

Redline version
compares Second edition to
First edition



Risk management — Guidelines

Management du risque — Lignes directrices

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

ISO 31000:2018

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



Reference number
ISO 31000:redline:2018(E)

© ISO 2018

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.



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

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
2 3 Terms and definitions	1
3 4 Principles	7
4 5 Framework	9
4.1 5.1 General	9
4.2 5.2 Mandate Leadership and commitment	11
5.3 Integration	11
4.3 5.4 Design of framework for managing risk	12
4.3.1 5.4.1 Understanding of the organization and its context	12
4.3.2 5.4.2 Establishing Articulating risk management policy commitment	13
4.3.3 5.4.3 Accountability Assigning organizational roles, authorities, responsibilities and accountabilities	13
4.3.4 Integration into organizational processes	14
4.3.5 5.4.4 Resources Allocating resources	14
4.3.6 5.4.5 Establishing internal communication and reporting mechanisms consultation	14
4.3.7 Establishing external communication and reporting mechanisms	15
4.4 5.5 Implementing risk management Implementation	15
4.4.1 Implementing the framework for managing risk	15
4.4.2 Implementing the risk management process	15
4.5 5.6 Monitoring and review of the framework Evaluation	16
4.6 5.7 Continual improvement of the framework Improvement	16
5.7.1 Adapting	16
5.7.2 Continually improving	16
5 6 Process	16
5.1 6.1 General	16
5.2 6.2 Communication and consultation	18
5.3 6.3 Establishing the context Scope, context and criteria	18
5.3.1 6.3.1 General	18
5.3.2 6.3.2 Establishing the external context Defining the scope	19
5.3.3 6.3.3 Establishing the External and internal context	19
5.3.4 6.3.4 Establishing the context of the risk management process	20
5.3.5 6.3.4 Defining risk criteria	20
5.4 6.4 Risk assessment	21
5.4.1 6.4.1 General	21
5.4.2 6.4.2 Risk identification	21
5.4.3 6.4.3 Risk analysis	22
5.4.4 6.4.4 Risk evaluation	23
5.5 6.5 Risk treatment	24
5.5.1 6.5.1 General	24
5.5.2 6.5.2 Selection of risk treatment options	24
5.5.3 6.5.3 Preparing and implementing risk treatment plans	25
5.6 6.6 Monitoring and review	26
5.7 6.7 Recording the risk management process and reporting	27
Annex A (informative) Attributes of enhanced risk management	28
Bibliography	30

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

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

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

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,~~