EESTI STANDARD EVS-ISO 31000:2018

RISKIJUHTIMINE. Juhised

Risk management - Guidelines (ISO 31000:2018, identical)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
See Eesti standard EVS-ISO 31000:2018 „Riskijuhtimine. Juhised“ sisaldab rahvusvahelise standardi ISO 31000:2018 „Risk management – Guidelines“ identset ingliskeelset teksti.	This Estonian Standard EVS-ISO 31000:2018 consists of the identical English text of the International Standard ISO 31000:2018 „Risk management – Guidelines“.
Ettepaneku rahvusvahelise standardi ümbertrüki meetodil ülevõtuks on esitanud EVS/TK 33, standardi avaldamist on korraldanud Eesti Standardikeskus.	Proposal to adopt the International Standard by reprint method has been presented by EVS/TK 33, the Estonian Standard has been published by the Estonian Centre for Standardisation.
Standard EVS-ISO 31000:2018 on jõustunud sellekohase teate avaldamisega EVS Teataja 2018. aasta märtsikuu numbris.	Standard EVS-ISO 31000:2018 has been endorsed with a notification published in the March 2018 issue of the official bulletin of the Estonian Centre for Standardisation.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Käsitlusala

See dokument esitab juhised riskijuhtimiseks, millega organisatsioonid silmitsi seisavad. Nende juhiste rakendamist saab kohandada mis tahes organisatsioonile ja selle kontekstile.

See dokument näeb ette ühtse käsitlusviisi mis tahes tüüpi riskide juhtimiseks ja ei ole tööstusharu- või tegevusalapõhine.

Seda dokumenti saab kasutada kogu organisatsiooni eluea jooksul ja seda saab rakendada mis tahes tegevuses, sealhulgas otsuste langetamisel kõigil tasanditel.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 03.100.01

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

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.

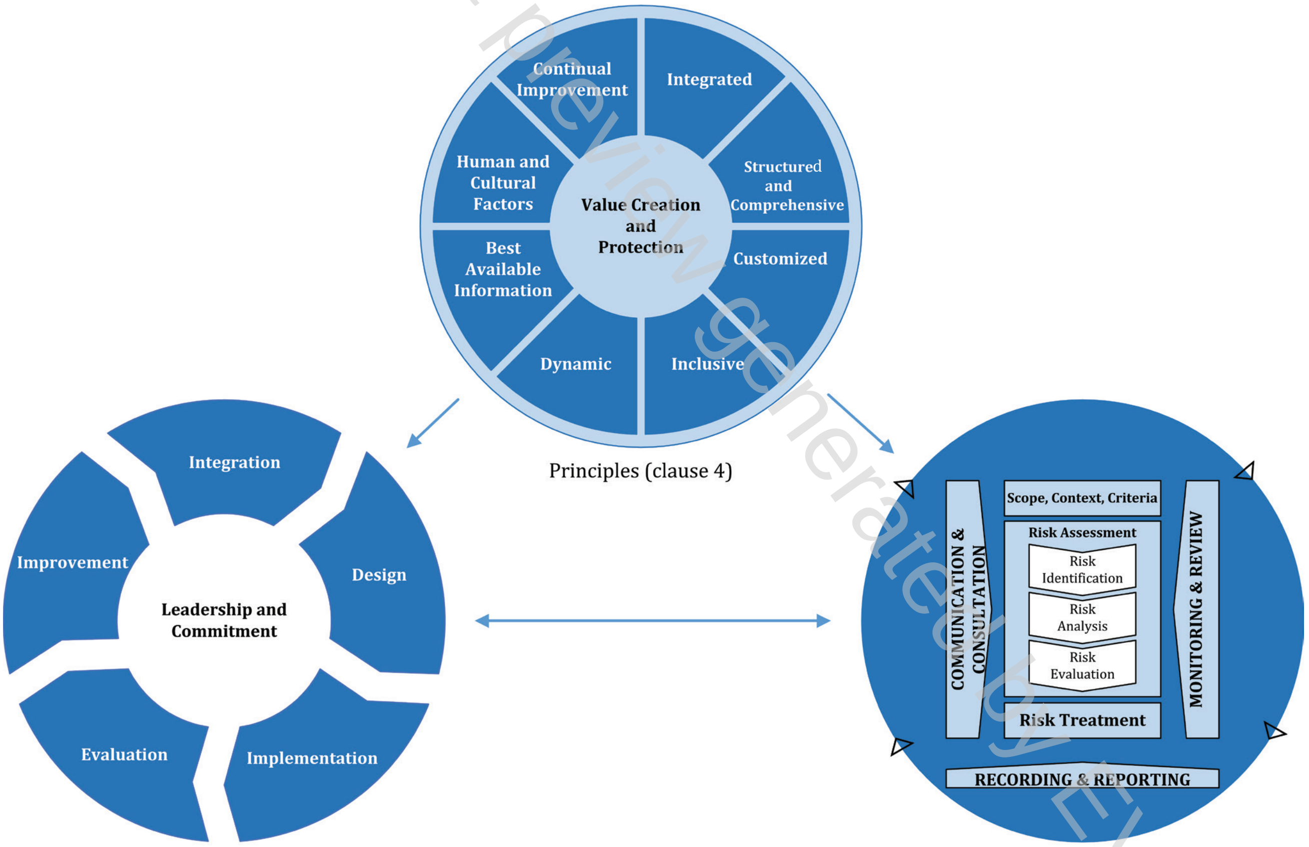
Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions.

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.



Principles (clause 4)

Framework (clause 5)

Process (clause 6)

Figure 1 — Principles, framework and process

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)