INTERNATIONAL STANDARD

ISO 31000

Second edition
2018-02

Risk management — Guidelines

Management du risque — Lignes directrices

SIST Preview
(https://ecommerce.sist.si)

ISO 31000:2018
https://ecommerce.sist.si/catalog/standards/sist/aac269d2-3e9b-4fd1-b678-1df56c39129d/iso-31000-2018

Reference number
ISO 31000:2018(E)

© ISO 2018

SIST Preview
(https://ecommerce.sist.si)

ISO 31000:2018
https://ecommerce.sist.si/catalog/standards/sist/aac269d2-3e9b-4fd1-b678-1df56c39129d/iso-31000-2018



COPYRIGHT PROTECTED DOCUMENT

© ISO 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

 © ISO 2018 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Principles ... **2**
5 Framework ... **4**
5.1 General ... 4
5.2 Leadership and commitment ... 5
5.3 Integration ... 5
5.4 Design ... 6
5.4.1 Understanding the organization and its context ... 6
5.4.2 Articulating risk management commitment ... 6
5.4.3 Assigning organizational roles, authorities, responsibilities and accountabilities 7
5.4.4 Allocating resources ... 7
5.4.5 Establishing communication and consultation ... 7
5.5 Implementation ... 7
5.6 Evaluation ... 8
5.7 Improvement ... 8
5.7.1 Adapting ... 8
5.7.2 Continually improving ... 8
6 Process ... **8**
6.1 General ... 8
6.2 Communication and consultation ... 9
6.3 Scope, context and criteria ... 10
6.3.1 General ... 10
6.3.2 Defining the scope ... 10
6.3.3 External and internal context ... 10
6.3.4 Defining risk criteria ... 10
6.4 Risk assessment ... 11
6.4.1 General ... 11
6.4.2 Risk identification ... 11
6.4.3 Risk analysis ... 12
6.4.4 Risk evaluation ... 12
6.5 Risk treatment ... 13
6.5.1 General ... 13
6.5.2 Selection of risk treatment options ... 13
6.5.3 Preparing and implementing risk treatment plans ... 14
6.6 Monitoring and review ... 14
6.7 Recording and reporting ... 14
Bibliography ... **16**

SIST Preview
(https://ecommerce.sist.si)
ISO 31000:2018
https://ecommerce.sist.si/catalog/standards/sist/aac269d2-3e9b-4fd1-b678-1dB0c39129d/iso-31000-2018

© ISO 2018 – All rights reserved

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.

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 editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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.

SIST Preview
(https://ecommerce.sist.si)

This document was prepared by Technical Committee ISO/TC 262, *Risk management*.

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

ISO 31000:2018
https://ecommerce.sist.si/catalog/standards/sist/aac269d2-3e9b-4fd1-b678-1df56c39129d/iso-31000-2018

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.

© ISO 2018 – All rights reserved

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 external and internal factors and influences that make it uncertain whether they will achieve their objectives.

Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions.

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.

Managing risk considers the external and internal context of the organization, including human behaviour and cultural factors.

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.

SIST Preview
(https://ecommerce.sist.si)
ISO 31000:2018
https://ecommerce.sist.si/catalog/standards/sist/...-1df56c39129d/iso-31000-2018

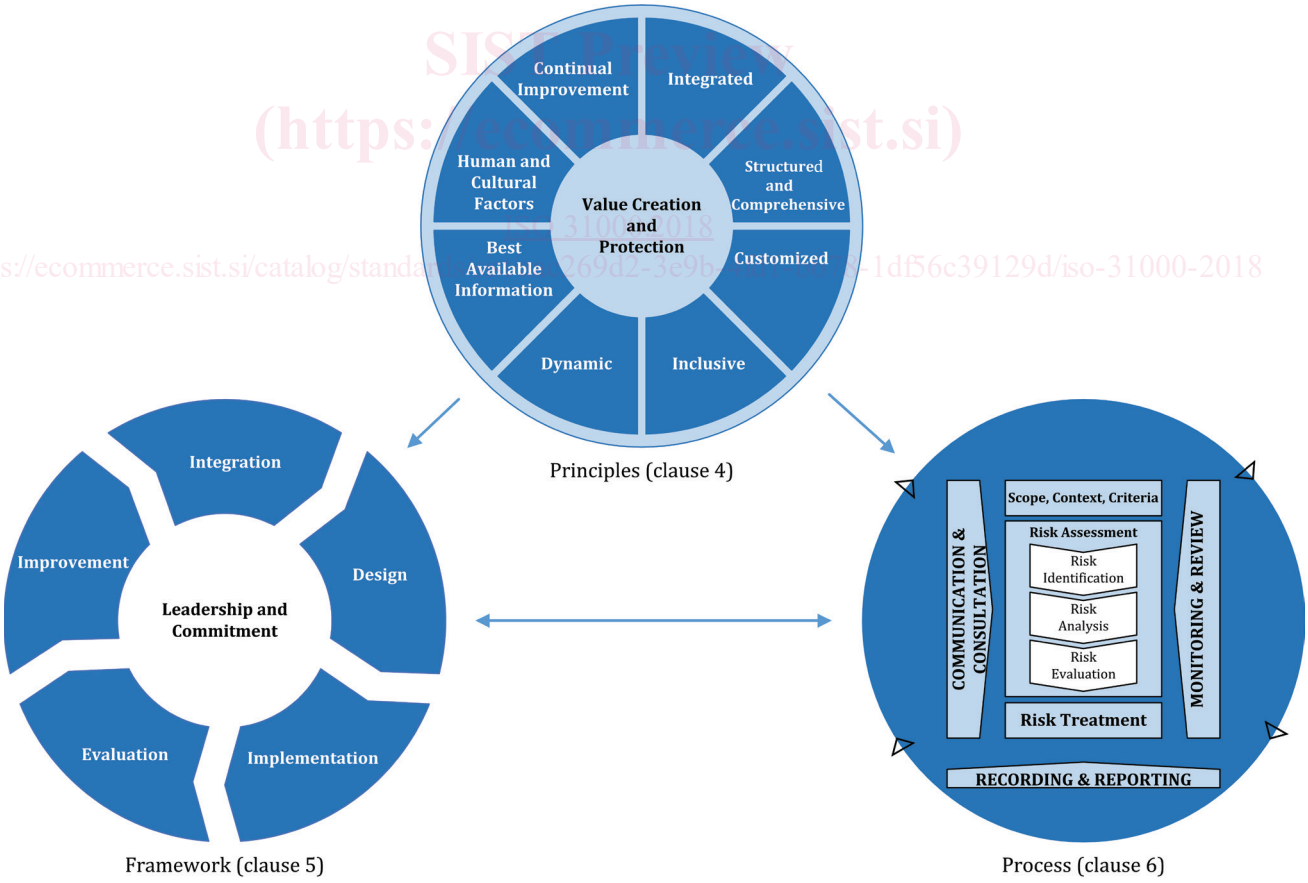


Figure 1 — Principles, framework and process

© ISO 2018 – All rights reserved

SIST Preview
(https://ecommerce.sist.si)

ISO 31000:2018
https://ecommerce.sist.si/catalog/standards/sist/aac269d2-3e9b-4fd1-b678-1df56c39129d/iso-31000-2018

Risk management — Guidelines

1 Scope

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

This document provides a common approach to managing any type of risk and is not industry or sector specific.

This document can be used throughout the life of the organization and can be applied to any activity, including decision-making at all levels.

2 Normative references

There are no normative references in this document.

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

SIST Preview
(https://standards.iteh.ai)
ISO 31000:2018
https://standards.iteh.ai/catalog/standards/sist/aac269d2-3e9b-4fd1-b678-1df56c39129d/iso-31000-2018

3.1
risk
effect of uncertainty on objectives

Note 1 to entry: 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 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of *risk sources* (3.4), potential *events* (3.5), their *consequences* (3.6) and their *likelihood* (3.7).

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

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

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

© ISO 2018 – All rights reserved

3.5
event
occurrence or change of a particular set of circumstances

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

Note 2 to entry: An event can 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 be a risk source.

3.6
consequence
outcome of an *event* (3.5) affecting objectives

Note 1 to entry: A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Note 2 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 3 to entry: Any consequence can escalate through cascading and cumulative effects.

3.7
likelihood
chance of something happening

Note 1 to entry: In *risk management* (3.2) 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).

SIST ISO 31000:2018
(https://ecommerce.sist.si)

Note 2 to entry: 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.

3.8
control
measure that maintains and/or modifies *risk* (3.1)

Note 1 to entry: 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 to entry: Controls may not always exert the intended or assumed modifying effect.

4 Principles

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives.

The principles outlined in Figure 2 provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. The principles are the foundation for managing risk and should be considered when establishing the organization's risk management framework and processes. These principles should enable an organization to manage the effects of uncertainty on its objectives.

© ISO 2018 – All rights reserved

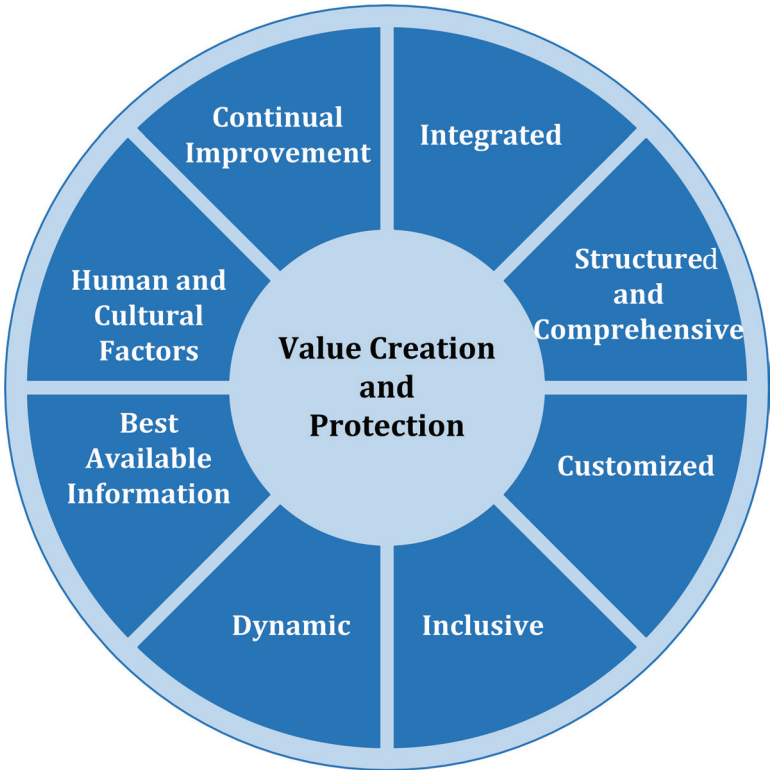


Figure 2 — Principles

SIST Preview
(https://ecommerce.sist.si)
ISO 31000:2018
https://ecommerce.sist.si/catalog/standards/sist/aaac2b9d-3e9b-4dd1-8078-fdf56c39129d/iso-31000-2018

Effective risk management requires the elements of Figure 2 and can be further explained as follows.

a) Integrated

Risk management is an integral part of all organizational activities.

b) Structured and comprehensive

A structured and comprehensive approach to risk management contributes to consistent and comparable results.

c) Customized

The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives.

d) Inclusive

Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

e) Dynamic

Risks can emerge, change or disappear as an organization's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

f) Best available information

The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

© ISO 2018 – All rights reserved

g) Human and cultural factors

Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

h) Continual improvement

Risk management is continually improved through learning and experience.

5 Framework

5.1 General

The purpose of the risk management framework is to assist the organization in integrating risk management into significant activities and functions. The effectiveness of risk management will depend on its integration into the governance of the organization, including decision-making. This requires support from stakeholders, particularly top management.

Framework development encompasses integrating, designing, implementing, evaluating and improving risk management across the organization. Figure 3 illustrates the components of a framework.



SIST Preview (https://ecommerce.sist.si)
ISO 31000:2018
https://ecommerce.sist.si/catalog/standards/sist/aac26ed2-3e9b-4d1-b628-1d56c39129d/iso-31000-2018

Figure 3 — Framework

The organization should evaluate its existing risk management practices and processes, evaluate any gaps and address those gaps within the framework.

The components of the framework and the way in which they work together should be customized to the needs of the organization.

© ISO 2018 – All rights reserved

5.2 Leadership and commitment

Top management and oversight bodies, where applicable, should ensure that risk management is integrated into all organizational activities and should demonstrate leadership and commitment by:

— customizing and implementing all components of the framework;

— issuing a statement or policy that establishes a risk management approach, plan or course of action;

— ensuring that the necessary resources are allocated to managing risk;

— assigning authority, responsibility and accountability at appropriate levels within the organization.

This will help the organization to:

— align risk management with its objectives, strategy and culture;

— recognize and address all obligations, as well as its voluntary commitments;

— establish the amount and type of risk that may or may not be taken to guide the development of risk criteria, ensuring that they are communicated to the organization and its stakeholders;

— communicate the value of risk management to the organization and its stakeholders;

— promote systematic monitoring of risks;

— ensure that the risk management framework remains appropriate to the context of the organization.

Top management is accountable for managing risk while oversight bodies are accountable for overseeing risk management. Oversight bodies are often expected or required to:

— ensure that risks are adequately considered when setting the organization's objectives;

— understand the risks facing the organization in pursuit of its objectives;

— ensure that systems to manage such risks are implemented and operating effectively;

— ensure that such risks are appropriate in the context of the organization's objectives;

— ensure that information about such risks and their management is properly communicated.

5.3 Integration

Integrating risk management relies on an understanding of organizational structures and context. Structures differ depending on the organization's purpose, goals and complexity. Risk is managed in every part of the organization's structure. Everyone in an organization has responsibility for managing risk.

Governance guides the course of the organization, its external and internal relationships, and the rules, processes and practices needed to achieve its purpose. Management structures translate governance direction into the strategy and associated objectives required to achieve desired levels of sustainable performance and long-term viability. Determining risk management accountability and oversight roles within an organization are integral parts of the organization's governance.

Integrating risk management into an organization is a dynamic and iterative process, and should be customized to the organization's needs and culture. Risk management should be a part of, and not separate from, the organizational purpose, governance, leadership and commitment, strategy, objectives and operations.

SIST Pregled
(https://ecommerce.sist.si)
ISO 31000:2018