

BS 31100:2021



BSI Standards Publication

**Risk management — Code of practice
and guidance for the implementation of
BS ISO 31000:2018**

bsi.

AVA **Documents**
Document Sharing Hub

Publishing and copyright information

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

© The British Standards Institution 2021

Published by BSI Standards Limited 2021

ISBN 978 0 539 16219 6

ICS 03.100.01

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

Committee reference RM/1

Draft for comment 21/30430517 DC

Amendments/corrigenda issued since publication

Date	Text affected

Contents

	Page
Foreword	ii
Introduction	1
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Risk management principles	3
4.1 Value creation and protection	3
<i>Figure 1 — Risk management principles</i>	4
4.2 Integrated	4
4.3 Structured and comprehensive	4
4.4 Customized	5
4.5 Inclusive	5
4.6 Dynamic	5
4.7 Best available information	5
4.8 Human and cultural factors	6
4.9 Continual improvement	6
5 Risk management framework	7
5.1 General	7
<i>Figure 2 — Risk management framework</i>	8
5.2 Leadership and commitment	9
5.3 Integration	9
5.4 Design	10
5.5 Implementation	12
5.6 Evaluation	12
5.7 Improvement	12
6 Risk management process	13
6.1 General	13
<i>Figure 3 — Risk management process</i>	13
6.2 Relationship between risk management process and risk management framework	13
6.3 Communication and consultation	15
6.4 Scope, context and criteria	16
6.5 Risk assessment	18
<i>Figure 4 — Risk criteria to determine where additional action is required</i>	20
6.6 Risk treatment	20
6.7 Monitoring and review	22
6.8 Recording and reporting	23
Annex A (informative) Emerging risk	25
Annex B (informative) Risk tools	27
<i>Figure B.1 — Application of techniques in the BS ISO 31000 risk management process</i>	28
Annex C (informative) Assessing progress and risk maturity	29
<i>Table C.1 — Questions to prompt discussion based on key elements of the standard</i>	30
<i>Table C.2 — Questions for the selection of a risk maturity model</i>	32
Bibliography	33

Summary of pages

This document comprises a front cover, an inside front cover, pages I to IV, pages 1 to 33, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 30 November 2021. It was prepared by Technical Committee RM/1, *Risk management*. A list of organizations represented on this committee can be obtained on request to the committee manager.

Supersession

This British Standard supersedes [BS 31100:2011](#), which is withdrawn.

Information about this document

Copyright is claimed on [Figure 1](#), [Figure 2](#) and [Figure 3](#). Copyright holders are the International Organization for Standardization (ISO), Chemin de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland. Copyright is claimed on [Figure B.1](#). Copyright holders are the International Electrotechnical Commission (IEC), 3 rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland.

BSI thanks the ISO and IEC for permission to reproduce information from their standards. All such extracts are copyright of the ISO and IEC. All rights reserved. The ISO and IEC have no responsibility for the placement and context in which the extracts and contents are reproduced, nor are ISO or IEC in any way responsible for the other content or accuracy therein.

Further information on the ISO and the IEC is available from www.iso.org and www.iec.ch respectively.

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at bsigroup.com/standards, or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

Use of this document

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

Users may substitute any of the recommendations in this British Standard with practices of equivalent or better outcome. 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 provisions of this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

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

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. “organization” rather than “organisation”).

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

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

Introduction

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

Effective risk management continuously, systematically and proportionally addresses the known risks surrounding the organization’s activities. It cannot be separated from the culture of the organization. Risk management comprises a framework and process(es) based upon eight core principles as described in BS ISO 31000:2018. This British Standard has been revised to align with BS ISO 31000:2018 and to add supplementary material (examples, concepts).

These are intended to help an organization to manage uncertainty in an effective, efficient and systematic way from strategic, programme, project and operational perspectives, as well as to support continual improvement. Risk management applies at all levels of an organization and to all activities.

Risk management is part of good management and organizations that manage risk well are more likely to achieve their objectives.

1 Scope

This British Standard gives recommendations for implementing the principles and guidelines in BS ISO 31000:2018 for developing a risk management framework and associated processes. It provides a basis for understanding, developing, implementing and maintaining proportionate and effective risk management throughout an organization, to enhance the organization’s likelihood of achieving its objectives.

This British Standard is intended for use by anyone with responsibility for, or who is involved in, any of the following:

- a) ensuring an organization achieves its objectives and enhances decision-making;
 - 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.
-

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes provisions of this document¹⁾. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS ISO 31000:2018, *Risk management – Guidelines*

¹⁾ Documents that are referred to solely in an informative manner are listed in the Bibliography.

3 Terms and definitions

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

3.1 consequence

outcome of an event (3.4) affecting objectives

NOTE 1 A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

NOTE 2 Consequences can be expressed qualitatively and/or quantitatively.

NOTE 3 Any consequence can escalate through cascading and cumulative effects.

[SOURCE: BS ISO 31000:2018, 3.6, modified]

3.2 control

measure that maintains and/or modifies risk (3.7)

NOTE 1 Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

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

[SOURCE: BS ISO 31000:2018, 3.8, modified]

3.3 control framework

structure that organizes and categorizes an organization's internal controls

NOTE This helps in the identification and assessment of risk and informs the organizational response.

3.4 event

occurrence or change of a particular set of circumstances

NOTE 1 An event can have one or more occurrences and can have several causes and several consequences (3.1).

NOTE 2 An event can also be something that is expected which does not happen, or something that is not expected which does happen.

NOTE 3 An event can be a risk source.

[SOURCE: BS ISO 31000:2018, 3.5]

3.5 likelihood

chance of something happening

NOTE 1 In risk management (3.8) 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 has the same broad interpretation as the term "probability" has in many languages other than English.

[SOURCE: BS ISO 31000:2018, 3.7]

3.6 organization-wide risk management

management of risks (3.7) related to the achievement of strategic objectives

NOTE Also known as "enterprise-wide risk management".

3.7 risk

effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

NOTE 2 Objectives can have different aspects and categories, and can be applied at different levels.

NOTE 3 Risk is usually expressed in terms of risk sources (3.11), potential events (3.4), their consequences (3.1) and their likelihood (3.5).

[SOURCE: BS ISO 31000:2018, 3.1]

3.8 risk management

coordinated activities to direct and control an organization with regard to risk (3.7)

[SOURCE: BS ISO 31000:2018, 3.2]

3.9 risk management framework

structure created by the collective application of policies, procedures, codes of conduct and documented information, along with values and beliefs, ways of communicating and resourcing, which construct the support needed from which systems can be built

3.10 risk management policy

statement of the overall intentions and direction of an organization related to risk management (3.8)

[SOURCE: PD ISO Guide 73:2009, 2.1.2]

3.11 risk source

element which alone or in combination has the potential to give rise to risk (3.7)

[SOURCE: BS ISO 31000:2018, 3.4]

3.12 stakeholder

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

NOTE The term “interested party” can be used as an alternative to “stakeholder”.

[SOURCE: BS ISO 31000:2018, 3.3]

3.13 top management

person or group of people who directs and controls an organization at the highest level

NOTE Top management is typically the senior executives (“C-suite”) of the organization. The term can be used more loosely if a large organization is spread over multiple regions or jurisdictions. For example, the scope of a management system for a business unit located in the UK might define its top management as the senior management team of the British business unit, despite the fact that the organization is from the United States, with its C-suite based in that region.

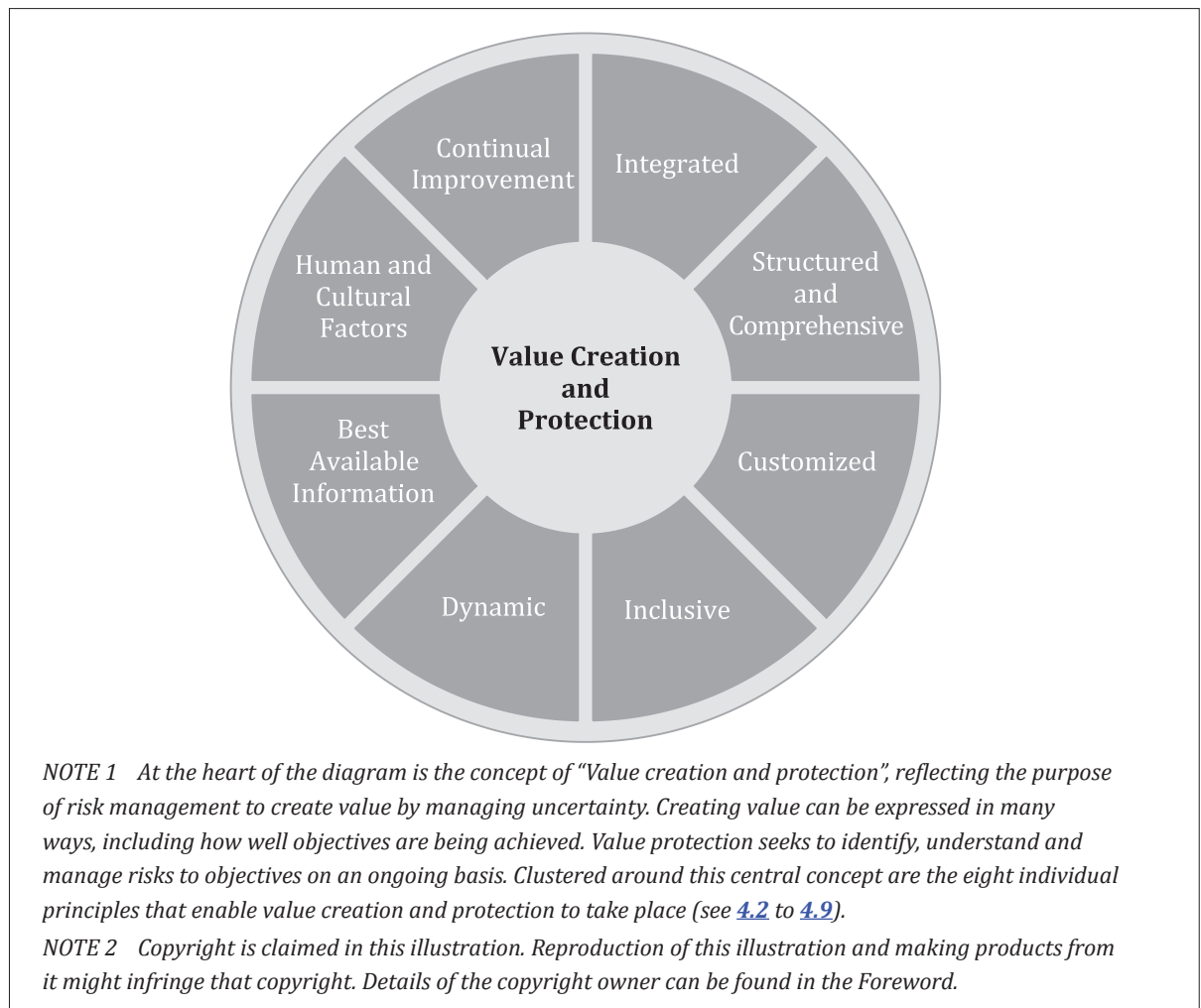
4 Risk management principles

4.1 Value creation and protection

To create and protect value, improve performance and sustainability, encourage innovation and support the achievement of the organization’s objectives, the principles set out in 4.2 to 4.9 (see [Figure 1](#)) should be implemented.

These principles should inform the foundation for managing risk and the establishment of the organization's risk management framework and processes.

Figure 1 — Risk management principles



4.2 Integrated

Risk management should be part of all organizational activities and processes, including strategic planning, ESG (environmental, social and governance), operational, financial, legal, IT (information technology), and project and change management. It should be integrated into wherever decisions are made and discussions are held, to enable the organization to grasp new opportunities whilst reducing the risk of business threats in a controlled manner.

NOTE 1 Management systems are important to enable integration of risk management, but arguably more critical are employee, social and other stakeholder participation and shared ownership, regardless of functional or business unit reporting lines. See PD ISO IWA 31 for the integration of risk management into the management system.

NOTE 2 Risk management could be fully integrated into a three lines framework (ownership, oversight and assurance, previously known as “the three lines of defence”) to ensure that robust assurance can be provided on the effectiveness of the controls in place.

4.3 Structured and comprehensive

Risk should be managed in a consistent and structured way across different parts of the organization, allowing for decisions to be taken with confidence and avoiding duplication of effort through efficient use of resources and management tools. The risk management framework should comprehensively cover all areas of risk, both internal and external, of relevance to the organization.

Whilst the framework is expected to provide clear guidance to members of staff with risk roles and responsibilities, it should not be so bureaucratic as to hinder implementation.

4.4 Customized

The risk management framework and processes should be customized to complement and meet the needs of the organization's external and internal context. There is no single correct approach for a risk management framework; each organization should customize the design and implementation based upon its culture, mission, vision and objectives, as well as its size and complexity.

NOTE For example, an organization working in a complex environment such as the nuclear industry has a more sophisticated risk management approach than a small retailer. Business ownership and growth trajectory are also important considerations, for example, a privately held business seeking an initial public offering (IPO) has a considerably different framework to that of a partner-owned organization.

4.5 Inclusive

COMMENTARY ON 4.5

Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be taken into account. This results in improved awareness and informed risk management and decision-making. Some stakeholders of the organization are likely to have formal accountabilities and responsibilities for risk management.

Top management should verify that all internal and external stakeholders are identified, and that effective communication is maintained. For those risks identified by stakeholders, the organization should have a process in place to explore such risks further and demonstrate that the stakeholders have been listened to. Everyone in the organization should be informed that they have a role in understanding, managing and communicating risks, issues, near misses and incidents.

4.6 Dynamic

COMMENTARY ON 4.6

The world is increasingly fast-changing, complex, connected and uncertain. The underlying business dynamics are changing fast and this context can trigger the need to recalibrate and rebalance risk management with increasing frequency.

In this changing world the concepts of ESG and “emerging” risk are of increasing concern.

In simple terms, emerging risks are risks that are new or changing in significance. Their possible trajectories exhibit high levels of uncertainty. Similarly, they often lead to multiple knock-on consequences. This topic is explored further in [Annex A](#).

Risks can emerge, change or disappear as the organization's external and internal context changes, so risk management should anticipate, detect, acknowledge, report, escalate and respond to changes and events in an appropriate and timely manner.

The risk management framework should be able to facilitate the continual identification of and response to change, recognizing that some risks are subject to frequent change whereas others can remain constant over long periods.

4.7 Best available information

Everyone in the organization should be proactive in sourcing the best available information, using relevant organizational and external information to inform their risk management decision-making, and collaborating with other stakeholders. Collaboration with others should be encouraged to prevent people becoming siloed in their approach to risk.

Sources of risk data should be recorded and can include subjective opinion as well as empirical data and forecast information. Data should be as accurate as possible and their limitations understood (emerging risk data can never be entirely relied upon because there is so much uncertainty in respect of new and volatile risks), timely and verifiable, with quality assurance in place.

NOTE Horizon scanning, involving a combination of relevant forward-looking indicators, can be used.

Risk perception and attitudes can vary widely across the organization and people should be aware of biases which can lead to misinformed decisions being made.

4.8 Human and cultural factors

To be effective, risk management should be embedded within the culture of the organization. All those working within and on behalf of an organization should understand how their own roles and responsibilities help the organization achieve its short and long-term objectives.

The risk culture should include:

- a) a distinct and consistent tone from top management in respect of risk-taking and avoidance;
- b) a commitment to ethical principles and taking account of wider stakeholder positions in decision-making;

NOTE Examples of poor behaviour include bullying and inappropriate sales incentives.

- c) a common acceptance across the organization of risk management, including clear accountability for and ownership of specific risks and risk areas;
- d) transparent and timely risk information flowing up and down the organization, with adverse news rapidly communicated without fear of blame;
- e) active learning from mistakes and near misses by encouragement of risk event reporting and whistle-blowing;
- f) assurance that no process or activity is too large, complex or obscure for the risk not to be readily understood;
- g) rewarding and encouraging appropriate risk-taking behaviours, and addressing inappropriate behaviours;
- h) valuing, encouraging and developing risk management skills and knowledge;
- i) sufficient diversity of perspectives, values and beliefs to ensure that the status quo is consistently and rigorously challenged; and
- j) appropriate employee engagement to permit a focus on both business and personal needs.

4.9 Continual improvement

The risk management framework should be reviewed with other business processes on a regular, perhaps annual, basis.

The organization should implement processes to promote continual improvement, using such methods as:

- a) reviewing risk management information to determine the accuracy and effectiveness of data, for instance, whether the estimation of risk impact accurately reflects the consequences of an event that occurred;
- b) learning from its own and others' experiences (near misses), events which have occurred (positive and negative) and insurance claims, to verify that the root causes are understood and actions are put in place to control future events;