

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.

© BSI 2011

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

Foreword *ii*

Introduction 1

1	Scope	3
2	Terms and definitions	4
3	Framework	11
3.1	General	11
3.2	Mandate and commitment	13
3.3	Design of framework for managing risk	13
3.4	Implementing risk management	28
3.5	Monitoring and review of the framework	29
3.6	Continual improvement of the framework	30
4	Process	31
4.1	General	31
4.2	Communication and consultation	32
4.3	Establishing the context	32
4.4	Risk assessment	33
4.5	Risk treatment	35
4.6	Monitoring and review	37
4.7	Monitoring performance of the instance of the risk management process	37
4.8	Providing information to others	38
4.9	Recording the risk management process	38

Annexes

Annex A (informative)	Risk management tools	40
Annex B (normative)	Incorporating potentially positive consequences of risk	42
Annex C (informative)	Effects of controls	42

Bibliography 45

List of figures

Figure 1 – Risk management perspectives	2
Figure 2 – Relationships between the context, principles, framework and process	11
Figure 3 – Illustrative set of instances of the risk management process in a larger organization	12
Figure 4 – Development of components of the risk management framework	12
Figure 5 – Typical documentation for risk management	15
Figure 6 – Items to include in the description of the framework	16
Figure 7 – The risk management process	32

List of tables

Table 1 – Examples of tailoring	3
Table 2 – One possible breakdown of roles	17
Table 3 – Leadership responsibilities	18
Table 4 – Minimum responsibilities for everyone in the organization	18
Table 5 – Role of a risk management function	19
Table 6 – Items to cover related to risk management competence	22
Table 7 – Features of risk identification	33
Table A.1 – Examples of risk management tools (including techniques)	41

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.

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

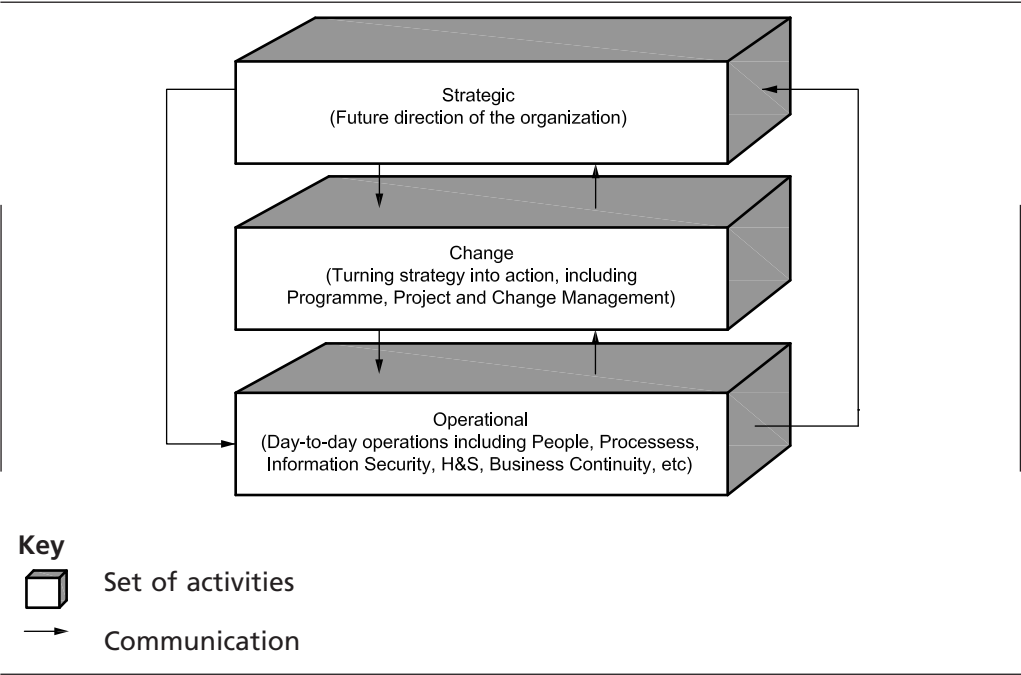


Table 1 Examples of tailoring

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:

- ensuring an organization achieves its objectives;
- ensuring risks are proactively managed in specific areas or activities;
- overseeing risk management in an organization;
- 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;*