INTERNATIONAL STANDARD

ISO 31000

Redline version
compares Second edition to
First edition

Risk management — Guidelines

Management du risque — Lignes directrices

Reference number
ISO 31000:redline:2018(E)

IMPORTANT — PLEASE NOTE

This is a mark-up copy and uses the following colour coding:

Text example 1	— indicates added text (in green)
~~Text example 2~~	— indicates removed text (in red)
	— indicates added graphic figure
	— indicates removed graphic figure
1.x ...	— Heading numbers containg modifications are highlighted in yellow in the Table of Contents

DISCLAIMER

This Redline version provides you with a quick and easy way to compare the main changes between this edition of the standard and its previous edition. It doesn't capture all single changes such as punctuation but highlights the modifications providing customers with the most valuable information. Therefore it is important to note that this Redline version is not the official ISO standard and that the users must consult with the clean version of the standard, which is the official standard, for implementation purposes.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

~~International Standards are~~The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the ~~rules given in~~editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

~~The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.~~

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

~~ISO 31000~~This document was prepared by ~~the ISO Technical Management Board Working Group on risk~~Technical Committee ISO/TC 262, *Risk management*.

This second edition cancels and replaces the first edition (ISO 31000:2009) which has been technically revised.

The main changes compared to the previous edition are as follows:

— review of the principles of risk management, which are the key criteria for its success;

— highlighting of the leadership by top management and the integration of risk management, starting with the governance of the organization;

— greater emphasis on the iterative nature of risk management, noting that new experiences, knowledge and analysis can lead to a revision of process elements, actions and controls at each stage of the process;

— streamlining of the content with greater focus on sustaining an open systems model to fit multiple needs and contexts.

Introduction

This document is for use by people who create and protect value in organizations by managing risks, making decisions, setting and achieving objectives and improving performance.

Organizations of all types and sizes face ~~internal and external~~external and internal factors and influences that make it uncertain whether ~~and when~~ they will achieve their objectives. ~~The effect this uncertainty has on an organization's objectives is "risk".~~

~~All activities of an organization involve risk. Organizations manage risk by identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Throughout this process, they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required. This International Standard describes this systematic and logical process in detail.~~

~~While all organizations manage risk to some degree, this International Standard establishes a number of principles that need to be satisfied to make risk management effective. This International Standard recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture~~Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions.

~~Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities.~~

~~Although the practice of risk management has been developed over time and within many sectors in order to meet diverse needs, the adoption of consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently and coherently across an organization. The generic approach described in this International Standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context~~Managing risk is part of governance and leadership, and is fundamental to how the organization is managed at all levels. It contributes to the improvement of management systems.

Managing risk is part of all activities associated with an organization and includes interaction with stakeholders.

~~Each specific sector or application of risk management brings with it individual needs, audiences, perceptions and criteria. Therefore, a key feature of this International Standard is the inclusion of "establishing the context" as an activity at the start of this generic risk management process. Establishing the context will capture the objectives of the organization, the environment in which it pursues those objectives, its stakeholders and the diversity of risk criteria – all of which will help reveal and assess the nature and complexity of its risks~~Managing risk considers the external and internal context of the organization, including human behaviour and cultural factors.

~~The relationship between the principles for managing risk, the framework in which it occurs and the risk management process described in this International Standard are shown~~Managing risk is based on the principles, framework and process outlined in this document, as illustrated in Figure 1. These components might already exist in full or in part within the organization, however, they might need to be adapted or improved so that managing risk is efficient, effective and consistent.

~~When implemented and maintained in accordance with this International Standard, the management of risk enables an organization to, for example:~~

- ~~increase the likelihood of achieving objectives;~~
- ~~encourage proactive management;~~
- ~~be aware of the need to identify and treat risk throughout the organization;~~

- improve the identification of opportunities and threats;
- comply with relevant legal and regulatory requirements and international norms;
- improve mandatory and voluntary reporting;
- improve governance;
- improve stakeholder confidence and trust;
- establish a reliable basis for decision making and planning;
- improve controls;
- effectively allocate and use resources for risk treatment;
- improve operational effectiveness and efficiency;
- enhance health and safety performance, as well as environmental protection;
- improve loss prevention and incident management;
- minimize losses;
- improve organizational learning; and
- improve organizational resilience.

This International Standard is intended to meet the needs of a wide range of stakeholders, including:

a) those responsible for developing risk management policy within their organization;

b) those accountable for ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity;

c) those who need to evaluate an organization's effectiveness in managing risk; and

d) developers of standards, guides, procedures and codes of practice that, in whole or in part, set out how risk is to be managed within the specific context of these documents.

The current management practices and processes of many organizations include components of risk management, and many organizations have already adopted a formal risk management process for particular types of risk or circumstances. In such cases, an organization can decide to carry out a critical review of its existing practices and processes in the light of this International Standard.

In this International Standard, the expressions "risk management" and "managing risk" are both used. In general terms, "risk management" refers to the architecture (principles, framework and process) for managing risks effectively, while "managing risk" refers to applying that architecture to particular risks.

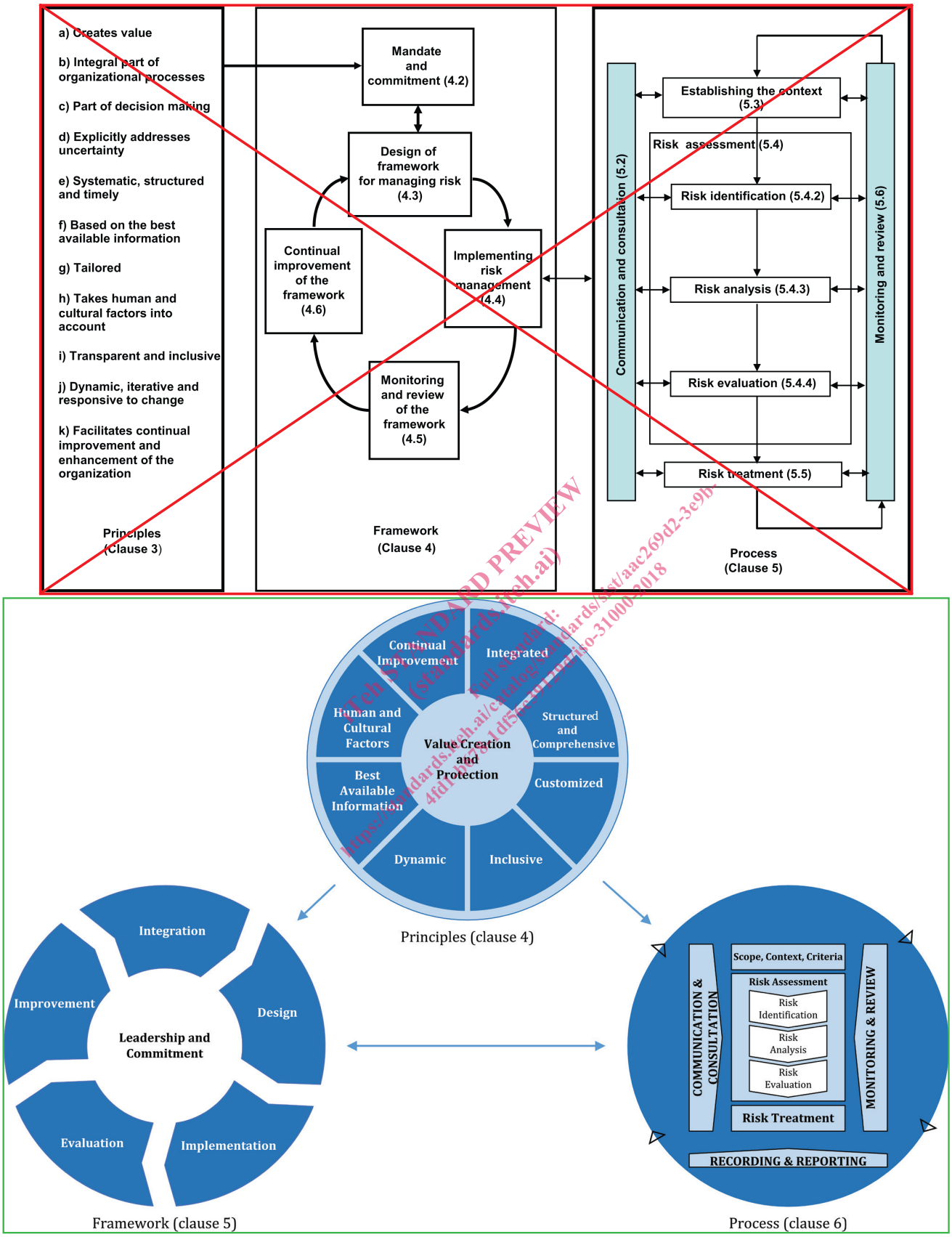

Figure 1 — ~~Relationships between the risk management principles~~ Principles, framework and process

Risk management — Guidelines

1 Scope

This ~~International Standard provides principles and generic guidelines on risk management.~~document provides guidelines on managing risk faced by organizations. The application of these guidelines can be customized to any organization and its context.

This ~~International Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any~~document provides a common approach to managing any type of risk and is not industry or sector specific.

~~NOTE For convenience, all the different users of this International Standard are referred to by the general term "organization".~~

This ~~International Standard~~document can be ~~applied~~used throughout the life of ~~an~~the organization~~, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets~~ and can be applied to any activity, including decision-making at all levels.

~~This International Standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.~~

~~Although this International Standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.~~

~~It is intended that this International Standard be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.~~

~~This International Standard is not intended for the purpose of certification.~~

2 Normative references

There are no normative references in this document.

~~2~~3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org

~~2.1~~3.1
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected ~~— positive and/or negative~~. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects ~~(such as financial, health and safety, and environmental goals) and can apply~~and categories, and can be applied at different levels ~~(such as strategic, organization-wide, project, product and process)~~.

~~Note 3 to entry: Risk is often characterized by reference to potential~~ *events* (2.17) ~~and~~ *consequences* (2.18)~~, or a combination of these.~~

Note 4 to entry: Risk is ~~often~~usually expressed in terms of ~~a combination of the consequences of an event (including changes in circumstances)~~ *risk sources* (3.4), potential *events* (3.5), their *consequences* (3.6) and ~~the associated~~their *likelihood* (~~2.19~~3.7) ~~of occurrence~~.

~~Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.~~

~~[SOURCE: ISO Guide 73:2009, definition 1.1]~~

~~2.2~~3.2
risk management
coordinated activities to direct and control an organization with regard to *risk* (~~2.1~~3.1)

~~[SOURCE: ISO Guide 73:2009, definition 2.1]~~

~~2.3~~
~~risk management framework~~
~~set of components that provide the foundations and organizational arrangements for designing, implementing, *monitoring* (2.28), reviewing and continually improving *risk management* (2.2) throughout the organization~~

~~Note 1 to entry: The foundations include the policy, objectives, mandate and commitment to manage *risk* (2.1).~~

~~Note 2 to entry: The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.~~

~~Note 3 to entry: The risk management framework is embedded within the organization's overall strategic and operational policies and practices.~~

~~[SOURCE: ISO Guide 73:2009, definition 2.1.1]~~

~~2.4~~
~~risk management policy~~
~~statement of the overall intentions and direction of an organization related to *risk management* (2.2)~~

~~[SOURCE: ISO Guide 73:2009, definition 2.1.2]~~

~~2.5~~
~~risk attitude~~
~~organization's approach to assess and eventually pursue, retain, take or turn away from *risk* (2.1)~~

~~[SOURCE: ISO Guide 73:2009, definition 3.7.1.1]~~

~~2.6~~
~~risk management plan~~
~~scheme within the *risk management framework* (2.3) specifying the approach, the management components and resources to be applied to the management of *risk* (2.1)~~

~~Note 1 to entry: Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.~~

~~Note 2 to entry: The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.~~

~~[SOURCE: ISO Guide 73:2009, definition 2.1.3]~~

~~**2.7**~~
~~**risk owner**~~
~~person or entity with the accountability and authority to manage a *risk* (2.1)~~

~~[SOURCE: ISO Guide 73:2009, definition 3.5.1.5]~~

~~**2.8**~~
~~**risk management process**~~
~~systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, *monitoring* (2.28) and reviewing *risk* (2.1)~~

~~[SOURCE: ISO Guide 73:2009, definition 3.1]~~

~~**2.9**~~
~~**establishing the context**~~
~~defining the external and internal parameters to be taken into account when managing risk, and setting the scope and *risk criteria* (2.22) for the *risk management policy* (2.4)~~

~~[SOURCE: ISO Guide 73:2009, definition 3.3.1]~~

~~**2.10**~~
~~**external context**~~
~~external environment in which the organization seeks to achieve its objectives~~

~~Note 1 to entry: 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* (2.13).~~

~~[SOURCE: ISO Guide 73:2009, definition 3.3.1.1]~~

~~**2.11**~~
~~**internal context**~~
~~internal environment in which the organization seeks to achieve its objectives~~

~~Note 1 to entry: 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.~~

~~[SOURCE: ISO Guide 73:2009, definition 3.3.1.2]~~

~~**2.12**~~
~~**communication and consultation**~~
~~continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with *stakeholders* (2.13) regarding the management of *risk* (2.1)~~

~~Note 1 to entry: The information can relate to the existence, nature, form, *likelihood* (2.19), significance, evaluation, acceptability and treatment of the management of risk.~~

~~Note 2 to entry: 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.~~

~~[SOURCE: ISO Guide 73:2009, definition 3.2.1]~~

~~2.13~~**3.3**
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Note 1 to entry: ~~A decision maker can be a stakeholder~~The term "interested party" can be used as an alternative to "stakeholder".

~~[SOURCE: ISO Guide 73:2009, definition 3.2.1.1]~~

~~**2.14**~~
~~**risk assessment**~~
~~overall process of *risk identification* (2.15), *risk analysis* (2.21) and *risk evaluation* (2.24)~~

~~[SOURCE: ISO Guide 73:2009, definition 3.4.1]~~

~~**2.15**~~
~~**risk identification**~~
~~process of finding, recognizing and describing *risks* (2.1)~~

~~Note 1 to entry: Risk identification involves the identification of *risk sources* (2.16), *events* (2.17), their causes and their potential *consequences* (2.18).~~

~~Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and *stakeholder's* (2.13) needs.~~

~~[SOURCE: ISO Guide 73:2009, definition 3.5.1]~~

~~2.16~~**3.4**
risk source
element which alone or in combination has the ~~intrinsic~~ potential to give rise to *risk* (~~2.1~~3.1)

~~Note 1 to entry: A risk source can be tangible or intangible.~~

~~[SOURCE: ISO Guide 73:2009, definition 3.5.1.2]~~

~~2.17~~**3.5**
event
occurrence or change of a particular set of circumstances

Note 1 to entry: An event can ~~be~~have one or more occurrences, and can have several causes and several *consequences* (3.6).

Note 2 to entry: An event can ~~consist of something not happening~~also be something that is expected which does not happen, or something that is not expected which does happen.

Note 3 to entry: An event can ~~sometimes be referred to as an "incident" or "accident"~~be a risk source.