loss occurred or could have occurred regardless of severity
inherent risk
exposure arising from a specific risk before any action has been taken to manage it
key risk
most significant risks or those on which the Board or equivalent focuses
level of risk
magnitude of a risk expressed in terms of the combination of consequences and their likelihood
ISO Guide 73
likelihood
chance of something happening
NOTE  The word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, and described using general terms (such as unlikely, likely, almost certain) or mathematically (such as a probability or a frequency over a given time period).
ISO Guide 73, modified
near miss
operational failure that did not result in a loss or give rise to an inadvertent gain
operational risk
risk of loss or gain, resulting from inadequate or failed internal processes, people and systems or from external events
programme risk
risk associated with transforming strategy into solutions via a collection of projects

project risk
risk relating to delivery of a product or service, usually with the constraints of time, cost and quality

residual risk
risk remaining after risk treatment
[ISO Guide 73, modified]

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, organization-wide, project, product and process.
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.
[ISO Guide 73]

risk acceptance
informed decision to take a particular risk
NOTE 1 Risk acceptance can occur without risk treatment or during the process of risk treatment.
NOTE 2 Risk acceptance can also be a process.
NOTE 3 Risks accepted are subject to monitoring and review.
[ISO Guide 73]

risk aggregation
process to combine individual risks to obtain a more complete understanding of risk
[ISO Guide 73]

risk analysis
process to comprehend the nature of risk and to determine the level of risk
NOTE Risk analysis provides the basis for risk evaluation and decisions about risk treatment.
[ISO Guide 73]
risk appetite
amount and type of risk that an organization is prepared to seek, accept or tolerate
[ISO Guide 73, modified]

risk assessment
overall process of risk identification, risk analysis and risk evaluation

risk avoidance
decision not to be involved in, or to withdraw from, an activity based on the level of risk
[ISO Guide 73, modified]

risk criteria
terms of reference against which the significance of a risk is evaluated

NOTE 1 Risk criteria are based on the context, and are regularly reviewed to ensure continued relevance.

NOTE 2 Risk criteria can be derived from standards, laws and policies.

[ISO Guide 73, modified]

risk evaluation
process of comparing the results of risk analysis against risk criteria to determine whether the level of risk is acceptable or tolerable

NOTE Risk evaluation assists in the decision about risk treatment.

[ISO Guide 73]

risk financing
form of risk treatment involving contingent arrangements for the provision of funds to meet the financial consequences should they occur

[ISO Guide 73, modified]

risk identification
process of finding, recognizing and describing risks

NOTE 1 Risk identification involves the identification of risk sources, events and their causes and their potential consequences.

NOTE 2 The identification can involve historical data, theoretical analysis, informed and expert opinions, and the stakeholders’ needs.

[ISO Guide 73]

risk management
coordinated activities to direct and control an organization with regard to risk

[ISO Guide 73]
risk management framework
set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organization
NOTE 1 The foundations include the objectives, mandate and commitment to manage risk.
NOTE 2 The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.
NOTE 3 The risk management framework is embedded within the organization’s overall strategic and operational policies and practices.
[ISO Guide 73]

risk management governance
system, structures, tone and behaviours by which the organization is directed and controlled, and accountabilities clearly assigned
NOTE Corporate governance permits decisions to be effectively made, objectives set and performance monitored to ensure the efficient and effective use of resources and safeguard assets.

risk management policy
overall intentions and direction of an organization related to risk management
[ISO Guide 73]

risk management process
systematic application of management policies, procedures and practices to the tasks of communicating, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk
[ISO Guide 73]

risk mitigation
measures taken to reduce an undesired consequence
[ISO Guide 73]

risk register
record of information about identified risks

risk owner
person or entity with the accountability and authority for managing the risk and any associated risk treatments
[ISO Guide 73]
risk profile
description of a set of risks

NOTE The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

[ISO Guide 73]

risk response
acceptance of a risk or action taken to address it

risk retention
acceptance of the benefit of gain, or burden of loss, from a particular risk

NOTE 1 Risk retention includes the acceptance of residual risks.
NOTE 2 The level of risk retained may depend on risk criteria.

[ISO Guide 73]

risk sharing
form of risk treatment involving the agreed distribution of risk with other parties

[ISO Guide 73, modified]

risk source
anything which alone or in combination has the intrinsic potential to give rise to risk

[ISO Guide 73]

risk tolerance
organization’s readiness to bear the risk after risk treatments in order to achieve its objectives

NOTE Risk tolerance can be limited by legal or regulatory requirements.

risk transfer
sharing with another party the burden of loss or benefit of gain for a risk

NOTE This might be achieved through legislation, contract, insurance or other means.

risk treatment
process of developing, selecting and implementing controls

NOTE 1 Risk treatment can involve:
— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
— seeking an opportunity by deciding to start or continue with an activity likely to create or enhance the risk;
— removing the source of the risk;
— changing the nature and magnitude of likelihood;
— changing the consequences;
— sharing the risk with another party or parties; and
— retaining the risk by choice.

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as risk mitigation, risk elimination, risk prevention, risk reduction, risk repression and risk correction.

[ISO Guide 73]

stakeholder
person or group concerned with, affected by, or perceiving themselves to be affected by an organization

NOTE A decision maker is also a stakeholder.

strategic risk
risk concerned with where the organization wants to go, how it plans to get there, and how it can ensure survival
Bibliography

Standards publications
BS 25999, Business continuity management
ISO 31000, Risk management — Principles and guidelines on implementation (in preparation)
ISO/IEC CD 2 Guide 73 (1 April 2008), Risk management — Vocabulary

Other publications
British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7400

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

You may also buy directly using a debit/credit card from the BSI Shop on the website www.bsigroup.com/shop

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library.

Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048 Email: info@bsigroup.com

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001 Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at www.bsigroup.com/BSOL

Further information about BSI is available on the BSI website at www.bsigroup.com

Copyright

Copyright subsists in all BSI publications. BSI also holds the copyright, in the UK, of the publications of the international standardization bodies. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI.

This does not preclude the free use, in the course of implementing the standard of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained. Details and advice can be obtained from the Copyright & Licensing Manager.

Tel: +44 (0)20 8996 7070 Email: copyright@bsigroup.com

raising standards worldwide™