BS 31100:2011

Risk management – Code of practice and guidance for the implementation of BS ISO 31000

BS 31100:2011

Risk management – Code of practice and guidance for the implementation of BS ISO 31000

Publishing and copyright information

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

ISBN 978 0 580 71607 2

ICS 03.100.01

The following BSI references relate to the work on this standard:
Committee reference RM/1
Draft for comment 11/30228063 DC

Publication history

First published October 2008
Second (present) edition, June 2011

Amendments issued since publication

Date	Text affected

Contents

Annexes

List of figures

List of tables

Summary of pages

This document comprises a front cover, an inside front cover, pages i to iv, pages 1 to 46, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard was published by BSI and came into effect on 30 June 2011. 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.

Supersession

BS 31100:2011 supersedes BS 31100:2008, which is withdrawn.

Relationship with other documents

BS ISO 31000, *Risk management – Principles and guidelines on implementation*, and ISO/IEC Guide 73, *Risk management – Vocabulary*, were published after the first edition of BS 31100, so that there were some minor structural differences between the documents. This edition was drafted to be consistent with the principles and guidelines on risk management in BS ISO 31000:2009 (see Introduction), and to acknowledge 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.

The provisions in this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should".

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.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

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.

This page deliberately left blank

Introduction

This code of practice gives recommendations for implementing the principles and guidelines on risk management in BS ISO 31000:2009.

This edition of BS 31100 closely matches the structure, terminology and diagrams of BS ISO 31000:2009 and ISO Guide 73:2009 to make it easier to use the three documents side by side. This edition also expands on the recommendations of BS 31100:2008.

The principles in BS ISO 31000:2009 are as follows.

a) Risk management creates and protects value.

b) Risk management is an integral part of all organizational processes.

c) Risk management is part of decision-making.

d) Risk management explicitly addresses uncertainty.

e) Risk management is systematic, structured and timely.

f) Risk management is based on the best available information.

g) Risk management is tailored.

h) Risk management takes human and cultural factors into account.

i) Risk management is transparent and inclusive.

j) Risk management is dynamic, iterative and responsive to change.

k) Risk management facilitates continual improvement of the organization.

The recommendations in this code of practice will help organizations implement these principles in a way that is right for each organization. The recommendations are more practical and specific than the principles and guidelines, but they focus on the key aspects of management and allow for variations in the detail of techniques.

Risks are best managed by people following a defined risk management process. In large organizations there could be many groups and many processes, each with its own scope, meetings, documents and methods. This could be because they are working at different management levels in the organization and have different perspectives (see Figure 1), are working in different organizational sub-units, or are focusing on different types of risks.

The approach recommended here is to provide an outline risk management process that can be followed and interpreted so that each group works in a way that is appropriate for them, and there is consistency and communication across the organization.

Each example of a risk management process within an organization is called an instance of the risk management process.

The outline risk management process is just one component of a broader risk management framework that also contains activities to govern one or more instances of the risk management process and to drive improvements over time.

The recommendations cover the whole organization and all risks. This includes outcomes that are better than expected, as well as those that are worse than expected. In keeping with the definition of risk as ”the effect of uncertainty on objectives” the approach encourages people to think widely about what might happen, not just to look for potential dangers. It also encourages greater awareness of uncertainty.

This is achieved using a process and language that apply equally to all risks. For example, risks are "modified" by controls rather than "mitigated" because a risk whose consequences are mostly desirable is one to promote or exploit rather than reduce.

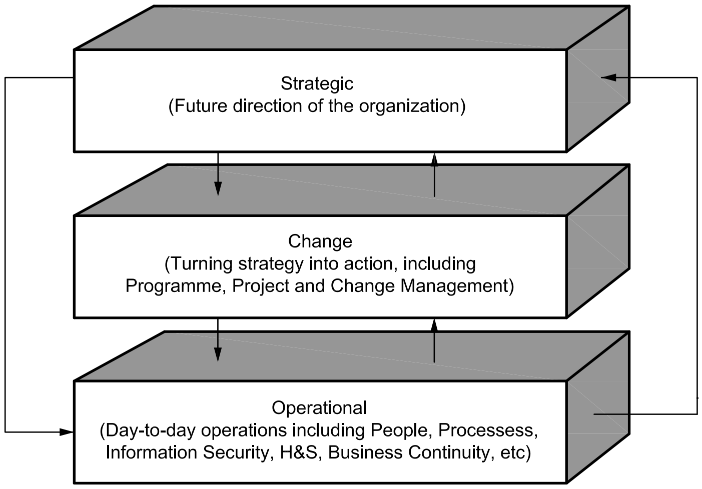
EXAMPLE

A major construction project on a city site had very little land for storing materials and so needed many costly lorry deliveries. There was space on an adjacent site where another developer was working. If a deal could be made it would be possible to use that space to store materials. This possibility was recorded as a risk with predominantly positive consequences, and evaluated. Although there would be an up-front commitment to the other developer, there were possible beneficial consequences from lower transport costs and reduced likelihood of interruptions to work due to late deliveries. Actions were identified to increase the likelihood of the risk being realized, such as working out delivery times and access routes that would avoid interference between the projects. Subsequently, the risk was realized: a deal was made benefiting both developers.

Risk management needs to be integrated into all management activities. This code of practice gives recommendations on how to achieve this integration.

The recommendations in this British Standard have been written for organizations of all types and sizes, and include guidance on how to choose an approach that is appropriate. Table 1 gives examples of how large and small organizations might tailor their risk management.

Figure 1 **Risk management perspectives**


Strategic
(Future direction of the organization)
Change
(Turning strategy into action, including
Programme, Project and Change Management)
Operational
(Day-to-day operations including People, Processess,
Information Security, H&S, Business Continuity, etc)

Key

□ Set of activities

→ Communication

Table 1 **Examples of tailoring**

Point of difference	Small organization	Large organization
Business	Law partnership	Food manufacturer
Employees	10	15,000
Business units and locations	One business unit in one office	36 business units in 27 countries
Ongoing projects	None (presently)	Hundreds
Risk management framework description	A 12-page document	A database with several documents and tools, including risk analysis software
Delegation of risk management activities by the board (or equivalent)	Very little – the partners do almost everything	The main board delegates risk management activities extensively to sub-committees, a risk management support team, and business unit management. Extra assurance is provided by internal auditors.
Instances of the risk management process	One	Hundreds due to the many business units and projects
Detail in procedures for initiating and terminating instances of the risk management process	Described in one paragraph just in case a project is started that justifies it	Described in detail and this activity is tracked using a database
Range of risk analysis techniques	Almost entirely by judgement and conversations among the partners	Varies from conversations and judgement to mathematical modelling (particularly for food safety risks and commodity price hedging) and reliability analyses based on models of manufacturing systems
Quantity and usefulness of risk data generated by the business	Low volume and of limited use	Huge volume, providing a strong basis for quantitative analyses
Detail in procedures for internal reporting about risk management	Described in one paragraph as a topic in the regular partner meetings	Described in detail, with committees involved, help from the risk management support team, and a computer system
Required external reporting about risk management	Limited – for certain activities	Extensive, mainly because of stock market listings and health and safety laws

1 Scope

This British Standard gives recommendations for implementing the principles and guidelines in BS ISO 31000:2009, including the risk management framework and process. It 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 is intended for use by anyone with responsibility for, or involved in, any of the following:

a) ensuring an organization achieves its objectives;

b) ensuring risks are proactively managed in specific areas or activities;

c) overseeing risk management in an organization;

d) providing assurance about the effectiveness of an organization’s risk management; and/or

e) reporting to stakeholders, e.g. through disclosures in annual financial statements, corporate governance reports and corporate social responsibility reports.

2 Terms and definitions

For the purposes of this British Standard the following terms and definitions apply.

2.1 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.

2.2 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]

2.3 communication and consultation

continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk

NOTE 1 The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of the management of risk.

NOTE 2 Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:

- *a process which impacts on a decision through influence rather than power; and*
- *an input to decision-making, not joint decision-making.*

[ISO Guide 73]

2.4 consequence

outcome of an event (**2.6**) affecting objectives

NOTE 1 An event can lead to a range of consequences.

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

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

NOTE 4 Initial consequences can escalate through knock-on effects.

[ISO Guide 73]

2.5 control

measure that is modifying risk

NOTE 1 Controls include any process, policy, device, practice, or other actions designed to modify risk.

NOTE 2 Controls may not always exert the intended or assumed modifying effect.

[ISO Guide 73]

2.6 event
occurrence or change of a particular set of circumstances

NOTE 1 An event can be one or more occurrences, and can have several causes.

NOTE 2 An event can consist of something not happening.

NOTE 3 An event can sometimes be referred to as an "incident" or "accident".

NOTE 4 An event without consequences can also be referred to as a "near miss", "incident", "near hit" or "close call".

[ISO Guide 73]

2.7 exposure
extent to which an organization and/or stakeholder is subject to an event

[ISO Guide 73]

2.8 external context
external environment in which the organization seeks to achieve its objectives

NOTE External context can include:

- *the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;*
- *key drivers and trends having impact on the objectives of the organization; and*
- *relationships with, and perceptions and values of external stakeholders.*

[ISO Guide 73]

2.9 governance
system, structures, tone and behaviours by which the organization is directed and controlled, and accountabilities clearly assigned

NOTE Governance permits decisions to be effectively made, objectives set and performance monitored to ensure the efficient and effective use of resources and safeguard assets.

2.10 inherent risk
exposure arising from a specific risk before any action has been taken to manage it

2.11 instance of the risk management process
specific application of the risk management process described in the risk management framework to a specific, logical set of risks related to a particular area or activity of the organization

2.12 internal context
internal environment in which the organization seeks to achieve its objectives

NOTE Internal context can include:

- *governance, organizational structure, roles and accountabilities;*
- *policies, objectives, and the strategies that are in place to achieve them;*
- *the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);*
- *information systems, information flows and decision-making processes (both formal and informal);*
- *relationships with, and perceptions and values of internal stakeholders;*
- *the organization's culture;*

- *standards, guidelines and models adopted by the organization; and*
- *form and extent of contractual relationships.*

[ISO Guide 73]

2.13 level of risk

magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood

[ISO Guide 73]

2.14 likelihood

chance of something happening

NOTE 1 In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically [such as a probability or a frequency over a given time period].

NOTE 2 The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

[ISO Guide 73]

2.15 near miss

operational failure that did not result in a loss or give rise to an inadvertent gain

2.16 operational risk

risk of loss or gain, resulting from inadequate or failed internal processes, people and systems or from external events

2.17 programme risk

risk associated with transforming strategy into solutions via a collection of projects

2.18 project risk

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

2.19 residual risk

risk remaining after risk treatment

NOTE 1 Residual risk can contain unidentified risk.

NOTE 2 Residual risk can also be known as "retained risk".

[ISO Guide 73]

2.20 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).

[ISO Guide 73]

2.21 risk aggregation

combination of a number of risks into one risk to develop a more complete understanding of the overall risk

[ISO Guide 73]

2.22 risk analysis

process to comprehend the nature of risk and to determine the level of risk

NOTE 1 Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

NOTE 2 Risk analysis includes risk estimation.

[ISO Guide 73]

2.23 risk appetite

amount and type of risk that an organization is willing to pursue or retain

[ISO Guide 73]

2.24 risk assessment

overall process of risk identification, risk analysis and risk evaluation

[ISO Guide 73]

2.25 risk avoidance

informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk

NOTE Risk avoidance can be based on the result of risk evaluation and/or legal and regulatory obligations.

[ISO Guide 73]

2.26 risk criteria

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

NOTE 1 Risk criteria are based on organizational objectives, and external and internal context.

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

[ISO Guide 73]

2.27 risk evaluation

process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

NOTE Risk evaluation assists in the decision about risk treatment.

[ISO Guide 73]

2.28 risk financing

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

[ISO Guide 73]

2.29 risk identification

process of finding, recognizing and describing risks

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

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

[ISO Guide 73]

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

[ISO Guide 73]

2.31 risk management framework
set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization

NOTE 1 The foundations include the policy, 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]

2.32 risk management policy
statement of the overall intentions and direction of an organization related to risk management

[ISO Guide 73]

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

[ISO Guide 73]

2.34 risk modification
measures taken to change the characteristics of risks in desired ways

2.35 risk owner
person or entity with the accountability and authority to manage a risk

[ISO Guide 73]

2.36 risk profile
description of any 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]

2.37 risk register
record of information about identified risks

NOTE The term "risk log" is sometimes used instead of "risk register".

[ISO Guide 73]

2.38 risk reporting

form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management

[ISO Guide 73]

2.39 risk response

acceptance of a risk or action taken to address it

2.40 risk retention

acceptance of the potential 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 can depend on risk criteria.

[ISO Guide 73]

2.41 risk sharing

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

NOTE 1 Legal or regulatory requirements can limit, prohibit or mandate risk sharing.

NOTE 2 Risk sharing can be carried out through insurance or other forms of contract.

NOTE 3 The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.

NOTE 4 Risk transfer is a form of risk sharing.

[ISO Guide 73]

2.42 risk source

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

NOTE A risk source can be tangible or intangible.

[ISO Guide 73]

2.43 risk tolerance

organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives

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

[ISO Guide 73]

2.44 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.

2.45 risk treatment

process to modify risk

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;*
- *taking or increasing risk in order to pursue an opportunity;*

- *removing the risk source;*
- *changing the likelihood;*
- *changing the consequences;*
- *sharing the risk with another party or parties [including contracts and risk financing]; and*
- *retaining the risk by informed decision.*

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

NOTE 3 Risk treatment can create new risks or modify existing risks.

[ISO Guide 73]

2.46 stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by decision or activity

NOTE A decision maker can be a stakeholder.

[ISO Guide 73]

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

3 Framework

3.1 General

The organization should put in place a risk management framework. The components of its framework should support:

a) implementation and longer term development of risk management throughout the organization; and

b) ongoing management of one or more instances of its risk management process.

The extent to which the organization's risk management framework supports ongoing management of one or more instances of its risk management process should be tailored to its internal and external context (see Figure 2). In particular, a large organization, perhaps also with many projects, may find that multiple instances of its process are more appropriate than one large process (see Figure 3). Its framework should, therefore, include elements to maintain appropriate consistency between instances, initiate and terminate them when required (e.g. at the start of a new project or when a new business unit is created or acquired), and promote communication. These are not necessary for a small organization that expects to operate just one instance of its process.

EXAMPLE

Multiple instances of the risk management process might be needed because of outsourcing. A UK-based funds management organization executes thousands of funds transfers a day, having to ensure their timeliness, accuracy, probity and traceability. The processing work has been outsourced to India for some years and more recently the supervision of this has been outsourced to another company in the organization's home country. Consequently, risk management of this work is covered by four instances: 1) the enterprise-wide level, 2) in-house monitoring of funds transfers, 3) outsourced monitoring of funds transfers, and 4) the company in India that processes the transfers. Information flows up and down between these and the entire risk management effort is justified by the strategic importance of the identified risks.

Figure 2 **Relationships between the context, principles, framework and process**

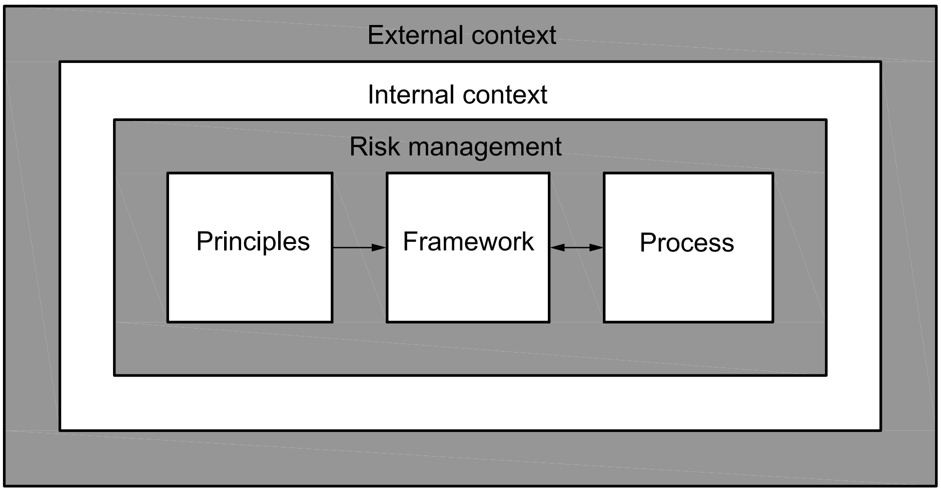
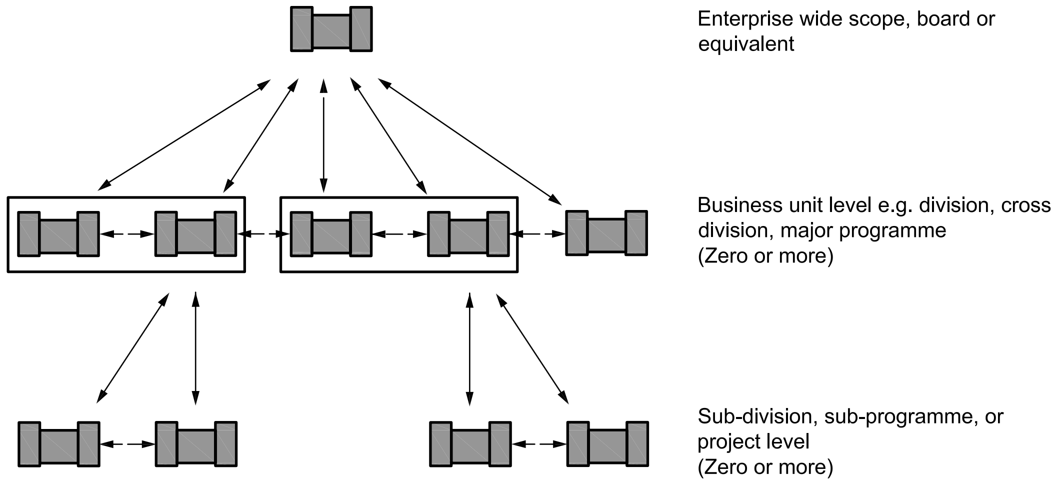


Figure 3 **Illustrative set of instances of the risk management process in a larger organization**


Enterprise wide scope, board or equivalent
Business unit level e.g. division, cross division, major programme (Zero or more)
Sub-division, sub-programme, or project level (Zero or more)

Key

▨ Instance of the risk management process

□ In the same business unit

←-→ Sharing information, e.g. about risks and controls

↔ Sharing information and command and control

When activities to develop risk management throughout the organization are first performed, the sequence of activities (see Figure 4) should be:

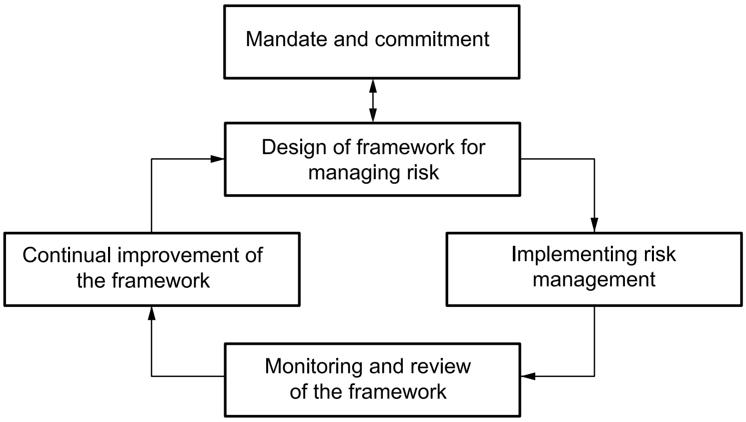
1) obtain mandate and commitment (see **3.2**);

2) design the risk management framework (see **3.3**);

3) implement risk management (see **3.4**); and

4) monitor and review (see **3.5**).

Figure 4 **Development of components of the risk management framework**


Mandate and commitment
Design of framework for managing risk
Continual improvement of the framework
Implementing risk management
Monitoring and review of the framework

Key

□ Activity

→ Initial/main sequence of activities

Subsequently, these activities should be maintained, leading to continual improvement and adaptation, either through frequent small changes or less frequent larger changes, or a combination of both. Commitment and monitoring should be maintained over time, but refreshing the formal mandate for risk management and major reviews of progress may be periodic events.

Initial implementation of risk management can take some time to achieve. Subsequent small improvements may be implemented as they arise or redesign and reimplementation may be performed only periodically.

3.2 Mandate and commitment

The board (or equivalent) should require the development of a risk management policy and, as the framework is designed and implemented, the board (or equivalent) should approve the risk management policy and support its implementation.

The organization's mandate for, and commitment to, risk management should acknowledge that:

a) risk management is important to creating and protecting value;

b) risk management is part of the organization's governance and operational management;

c) the board is accountable for risk management;

d) the ultimate goal is to integrate risk management with all processes and activities.

3.3 Design of framework for managing risk

*NOTE This subclause covers activities to design the framework for managing risk (subclauses **3.3.1** to **3.3.3**) and gives recommendations for features of the framework design (subclauses **3.3.4** to **3.3.13**).*

3.3.1 Understanding the organization and its context

The organization should gain an understanding of the external and internal context of its risk management and aim to design a risk management framework that is appropriate.

Before designing the risk management framework, the organization should therefore:

a) consult with its stakeholders to understand their capabilities and expectations;

b) recognize constraints on the organization's capacity to deliver;

c) identify legal and regulatory obligations;

d) review its existing processes and understanding of risk management; and

e) consider ways to use existing experience and resources, such as by extending the use of tools and documentation already in use.

Before designing the way that risk management will be developed over time throughout the organization, the organization should also:

1) examine the other parts of the risk management framework to identify key competence requirements;

2) identify weaknesses in its existing risk management framework, including weaknesses in elements that might hinder development of other elements, such as:

   i) limited commitment and resources from the board (or equivalent);

ii) lack of clear roles and ownerships;

iii) failure to integrate risk management into other management activities; and

iv) those charged with implementing risk management having insufficient skills or an inadequate mandate; and

3) aim to meet a chosen level of capability in a way that is efficient for the organization.

3.3.2 Establishing risk management policy

The organization should develop:

a) objectives for risk management;

b) plans for embedding and maintaining risk management throughout the organization; and

c) plans for all other elements of the risk management framework.

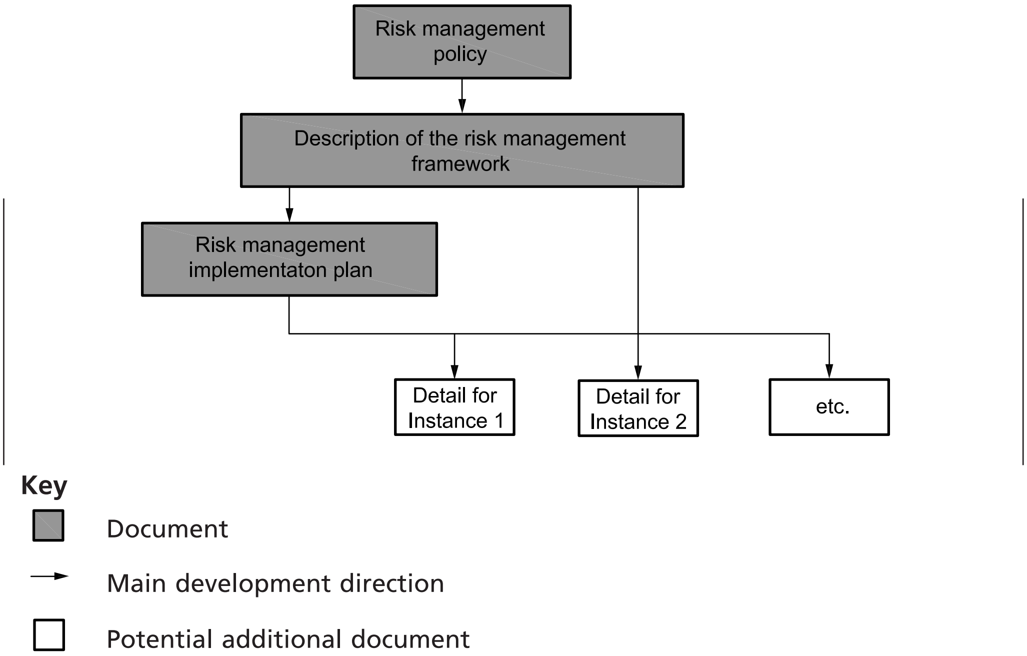
This should include documenting (see Figure 5):

1) the risk management policy, which is for approval by senior management and the board (or equivalent); and

2) the risk management framework, including plans for risk management processes, which is for guidance to everyone involved in risk management in the organization.

Small organizations should have the same elements in their documentation set as large organizations, but may create much shorter documents that reflect their size, simplicity and the lower number of instances of their risk management process.

Figure 5 **Typical documentation for risk management**


Risk management policy
Description of the risk management framework
Risk management implementaton plan
Detail for Instance 1
Detail for Instance 2
etc.
Key
▨ Document
→ Main development direction
□ Potential additional document

The risk management policy should be developed, documented, approved by senior management and the board (or equivalent), and communicated effectively.

The risk management policy may be brief, with the detail appearing in the framework design. It should set the direction, scope and objectives for risk management, and take into consideration the context, key stakeholders and the organization’s existing risk management capability and maturity.

Depending on the organization’s size and management style, the risk management policy may also include:

i) the risk management activities to be undertaken to meet the objectives, and the timeframes for these;

ii) the resources required, including people, knowledge and budget;

iii) risk criteria and other policies to control risk-taking and exposure;

iv) the chosen level of risk management capability;

v) specific activities to be taken to develop and embed risk management in the organization, and the timeframes for these; and

vi) how progress against the risk management policy will be monitored, reviewed, reported and communicated.

Approval for the risk criteria (see **3.3.12**) and any other risk policies to control risk-taking and exposure (see **3.3.13**) may be obtained either as part of approval of the risk management policy or as part of the approval of the strategy and implementation plans.

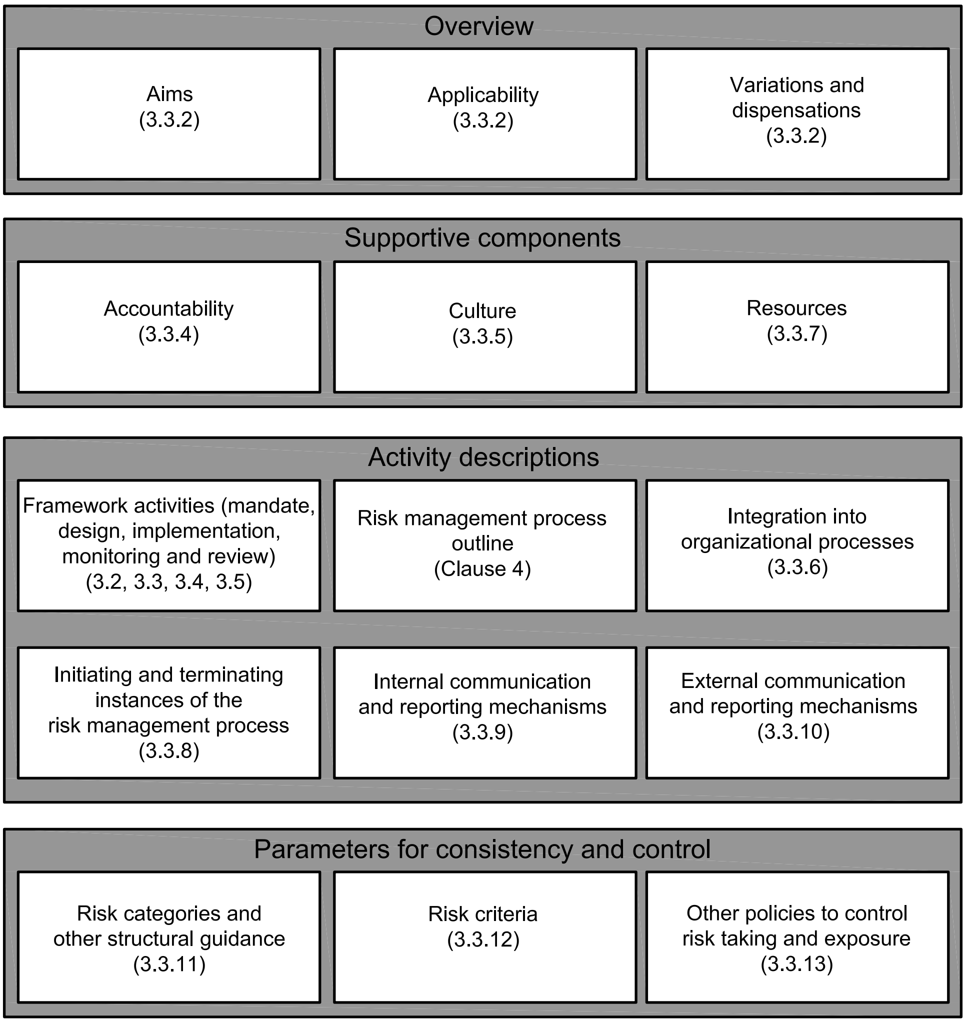
3.3.3 Documenting and communicating the framework

The design of the organization’s risk management framework should be documented, agreed by appropriately senior management, and communicated effectively.

The documentation of the risk management framework should provide a clear and concise statement and explanation of the organization's requirements for risk management. The design of the risk management framework should make risk management an integral part of the organization's overall approach to governance.

The description of the risk management framework should be based on the topics shown in Figure 6.

Figure 6 **Items to include in the description of the framework**


Overview
Aims (3.3.2)
Applicability (3.3.2)
Variations and dispensations (3.3.2)
Supportive components
Accountability (3.3.4)
Culture (3.3.5)
Resources (3.3.7)
Activity descriptions
Framework activities (mandate, design, implementation, monitoring and review) (3.2, 3.3, 3.4, 3.5)
Risk management process outline (Clause 4)
Integration into organizational processes (3.3.6)
Initiating and terminating instances of the risk management process (3.3.8)
Internal communication and reporting mechanisms (3.3.9)
External communication and reporting mechanisms (3.3.10)
Parameters for consistency and control
Risk categories and other structural guidance (3.3.11)
Risk criteria (3.3.12)
Other policies to control risk taking and exposure (3.3.13)

The outline of the organization's risk management process should provide guidance that allows people to create an instance of the risk management process.

The description of the risk management process given in Clause **4** may be adopted for this purpose, but additional or alternative guidance consistent with Clause **4** may be used to, for example:

a) achieve greater consistency within the organization;

b) make use of particular tools; or

c) use language and concepts more familiar to people in the organization and suited to the interpretation of the process the organization wishes to encourage.

The design of the risk management framework should be:

1) owned by a manager, preferably at board (or equivalent) level;

2) developed in consultation with key stakeholders;

3) developed with consideration of how the organization will monitor adherence to the risk management policy and reference any relevant standards, regulations and policies that have to be included or taken into account; and

4) subject to quality assurance practices, e.g. document, change and version control.

3.3.4 Accountability

3.3.4.1 Identification

The organization's risk management framework should define and document roles in terms of responsibilities, authorities and accountabilities for risk management, and should allocate the roles to people and to groups (e.g. existing teams, committees).

This allocation should align with existing roles and responsibilities, and be documented in the description of the risk management framework and communicated through existing means of communicating roles (e.g. written job descriptions).

NOTE These roles do not have to be full-time appointments or assigned to different people, so this approach can be applied even to very small organizations.

All the work implied by the organization's framework and process should be included. The breakdown of roles shown in Table 2 may be used.

Table 2 **One possible breakdown of roles**

Role	Illustrative allocation in a large organization
Framework	
longer term development of risk management in the organization, including development and implementation of the risk management framework	a committee of the board (or equivalent) supported by a risk manager
overall coordination of instances of the risk management process	a committee of the board (or equivalent) supported by a risk manager with a team
providing independent assurance	internal audit and some external reviews
Process	
operating an instance of the risk management process	a committee of the board (or equivalent) operates at least one instance while other instances are operated by groups such as business unit management teams, project management teams and risk specialists
monitoring a particular risk and relevant controls (i.e. being a risk owner)	managers at a variety of levels (often people included in the group operating the relevant instance of the risk management process)
monitoring a particular control (i.e. being a control owner) • implementing a control • operating a control	people at a variety of levels, often people included in the group operating the relevant instance of the risk management process everyone is responsible for managing risk as it affects their jobs
providing information on the internal and external context, and on controls	everyone
providing independent assurance	internal audit and some external reviews

The allocation of roles should reflect the size and structure of the organization. Ultimate responsibility for risk management lies with the board (or equivalent), but this should be delegated appropriately. Table 2 illustrates possible allocations of roles in a large organization. In a smaller organization the extent of delegation will be correspondingly less. The roles that may be delegated most extensively are those for:

a) operating instances of the risk management process (except for those covering all risks across the whole organization);

b) implementing and operating controls; and

c) providing information.

The responsibilities in Table 3 should be retained by the board (or equivalent) or a committee of its members (perhaps acting as a risk oversight committee), and not delegated.

Table 3 **Leadership responsibilities**

1) Approve the risk management policy and take the lead on setting the tone and culture for managing risk and embedding risk management, not least by their own example.
2) Ensure there is an appropriate risk management framework and process in place and that risk management is adequately resourced.
3) Provide strategic direction on the appropriate consideration of risk in decisions and setting risk criteria and other policies to control risk-taking and exposure.
4) Operate an instance of the risk management process covering the whole organization and all types of risk.
5) Provide direction and receive assurance on the effectiveness of risk management and compliance with the risk management framework.
6) Report on risk management to stakeholders and sign off public disclosures related to risk and risk management.

Responsibility for risk management should be delegated so that everyone in the organization has some role in risk management, including at least those responsibilities shown in Table 4.

Table 4 **Minimum responsibilities for everyone in the organization**

1) Be aware of the risks that relate to their roles and their activities.
2) Continuously improve their management of risk.
3) Provide information to help operate the risk management framework and process, such as information that helps to identify risks and assess controls.
4) Implement controls, or support the implementation of controls, as part of their day-to-day duties.
5) Report ineffective and/or inefficient controls.

3.3.4.2 Risk and control owners

All risks and controls should be allocated owners as part of the risk management process.

The owner of a risk should own the organization's assessment of the risk, monitor it, and report its status. The owner of a control should respond to the risk, contribute to the development and maintenance of the control, and report its status. Risks and their related controls may be owned by the same person.

3.3.4.3 Risk management manager or team

The organization may, depending on its size and complexity, have a dedicated manager or risk management department to support its risk management. The role of the risk manager and/or risk management function may include the items shown in Table 5.

Table 5 **Role of a risk management function**

1) Develop, implement and review the risk management framework and process.
2) Promote effective risk management at all levels of the organization.
3) Encourage an appropriate risk culture and develop resources for risk management within the organization, for example, by providing education and training.
4) Coordinate other functions that advise on specific aspects of risk management.
5) Coordinate responses where risks impact more than one area, e.g. security, business continuity, communications, health and safety and supply chain security.
6) Report, escalate and communicate risk management issues to key stakeholders.
7) Provide assurance regarding risk management within the organization.

3.3.4.4 Internal audit

If the organization has an internal audit function, this may provide independent assurance on:

a) the design, operation and effectiveness of the risk management framework and instances of the process;

b) management of key risks, including the effectiveness of the controls;

c) reporting of risk and control status; and

d) the reliability of assurances provided by management relating to risk management.

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

1) each function’s annual activity plans;

2) key risks;

3) methods of managing risks effectively;

4) key control issues;

5) output from risk management process activity and audits; and

6) reporting and management information.

3.3.5 Risk management culture

The risk management framework should incorporate the means to shape an effective risk management culture that encourages and motivates people to:

a) give appropriate attention and resources to achieve risk management objectives;

b) comply with the intent and details of risk management policies and procedures;

c) solve practical difficulties in implementing risk management policies and procedures, and do so in a way that is consistent with good risk management principles;

d) manage risk in ways that go beyond compliance with formal policies and procedures; and

e) communicate about risk openly and appropriately.

EXAMPLE

A medium sized investment bank managed risk very effectively with just a few full-time risk management staff. This was possible because employees felt rather like members of a family, were proud of their company and each other, and normal human mistakes were tolerated. This made it easier for people to admit to mistakes, weaknesses and risks. This openness was seen as everyday good practice within the company, part of improving service to clients and increasing revenue.

Features of culture that may be considered include the following helpful features.

1) Focus on thinking widely about the future and what is uncertain, rather than focusing only on what could go wrong or what is already understood.

2) Emphasis on using risk management to help the organization do difficult things rather than create obstacles.

3) Low power distance (i.e. differences in organizational status should not imply important differences in social status).

4) Low collectivism (i.e. the desire for consensus should not lead to lack of clear responsibility for action).

5) Long-term thinking and the avoidance of short-termism.

6) Limited emphasis on targets and also avoidance of thresholds linked to powerful incentives, such as large financial rewards or job loss.

7) Avoidance of blaming.

8) Pursuit of objectivity and lack of bias, avoiding baseless optimism and positive thinking.

9) Attention to evidence.

10) Participation and sharing of information generally.

11) Acceptance of formality.

The arrangements in the framework should allow the organization to monitor and develop its risk management culture through, for example:

i) monitoring attitudes to risk management;

ii) demonstrating effective risk management leadership at senior levels as an example to others (which can often be the main method in smaller organizations);

iii) monitoring and communicating the value added by risk management, either proven by measurement over time, or anticipated when an acknowledged improvement to a plan or process is made as a result of risk management;

iv) providing education and training in risk management, including practical examples;

v) including risk management within individual objectives and performance appraisals;

vi) integrating risk management into organizational processes (see **3.3.6**); and

vii) continually maintaining and improving risk management.

3.3.6 Integration into organizational processes

The risk management framework should be designed to integrate risk management with other activities in the organization through:

a) controls that are well integrated into the organization's processes, systems, tools, skills, etc.; and

b) integration of other activities that are part of the risk management framework and process with other management activities, including those for managing performance by:

   1) establishing objectives and strategies;

   2) forecasting;

   3) planning, including annual planning and planning of investment; and

   4) appraising individual and team performance and deciding rewards.

Features of risk management that contribute to integration include:

i) teams for risk management being the same as, or similar to, those for other management activities;

ii) risk management being covered in meetings at the same time as other management matters;

iii) management information reports including risk-related information, rather than all risk reporting being separate from other reporting;

iv) risk analysis and reporting providing analyses of risks that are the risks involved in decision-making, including strategic decisions;

v) risk analysis supporting the development of objectives and strategies as well as helping to achieve objectives and strengthen strategies;

vi) risk information being used in general management meetings; and

vii) where any risk management activities are separate from other management activities, the schedules are coordinated so that outputs from risk management are available at the right time.

EXAMPLE

In a large company that delivers hundreds of capital projects, project risk management has been integrated with project management and with the process by which funding for projects is approved. Guidance on risk management is woven in with other requirements in the project management framework guidance, instead of being in a separate section or document. At funding gateway meetings, where decisions to fund projects are made, risk information has to be included along with other information. The risk information is provided in a standard format from a database of risks and has to be aligned with risk funds shown in the accounting system.

3.3.7 Resources

3.3.7.1 General

The risk management framework should identify the resources of all kinds to be applied to:

a) develop risk management over time; and

b) manage instances of the risk management process.

The risk management framework may identify the resources to be applied to operate instances of the risk management process already in place or planned.

The framework may also provide estimated resource requirements for:

1) operating additional instances of the risk management process (e.g. for projects not yet planned); and/or

2) implementing and operating risk responses.

3.3.7.2 Tools

The framework should provide tools (e.g. techniques, templates, software, documents) that help people manage risk. These tools should fit the organization's framework and process, and its maturity.

The organization should communicate information about the tools to those who ought to use them, with guidance on where to get the tools and who to contact for further assistance.

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

3.3.7.3 Competence

The framework should include arrangements to ensure that any person performing risk management tasks is competent to do so, on the basis of appropriate education, training or experience.

To build the capability needed to embed risk management throughout the organization and develop risk management maturity, the framework should provide relevant people with appropriate experience, skills and knowledge covering the items listed in Table 6.

Table 6 **Items to cover related to risk management competence**

1) Current corporate governance requirements and their source.
2) The legislative and compliance context of the organization's risk management.
3) The organization's risk management framework and process, including:
   a) roles, accountabilities and responsibilities (see **3.3.4**);
   b) how to identify, assess and manage risks;
   c) the organization's risk criteria and other policies to control risk-taking and exposure;
   d) risk tools and how and where they are applied;
   e) risk reporting requirements.
4) Statements on controls.
5) Where the organization's risk management capability stands (its risk management maturity).
6) An assessment of performance as part of the organization's overall appraisal system.

3.3.8 Initiating and terminating instances of the risk management process

3.3.8.1 General

Risks should be managed through one or more instances of the risk management process outlined in the framework, each tailored to fit its context but consistent with the others. The framework should include rules that govern what instances will be operated.

The design of the risk management framework should also include appropriate arrangements for:

a) initiating new instances of the risk management process;

b) revising the terms of reference of existing instances of the risk management process; and

c) terminating instances of the risk management process.

In a small organization expecting to operate only one instance of its risk management process, these arrangements may be very simple, providing enough guidance to start and modify that instance. In a large organization with many projects the arrangements should be more fully developed.

These arrangements should be designed to ensure that:

1) responsibility for initiating, revising or terminating each instance is clearly allocated;

2) there is always at least one instance whose scope covers all risks across the whole organization, and that those responsible for operating that instance are appropriately senior;

3) the number and scope of instances remains appropriate to the context of the organization, including its governance, structure, size and complexity; and

4) instances operate effectively together.

EXAMPLE

A multinational conglomerate with an effective, but aggressive, acquisition, restructuring and disposals strategy puts its success in this area down to a strong focus on the initiation, evolution and termination of instances of its "risks and opportunities" regime. This starts with an instance of its risk management process being a workstream within its acquisition and due diligence projects. Once a company is acquired this instance of the risk management is turned into one that addresses the risks in the various stages of transforming the business, to bring forward the time at which most benefit from the acquisition is gained.

Once the transformation is complete the project is terminated along with its instance of the risk management process, and information from it is fed into operational and strategic direction activities. On disposal, an instance of the risk management process is initiated to maximize value from the disposal. Their process for initiating new instances clearly communicates the scope, objectives and considerations for each instance.

3.3.8.2 Initiating instances of the risk management process

The approach to initiating new instances of the risk management process should be designed to ensure that:

a) new instances are created promptly when trigger events happen (i.e. events mentioned in the rules [see **3.3.8.1**] for what instances will be operated, such as the creation of a new organizational unit, the start of a project, or a regulatory change);

b) those operating new instances are given clear terms of reference covering the scope of risks they should consider, the nature of the team and any special resources allocated;

c) those operating new instances have the ability to carry out the instance, including the required resources and knowledge of the risk management process; and

d) new instances are included in internal and external reporting to the appropriate extent.

Instances of the risk management process may differ as to the types of risk within their scope, the parts of the organization whose risks are included, and the people operating them.

To help integrate risk management into other management activities, those operating instances of the risk management process may be existing line management or project management teams. Alternatively, committees may be formed specifically to gain a perspective that is not provided by existing management teams.

3.3.8.3 Terminating instances of the risk management process

The approach to terminating instances of the risk management process should be designed to ensure that:

a) instances are terminated promptly when trigger events happen [see **3.3.8.2**a)];

b) termination of an instance does not lead to an unintended gap in risk management and specific risks identified by the instance are covered by another instance or do not need to be; and

c) any tools of instances terminated are reviewed to see if they should be reused elsewhere.

3.3.9 Establishing internal communication and reporting mechanisms

The risk management framework should include arrangements for communication (including formal reporting) about risk management. These should support:

a) operation of each instance of the risk management process;

b) ongoing management of one or more instances of the risk management process (including, where appropriate: initiating, revising and terminating instances of the process; monitoring; and communication between instances of the process); and

c) development of risk management capability, including implementation of the risk management framework itself.

Communication, whether or not as formal reporting, should encompass all roles involved in risk management (see **3.3.4**) and all relevant information.

The organization's internal reporting should be aligned with its governance structure and allow the flow of risk information through the organization. Reporting about risk should be integrated with other internal reporting for efficiency and integration with other management activities.

The organization should identify the specific risk information, and its level of detail and frequency, that allows those involved to fulfil their roles. The structure and process for internal reporting should be documented, and a timetable developed detailing responsibilities and timescales.

3.3.10 Establishing external communication and reporting mechanisms

The organization's framework should include arrangements for external communication and reporting mechanisms that support:

a) consultation with appropriate external stakeholders; and

b) reporting on the current risk profile, ongoing risk management performance, and development of risk management over time.

The organization's external risk reporting should be:

1) based upon an understanding of the stakeholders' needs, priorities and time scales, and aligned to their responsibilities;

2) timely, concise, specific and reliable;

3) sufficiently detailed that the stakeholders can gain an appropriate understanding of the key issues;

4) integrated with other reporting processes where practical and appropriate;

5) delivered in time to let recipients adequately review the content; and

6) independently reviewed periodically to validate its quality and ensure it is aligned to its stakeholders.

3.3.11 Risk categories and other structural guidance

The organization's framework should include a system of risk categories and/or other structural guidance for risk analysis that suits its context, aligns with its risk management process and tools, and is appropriate for the maturity of its risk management.

NOTE 1 Grouping similar risks in risk categories and/or applying guidelines for structuring models helps to:

a) organize risk identification and promote comprehensive coverage; and

b) identify similar risks appearing in risk analyses by different organizational units.

NOTE 2 Risk categories and other structural guidance can be seen as parameters of the risk management process that can be varied while its procedures stay the same.

Where there are multiple instances of the risk management process, risk categories and/or other structural guidance should be designed to promote consistency between risk analyses in different instances.

Risk categories and other structural guidance may also be used to improve alignment with other management activities by ensuring that risk analyses provide assessments for the risks that are considered in decision-making, such as in annual business planning, mergers and acquisitions, or software development projects.

NOTE 3 While risk categories differ between organizations, risk categories in common use include:

a) strategic risk;

b) programme risk;

c) project risk;

d) financial risk;

e) safety risk;

f) compliance risk; and

g) operational risk.

The choice of risk categories can be influenced by legal and regulatory requirements or sector practice.

Other structural guidance can, for example, guide model structures and the structure of individual risk definitions.

3.3.12 Risk criteria

3.3.12.1 General

To enable risks to be assessed consistently the framework should include appropriate risk criteria that guide people in deciding the significance of each risk based on its possible effects and their likelihoods.

NOTE These criteria are another important parameter of the risk management process and allow overall direction as to the extent to which controls are evaluated as necessary or worthwhile.

3.3.12.2 Characteristics of effective risk criteria

Risk criteria should be designed to help people choose the control changes to implement by considering:

a) the possible net benefits from changing risks compared with the cost of implementing and operating the controls;

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

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

NOTE 1 Analysis of costs and benefits need not be purely in financial terms or be fully quantified.

Risk criteria should state the following.

1) *The consequences to be considered in judging the importance of risks* (such as lives lost, financial gain or loss, legal penalties or awards, reputation effects and environmental impact). This should include guidelines for deciding the time periods over which consequences are to be considered.

2) *Measures of the level of risk, taking into account the likelihoods of different levels of the consequences*. These should combine the different consequences and simplify distributions of effects into a level of risk. They should include guidelines for deciding which expectations to use in assessing the effects of risks.

3) *The importance of different levels of risk, for use in decision-making*. This may be demonstrated using thresholds that determine when action has to be taken to manage risk, and/or by defining scales of importance linked to level of risk.

Once instances of the risk management process have begun to operate and risks have been identified and considered, additional risk criteria may be developed that apply to particular risks or sets of risks considered together. These criteria should identify the risks involved and the instances of the risk management process where those risks have been identified.

The organization’s risk criteria should allow for all risks to be measured, including those that do not naturally lend themselves to numerical analysis.

Measures of risk should adequately reflect the realistic possibility of unusual levels of consequences, not just typical or average levels.

Where thresholds are applied to risks they should be appropriate to each risk so that, if a risk is split into components or some risks are pooled into one, the decisions resulting from applying the risk criteria are not unduly changed.

Risk criteria should take into account combinations of multiple risks if decisions involving multiple risks are to be taken (e.g. where multiple risks affect a strategic decision or are addressed by the same control, and where the combined effect of multiple risks is to be compared with some risk limit).

*NOTE 2 Risk criteria that take into account combinations of multiple risks (as mentioned in BS ISO 31000:2009, **5.3.5**) are usually required.*

Where risk criteria take into account combinations of multiple risks they should:

i) identify in principle, or enumerate, the sets of risks the criteria are applicable to; and

ii) take into account the effect of dependencies between risks in a combination.

NOTE 3 Dependencies usually mean that the level of risk for a set of risks is not equal to the sum of the level of risk for each risk individually.

EXAMPLE 1

In financial services companies, risk-adjusted performance measures have become increasingly common risk criteria. These express results such as profit in a way that is adjusted to reflect the risks run by engaging in different business activities. The most common technique is risk-adjusted return on capital (RAROC). The risk adjustments mean that risk is considered in decisions such as how to judge the performance of different business units and products, and how to allocate capital between them.

EXAMPLE 2

One approach to choosing healthcare interventions and allocating resources is to express consequences in terms of quality-adjusted life years (QALY). These represent the number of extra years of life provided by a treatment, adjusted if that life is lived in less than perfect health (e.g. because of pain or loss of mobility). The QALY impact of alternative treatments can be estimated over possible outcomes, taking into account their likelihood, and may be expressed in terms of cost per QALY.

3.3.12.3 Approach to developing risk criteria

The approach taken to developing risk criteria should ensure that the interests of legitimate stakeholders are fairly reflected in accordance with the organization’s governance arrangements.

Factors that may be taken into consideration when determining the importance of different levels of risk include:

a) the potential for particular levels of consequences to cause or contribute to a serious outcome, such as commercial ruin or loss of life, or to lead to dramatic benefits, such as winning an important competition;

b) the organization’s resources and reserves, now and in future, and the variability of those resources;

c) the organization’s financial flexibility;

d) the organization’s ability to withstand or exploit risk occurrences efficiently, which is influenced by its commitments, management style and other factors;

e) the greater opportunity to prepare for outcomes anticipated with certainty, and reduced cost arising from not preparing for outcomes that do not occur; and

f) the interests of stakeholders, including external stakeholders where relevant.

Where criteria are applied to particular risks or sets of risks, the likely cost and effectiveness of potential controls should also be considered.

To integrate risk management with other management activities, and to link risk-taking with rewards, decisions on risk criteria may be made in conjunction with other planning decisions, such as those on revenue and growth targets, and budgets.

The risk criteria may be interpreted and developed in detail when the risk management process is applied.

3.3.13 Other policies to control risk-taking and exposure

In addition to providing guidance on risk criteria, the risk management framework may provide further rules that constrain decision-making on risk-taking and exposure, and that are applicable to the whole organization.

These may be set and stated separately from risk criteria, or with them.

NOTE 1 Statements of rules on risk-taking and exposure are sometimes called "risk appetite statements" and often include risk criteria in addition to rules that go beyond risk criteria by using measures that are not risk measures (e.g. level of investment), requiring a wider range of actions (e.g. escalation of decisions) and applying to decisions outside instances of the risk management process,

NOTE 2 Such statements, and their implementation, may also be regarded as controls.

Similar to risk criteria, these further policies may include rules that:

a) prescribe approaches to taking particular decisions and to taking risk into consideration; and

b) provide values for decision-making parameters such as limits, weights or thresholds for escalation of decisions, defined using:

   1) levels of particular risks or sets of risks; and/or

   2) levels of other measures related to risk, such as indicators of inherent risk, indicators of the operation or performance of controls and actual results achieved by the organization.

These rules should clearly specify when they are to be applied (the circumstances or times) and what they require, such as escalation of decisions, consideration of factors, weighting of risks, or adaptation of controls. Where a statement concerns a quantity then that quantity should be clearly defined and helpfully named.

Where rules apply to particular risks or sets of risks, the rules should identify both the risks and the instance(s) of the risk management process whose risk analysis contains them.

The rules should recognize that higher-than-expected risk in some areas can be compensated for by lower than expected risk in others.

The organization may monitor a wide range of indicators related to risk for which there are no such rules.

Application of these rules should be integrated into management activities, including the risk management process and risk management framework.

3.4 Implementing risk management

3.4.1 Implementing the framework for managing risk

A risk management implementation plan should be prepared and carried out, and progress in implementing changes should be monitored.

The risk management implementation plan should allocate owners to the actions planned to embed and maintain risk management throughout the organization and provide a schedule for their implementation. The schedule, including frequency of reviews, should be appropriate for the context of the organization, including its size and level of risk management maturity. The plan should include communication to each person in the organization, covering the content of the risk management framework that is relevant to them.

The risk management framework and risk management implementation plan should be revised appropriately in light of what is learned during implementation. Methods and tools may be trialled to accelerate improvement.

Depending on the context, the information in the risk management implementation plan may also include:

a) objectives and strategy;

b) budget for risk management activities;

c) risk management performance indicators;

d) background of individuals, particularly for a new team; and

e) references to supporting information such as templates and techniques.

A large or medium sized organization may have one or more sub-plans for different levels, such as organizational unit, programme, project and different risk functions such as financial and operational risk.

The risk management implementation plan may be integrated into other organizational plans.

3.4.2 Implementing the risk management process

The risk management implementation plan should also cover implementation of the risk management process.

The risk management process (or any revision to it) should be implemented mainly using the processes in the risk management framework for initiating, revising and terminating instances of the risk management process (see **3.3.8**). However, where this implies a lot of change, as when introducing formal risk management for the first time, additional activities may be planned to ensure success.

3.5 Monitoring and review of the framework

3.5.1 General

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

Monitoring should identify where the set of instances of the risk management process currently operating is inconsistent with the risk management framework. In particular, it should identify missing instances and instances with the wrong scope and ensure that problems are promptly resolved.

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

a) the framework and processes are fit-for-purpose and aligned to the objectives and priorities of the organization;

b) the framework and processes adopted are operating as planned;

c) risks are being managed in accordance with the risk criteria and other policies to control risk-taking and exposure;

d) relevant stakeholders are receiving sufficient reporting to enable them to discharge their roles and responsibilities in the governance structure;

e) people across the organization have sufficient risk management skills, knowledge and competence to carry out any risk role, or risk element of a role, they are required to perform on a daily basis;

f) the risk management resources are adequate;

g) lessons have been learned from actual outcomes, including losses, near misses and opportunities that were identified in advance, occurred and yet were not acted on; and

h) overall current risk management maturity and capability achieve the objectives set out in its risk management policy.

More frequent reviews may be performed during periods of rapid change to the risk management framework, the organization or its environment, and where the risks being managed are themselves volatile and/or severe.

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

3.5.2 Learning from outcomes

The organization should learn from actual outcomes, including those captured within risk analyses and those that perhaps ought to have been. These should include losses, near misses, and opportunities that were identified in advance, occurred, and yet were not acted on.

Individually significant outcomes should be reviewed promptly to identify relevant mechanisms. Points that may be considered in such a review include:

a) what happened;

b) how and why the risk occurrence came about;

c) what action has been taken (if any) in response;

d) the likelihood of the risk occurrence happening again;

e) any additional responses or steps to be taken; and

f) key learning points and who they need to be communicated to.

Outcomes that were significant collectively, where consequences were insignificant but might not be in future, or that could point to important trends, should also be reviewed. This may be carried out in a statistical way.

This may involve implementing suitable reporting and recording procedures, and a database.

In addition, the organization should consider readily available information about relevant outcomes of other organizations (e.g. industry peers) and the controls they have used.

3.5.3 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 can cover:

a) the organization's risk management framework, including management responsibilities for risk management;

b) the key risks and the primary control systems in place to manage these;

c) the monitoring and review of control systems in place; and

d) any major deficiencies uncovered and the steps taken to deal with them.

3.6 Continual improvement of the framework

The organization should continue to improve the effectiveness of its risk management framework through, for example:

a) a review process (see **3.5**).

b) learning from risk outcomes and the application of controls; and

c) internal audit (if an internal audit function is present).

Lessons learned should be applied to adapt and improve components of the risk management framework through continuing with the activities described in **3.2** to **3.5**.

4 Process

4.1 General

Each instance of the risk management process should provide a systematic, effective and efficient way by which risks can be managed. It should be consistent with the risk management process (see Figure 7) outlined in the risk management framework, but should be tailored to the context in which it is to operate. Each instance should be:

a) an ongoing undertaking by a group of people within the organization as an integral part of their decision-making; and

b) operated using the parameters set out by the risk management framework (e.g. risk criteria, risk categories).

The organization's risk management process should, as a minimum, comprise the following activities:

1) communication and consultation (see **4.2**);

2) establishing the context (see **4.3**);

3) risk assessment (see **4.4**);

4) risk treatment (see **4.5**); and

5) monitoring and review (see **4.6**).

When the activities of the risk management process are carried out for the first time the sequence of activities should be: 1) establish the context, 2) assess risks and 3) treat risks. Communication, consultation, monitoring and review should occur throughout.

Subsequently, the activities should continue so that risks are reassessed and risk treatment is revised at appropriate times. This may be in response to new information or new insights about risk, or new ideas for risk responses, and may also be carried out regularly to draw in new information and generate insights and new ideas. The context may also be re-established in response to events, and regularly, but need not be on the same schedule as risk assessment and treatment.

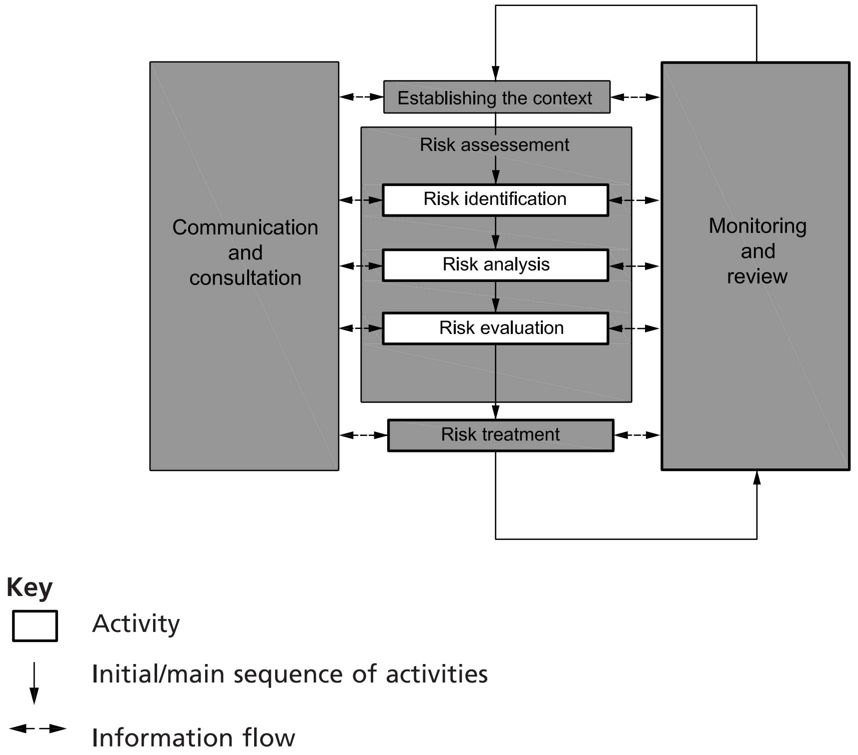
The main direction of inferences should be from risk assessment to risk treatment, but ideas on risk treatment should also influence risk assessment because they are one of the reasons for grouping or aggregating risks (see **4.4.2**).

NOTE 1 As skill in applying the risk management process increases it can become easier to apply it responsively and to cope with inter-related risks and decisions.

NOTE 2 There are many tools for presenting and communicating the results of risk management; examples can be found in Annex A.

The scheduling of these activities should be designed to help integrate them with other management activities.

Figure 7 **The risk management process**



4.2 Communication and consultation

Communication and consultation should take place when an instance of the risk management process is being designed and when particular risks are being managed.

The extent of consultation, particularly with external stakeholders, should be proportionate. Consultation should focus on those stakeholders and matters that are important, within the constraints of any requirements for confidentiality.

Plans for communication and consultation may cover individual risks, groups of risks, or all risks covered by the instance of the risk management process. More detail may be added for particular risks once they have been identified and evaluated as important, or once their proposed treatment has emerged as costly or requiring more discussion.

4.3 Establishing the context

Those involved in an instance should gain an understanding of the internal and external context and create an interpretation of the risk management process that fits them.

Each instance of the risk management process should be aligned with other management activities through its schedule, team composition, risk analysis, reporting channels, and other details.

Those involved in an instance should:

a) consider the terms of reference provided for their instance of the risk management process, including its team composition, organizational scope and types of risk to be covered;

b) confirm the scope and ground rules for the risk management process;

c) review the relevant elements of the risk management framework, including the description of the risk management process, risk communication mechanisms, risk categories and other structural guidance, and risk criteria;

d) consider the external context and other aspects of the internal context, including relevant objectives and strategies;

e) select appropriate procedures, tools and techniques, and a schedule for the instance of the risk management process;

f) define the risk criteria, either accepting or interpreting those defined by the risk management framework;

g) involve appropriate people at each stage; and

h) establish relevant documentation.

These decisions should be reviewed over time as the context changes and more is learned about the nature of the risks to be managed.

4.4 Risk assessment

4.4.1 General

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

The scope of risk assessment should include revising views of risks previously identified and identifying new (perhaps emerging) risks. This may involve replacing some risks with new ones that better describe the total risk faced.

The risk assessment activity should involve:

a) risk identification;

b) risk analysis; and

c) risk evaluation.

4.4.2 Risk identification

Risk identification should be carried out to develop a set of well-defined risks.

Risk identification should aim to include all risk, but not necessarily enumerate individually every possible outcome or every stage of every possible sequence of cause and effect.

Risk identification should be approached methodically and iteratively so that it is thorough, efficient and, wherever possible, has the features listed in Table 7.

Table 7 **Features of risk identification**

1) The full scope of the instance of the risk management process is explored.
2) All significant risk sources potentially affecting the achievement of objectives are identified and considered, including conflicts between stakeholders or objectives, which can be a significant source of risk, and dependencies on other business areas.
3) The results of early iterations of risk assessment guide later iterations, so that the analysis continues to identify important risks.
4) Risks are clearly defined and there are no unintended gaps or overlaps.
5) Good and bad consequences are addressed as appropriate (see Annex B).
6) Each risk's causes and effects are examined.
7) Assumptions are challenged.
8) The risks are given owners.
9) Existing risk responses perceived to be addressing the risks, and the owners of these responses, are identified.

The process of identifying risks should be iterative and one of refining the output until it is appropriate and at least adequately reflects the risks without being excessively detailed.

The initial set of risks should be reviewed and revised to take account of situations 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.

Rapid checks should be made as the identification process progresses to ensure that it remains relevant and that risks are adequately recorded.

Models of various kinds, ranging from conceptual diagrams to computer simulations, may be used to help structure risk identification, examine chains of cause and effect including inter-relationships between risks, and understand cumulative effects.

Risks should be recorded consistently and explicitly to allow review and development of effective responses.

4.4.3 Risk analysis

Risk analysis should be carried out to develop an understanding of the risks and assign a risk level to each one. Confidence in the assessment of the level of risk should be considered and communicated.

NOTE 1 A risk can have a number of consequences, some positive and some negative, some uncertain, and some positive or negative depending on what actions are taken to manage the risk.

Risk analysis should be performed in accordance with the risk criteria. Analysis may be qualitative or quantitative, or a combination of these provided it is consistent with the risk criteria.

Risk analysis may be undertaken to varying degrees of detail depending upon the risk, the purpose of the analysis, and the information and resources available. 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 iterative, being repeated as more information becomes available. It should take account of the controls in place. Inherent risk may also be considered.

NOTE 2 An understanding of inherent risk can help ensure that responses are proportionate to the overall exposures. It can also help the organization understand what its full exposure could be if controls fail, and thereby recognize the contribution of certain controls to overall risk modification.

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. If residual risk is estimated by considering inherent risk and the effect of controls, then controls should be ascertained, documented, and mapped to risks to clarify the residual risk currently being retained, and documentation that supports this many-to-many mapping should be used.

To allow appropriate methods of analysis to be applied to each risk, the documentation should support the methods used.

Confidence in the level of risk may be communicated in a variety of ways, depending on circumstances. They may range from explicit statements of statistical confidence to statements about the type of evidence used or the source of the information. Understanding the information used to determine the level of risk can lead to decisions to get more information.

4.4.4 Risk evaluation

Those managing risk should apply the risk criteria to establish the importance of acting on the risks, taking into account their level of risk, proximity (how soon the risks might materialize) and manageability.

This should take account of the context of the risks and the views of stakeholders.

The risk evaluation process should compile/calculate risk profiles by appropriately combining/aggregating analysed risks and applying the risk criteria.

4.5 Risk treatment

4.5.1 General

Risk treatment options (i.e. ideas for actions to change controls) should be developed, selected and implemented to adapt and/or improve the existing set of controls (if any).

This may be achieved by designing a revised set of controls to have in place and then working out the risk treatments that will change the existing set of controls to this revised set.

4.5.2 Selection of risk treatment options

4.5.2.1 Developing ideas for changes to risk responses

At each iteration of the risk management process, ideas for changes to controls (adaptations or improvements) relevant to the risks being considered should be developed in enough 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. Controls may be changes to existing plans or procedures, which may be more efficient and integrated than adding additional activities such as checks.

A control may be implemented to:

a) avoid risk;

b) seek risk (take opportunity);

c) modify risk;

d) share risk; and/or

e) 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.

Controls may include policies, expressed in words or numbers, that aim to constrain risk-taking and risk exposure, and go beyond risk criteria by applying to risk-related indicators (e.g. level of investment, duration of a project) as well as to risk measures. These policies reinforce the risk criteria and may use targets, single limits, bands, multiple thresholds, or other techniques to provide planning guidance, determine limits on authority, trigger alternative control procedures or escalation, and influence decision-making in other ways.

Such policies, if used, should be set and revised as part of existing processes for strategy making and planning, possibly at the same time as risk criteria. The policies may be part of the risk management framework (see **3.3.13**).

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.

4.5.2.2 Deciding which control changes to make

When deciding which control changes to implement, those managing risk should assess, in accordance with the risk criteria:

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

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

c) any legal or regulatory requirements, social responsibility factors or limits within the risk criteria or other policies on risk-taking and exposure that might override a cost-benefit analysis and necessitate or prevent a specific control change; and

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

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

All changes to controls and the resulting retained residual risk should be appropriately documented and authorized by the organization in accordance with risk management roles and any applicable policies to control risk-taking and exposure.

4.5.3 Preparing and implementing risk treatment plans

Risk treatment plans should be prepared and implemented, and progress towards implementation should be monitored.

In preparing risk treatment plans, those managing risk should:

a) prioritize changes to controls, taking into account the impact on other activities and the availability of resources;

b) allocate risks response owners to the control changes selected; and

c) prepare a schedule for their implementation.

The number of separate plans and the detail they contain should be appropriate, taking into consideration the size and complexity of the organization and the changes to be made. Integrated documentation can reduce repetition.

The controls implemented should be documented.

4.6 Monitoring and review

4.6.1 General

Monitoring and review by those operating an instance of the risk management process should cover:

a) the risks and controls that are within the scope of the instance of the risk management process; and

b) the performance of the instance, with a view to how it might be adapted and improved.

Information should be provided to others, as required by the risk management framework, to allow them to monitor and review.

4.6.2 Monitoring operation and performance of controls

The organization should monitor and test its controls to ensure:

a) they have named owners;

b) they are specified, communicated and understood;

c) they are operating as designed;

d) that where deficiencies in the implementation or operation of controls are identified:

   1) the implications of control deficiencies not being remedied are understood and options for resolution are identified;

   2) they are reported so that the consequence for the risk profile can be assessed; and

   3) the resolution of control deficiencies is planned and carried out;

e) that if their implementation introduced any additional risks, then these have been considered; and

f) they are operating effectively and efficiently, each is worthwhile, and collectively they managed the risk to a level agreed to be acceptable.

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

After control changes have been implemented, data should be gathered to support a revised estimate of the residual risk and used in future iterations of risk assessment and risk treatment.

4.7 Monitoring performance of the instance of the risk management process

Those carrying out the instance of the risk management process should regularly review their experiences, outputs, and results to identify opportunities to improve the instance, including any where they need assistance.

NOTE Matters requiring attention can include:

a) poor compliance with the process;

b) insufficient resources, lack of competence, or unsuitable tools or document formats;

c) inadequate information to support risk assessments;

d) risk analyses that are disorderly or do not support other management decision-making;

e) *poorly defined risks, inadequate cross-referencing, anomalous risk levels, unsuitable risk summaries, or lack of ideas for effective risk responses;*

f) *difficulties integrating risk management with other management activities;*

g) *inadequate information to support assessments of the effectiveness of controls; and*

h) *slow or otherwise ineffective implementation of risk treatments.*

This information should be used within continuing work to establish the context of the instance of the risk management process as recommended in **4.3** and assistance should be obtained where necessary.

4.8 Providing information to others

The key outputs from the instance of the risk management process and lessons learned about the framework and process should be communicated to the relevant stakeholders as part of ongoing communication and consultation, as described in the risk management framework.

This reporting should provide an appropriate level of detail, and be specific, relevant, timely and reliable.

If circumstances indicate that the instance of the risk management process ought to be terminated or its scope revised then this information should be communicated and appropriate action taken.

4.9 Recording the risk management process

Risk management should be recorded.

Records of the instance of the risk management process should include documentation of:

a) the design of the instance of the risk management process and key decisions taken in arriving at that design;

b) the thinking involved in risk assessment and risk treatment decisions, including risks, risk evaluations, risk responses, risk treatments and risk treatment plans;

c) mappings between risks and responses, between controls and risk treatments, and between risk treatments and risk treatment plans;

d) owners for risks and risk responses; and

e) dates for versions of the documentation.

Further, records should include:

1) the status of key risks identified by the process, highlighting:

    i) any material changes that alter their likelihoods and/or consequences, particularly if these are likely to affect what responses are worthwhile; and

    ii) any risk(s) for which completion of an important risk treatment is outstanding;

2) the status of risk responses for key risks, for example where progress is behind agreed target or is significantly threatened;

3) any significant emerging risks that need to be assessed and monitored;

4) a description of the uncertainty related to a particular activity, process or event; and

5) 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;

Records may also include:

i) the underlying causes/sources of risk(s), e.g. a particular activity or process;

ii) information about the timing of risks;

iii) the dates risks were raised, in order to monitor ageing of risks with respect to the progress of modification;

iv) the link between an identified source(s) of risk and the relevant performance objectives;

v) the links between risks; and

vi) separate analysis between risk responses in operation, agreed risk responses not yet in operation, and newly proposed risk responses.

The documentation should be able to capture links between items and provide appropriate summaries.

NOTE Documentation that records the thinking involved in risk management may use paper or electronic storage.

The documentation used to record risk management may also be used for reporting, where its design is suitable.

Annex A (informative) Risk management tools

Tools can be powerful aids to effective risk management. They can enable those managing risk to capture information in a consistent way, engage with stakeholders, provide more thorough and reliable analyses, make explicit the risks associated with different options, prioritize actions, improve communication, and produce a reliable audit trail.

There are many tools and each is suitable for particular tasks in particular situations (see Table A.1). Some choices of tool are easy while others are harder. Tool selection should be based on:

a) characteristics of the user

   1) competence and experience with the tool

   2) ability to understand the benefits of using the tool

   3) willingness to use the tool

b) characteristics of the task

   1) purpose of the risk management activity

   2) desired output

   3) uses to which risk management outputs will be put

   4) stage of the activity being undertaken

   5) time available for the risk study

   6) the importance of the risks involved

   7) required level of detail

c) characteristics of the tool

   1) availability of information on the productive use of the tool

   2) availability of information on the tools' functionality

   3) ease of use

   4) cost

d) characteristics of risk management within the organization

   1) degree to which risk management is embedded in the organization

   2) complexity of its framework and the number of instances of its process

   3) complexity of instances.

Table A.1 **Examples of risk management tools (including techniques)**

Tool	Risk identification	Risk analysis and evaluation	Risk treatment and decisions
Types of meeting/collaboration: Interviews, focus groups, scenario analysis and planning, horizon scanning, brainstorming, Delphi technique, nominal group technique, SWOT (strengths, weaknesses, opportunities and threats) analysis, risk questionnaires	✓	✓	✓
For exploring and visualizing the context: stakeholder engagement matrices, PESTLE (political, economic, sociological, technological, legislation and environment) analysis, Boston grid, gap analysis, Pareto analysis	✓		
Structural guidance for risk analysis: risk checklists/prompt lists, project profile model (PPM), risk breakdown structure, risk taxonomy	✓		
Modelling styles: process mapping, flow charts, cause-and-effect diagrams, hazard and operability study (HAZOPs), failure mode effects analysis (FMEA), fault and event tree modelling, probability trees, critical path analysis (CPA), cash flow analysis, portfolio analysis	✓	✓	✓
Data analysis: descriptive statistics, model fitting		✓	✓
Model analysis methods and tools: risk simulation (Monte Carlo/Latin Hypercube), sensitivity analysis, stress testing		✓	✓
Risk recording and visualization techniques and tools: heat maps, RAG status reports, graphs of distributions, bar chart/radar chart, risk mapping, risk profiling, probability and consequence grid, risk Indicators, risk register/database	✓	✓	✓
Decision bases: expected value, utility theory, cost-benefit analysis			✓

Annex B (normative) Incorporating potentially positive consequences of risk

B.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 consequences, as well as bad.

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

B.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".

B.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 consequences are predominantly desirable, as well as those whose consequences are predominantly undesirable.

Where a consequence of a risk could be anywhere within a range it might be that this range includes desirable and undesirable consequence levels. Summarizing this range of consequences using its average is likely to be misleading because desirable and undesirable possibilities could balance, indicating zero risk level 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.

B.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 limit.

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 scope for avoiding an activity can be severely limited in the public sector, compared to the private sector, due to legal and regulatory obligations 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 correct response may be to terminate the project.

Avoiding risk can occur inappropriately if an organization or individual is unnecessarily risk averse or has incorrectly assessed the risks or rewards involved. 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 pursue 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. Using risk modification involves changing causes and/or effects to increase the likelihoods of desired consequences and/or decrease the likelihoods of undesired consequences. This may involve preventative measures, contingency plans, or additional funding.

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 achieved 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 that the organization to which the risk is transferred might not manage the risk effectively. Many risks can never be transferred completely, for example:

a) 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;

b) 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

c) 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 typically 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. A risk might be retained because no further worthwhile actions can be devised, or because the only remaining responses are unacceptable for some reason or cannot yet be implemented. 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. Self-insurance and similar internal risk financing arrangements are forms of risk retention. Retention of risks by default because of a failure to identify or appropriately manage them ought not to be tolerated.

Bibliography

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Standards publications

BS 25999, *Business continuity management*

BS ISO 31000, *Risk management – Principles and guidelines on implementation*

ISO/IEC Guide 73, *Risk management – Vocabulary*

Other publications

[1] HM Treasury: *Management of Risk – Principles and Concepts* (the Orange Book), London: 2004

[2] Office of Government Commerce: *Management of Risk: Guidance for Practitioners* (Third Edition), London: 2010

[3] COSO: *Enterprise Risk Management – Integrated Framework*, 2004 (for application of the Framework, see: http://www.coso.org/Publications/ErM/COSO_ErM. ppt#258,1,applying COSO's Enterprise risk Management – integrated Framework)

[4] AIRMIC, Alarm, IRM: *A Standard for Risk Management*, London: 2002.

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. 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 9001 Fax: +44 (0)20 8996 7001

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

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

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.

Information on standards

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

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

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

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

BSI Subscribing Members 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/standards**

Copyright

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

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

raising standards worldwide™

This British Standard gives recommendations for implementing the principles and guidelines in BS ISO 31000:2009, including the risk management framework and process. It 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 is intended for use by anyone with responsibility for, or involved in, any of the following:

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

BSI
389 Chiswick High Road
London W4 4AL
United Kingdom

Tel: +44 (0)20 8996 9001
Fax: +44 (0)20 8996 7001
Website: www.bsigroup.com
Email: info@bsigroup.com

ISBN 978-0-580-71607-2
9 780580 716072