AS ISO 31000:2018

Risk management—Guidelines

AS ISO 31000:2018

This Australian Standard® was prepared by the Australian members of the Joint Technical Committee OB-007, Risk Management. It was approved on behalf of the Council of Standards Australia on 19 September 2018.

This Standard was published on 30 October 2018.

The following are represented on Committee OB-007:

Attorney-General's Department (Australian Government)
Australian and New Zealand Institute of Insurance and Finance
Australian Chamber of Commerce and Industry
Australian Industry Group
Australian Logistics Council
Australian Risk Policy Institute
Austroads
CivicRisk Mutual
Department of Finance (Australian Government)
Employers and Manufacturers Association
Engineers Australia
Financial Services Institute of Australasia
Governance Institute of Australia
Institute of Internal Auditors — Australia
Minerals Council of Australia
Queensland University of Technology
Risk Management Institute of Australasia
Royal Australian Chemical Institute
Safety Institute of Australia
Security Professionals Australasia
University of New South Wales
Water Services Association of Australia

This Standard was issued in draft form for comment as DR AS/NZS ISO 31000:2018.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76072 205 0

Australian STANDARD

Risk management—Guidelines

Originated as AS/NZS 4360:1995.
Third edition 2004.
Jointly revised and redesignated as AS/NZS ISO 31000:2009.
Revised and redesignated as AS ISO 31000:2018.

Preface

This was prepared by the Australian members of the Joint Standards Australia/Standards New Zealand Committee OB-007 Risk Management, to supersede AS/NZS ISO 31000:2009 *Risk management – Principles and guidelines*.

After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this Standard as an Australian Standard rather than an Australian/New Zealand Standard.

The objective of this Standard is to provide guidelines on managing risk faced by organizations. The application of these guidelines can be customized to any organization and its context.

This Standard also provides a common approach to managing any type of risk and is not industry or sector specific. This Standard may be used throughout the life of the organization and applied to any activity, including decision-making at all levels.

In addition to this Standard, the Australian members of the Joint Standards Australia/Standards New Zealand Committee OB-007 has prepared a range of guidance documents that support specific applications of risk management.

This Standard is identical with, and has been reproduced from ISO 31000:2018, *Risk management — Guidelines.*

As this document has been reproduced from an International Standard, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms 'normative' and 'informative' are used in Standards to define the application of the appendices to which they apply. A 'normative' appendix is an integral part of a Standard, whereas an 'informative' appendix is only for information and guidance.

Contents

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.

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.

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 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.

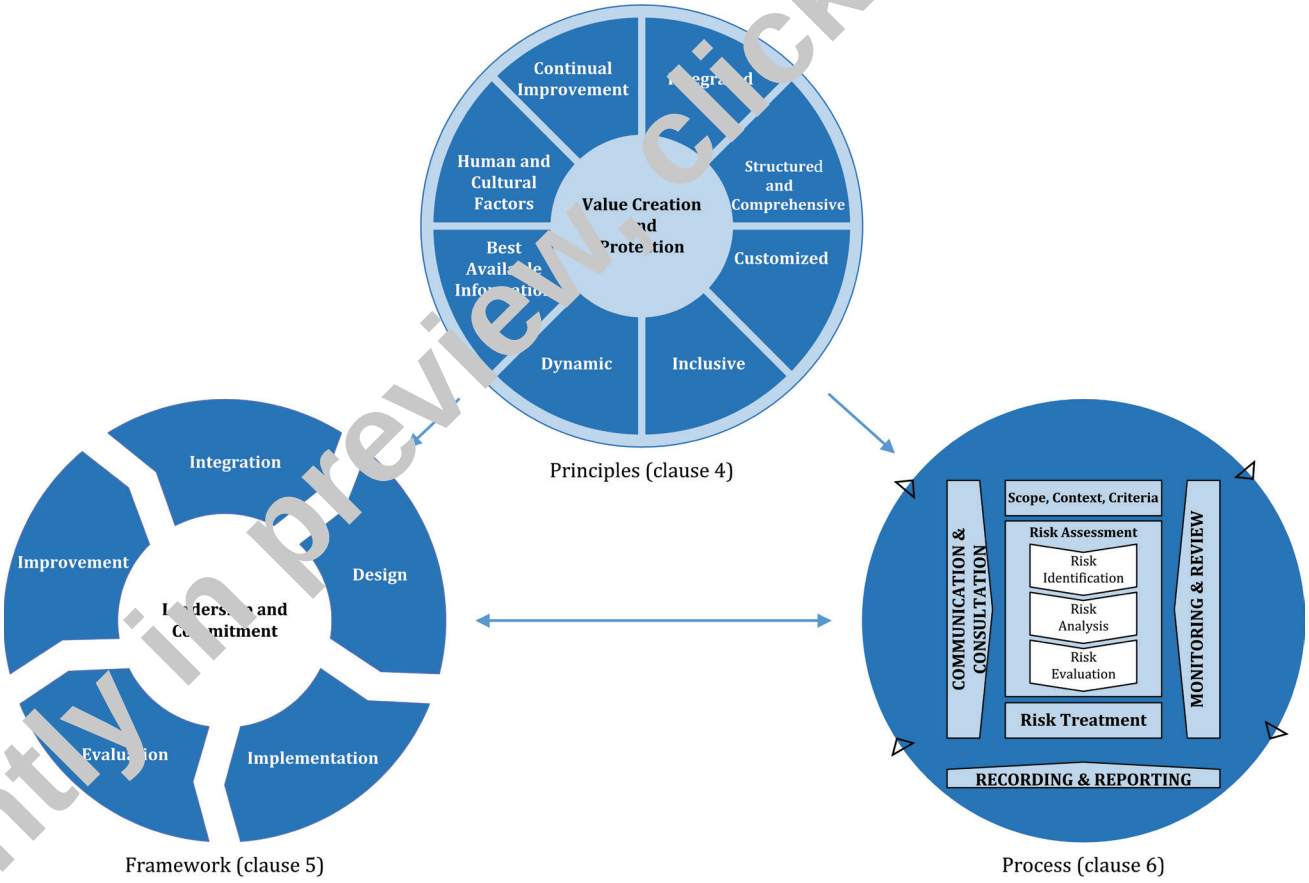

Figure 1 — Principles, framework and process

Australian Standard®

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

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)