SLOVENSKI STANDARD
oSIST ISO/DIS 31000:2017

01-april-2017

Obvladovanje tveganja - Smernice

Risk management - Guidelines

Management du risque -- Lignes directrices

Ta slovenski standard je istoveten z: **ISO/DIS 31000**

ICS:

03.100.01	Organizacija in vodenje podjetja na splošno	Company organization and management in general

oSIST ISO/DIS 31000:2017 **en,fr**

DRAFT INTERNATIONAL STANDARD

ISO/DIS 31000

ISO/TC **262**

Secretariat: **BSI**

Voting begins on:
2017-02-17

Voting terminates on:
2017-05-11

Risk management — Guidelines

Management du risque — Lignes directrices

ICS: 03.100.01

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 31000:2017(E)

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

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.

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 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.

The committee responsible for this document is ISO/TC 262

This second edition cancels and replaces the first edition which been technically revised.

Introduction

Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives.

Managing risk is dynamic and assists organizations in making informed decisions about setting strategy and achieving objectives.

Managing risk is part of governance and leadership and how the organization is managed.

Managing risk includes interaction with stakeholders as an integral part of all activities of the organization.

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

Managing risk is based on the principles, framework and process outlined in this document. 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 consistent, efficient and effective. See Figure 1.

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.

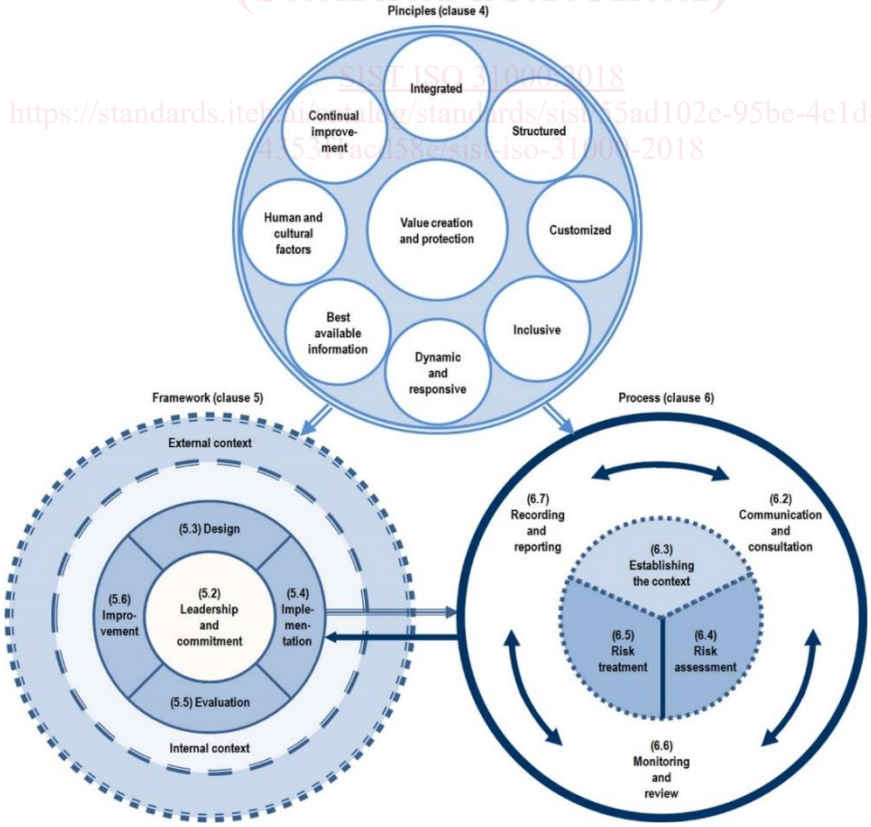

Figure 1 — Relationship between the principles, framework and process

Risk Management — Guidelines

1 Scope

This document provides adaptable guidelines on managing risk faced by organizations.

It can be used by any organization, provides a common approach to managing any type of risk and is not specific to any industry or sector.

This document can be used throughout the life of the organization and 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 terms and definitions given in ISO Guide 73 and the following 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 (sometimes expressed as opportunities), negative (sometimes expressed as threats) or both.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is often characterized by reference to potential events, their consequences and their likelihood."

[SOURCE: ISO Guide 73:2009, 1.1, modified — The original Notes 1, 2 and 3 to entry have been modified; the original Notes 4 and 5 to entry have been deleted.]

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

[SOURCE: ISO Guide 73:2009, 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: A decision maker can be a stakeholder.

[SOURCE: ISO Guide 73:2009, 3.2.1.1]

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

[SOURCE: ISO Guide 73:2009, 3.5.1.2, modified — The original Note to entry has been deleted.]

3.5
event
occurrence or change of a particular set of circumstances

Note 1 to entry: An event can be one or more occurrences, and can have several causes.

Note 2 to entry: An event can also be something that is expected, not happening.

[SOURCE: ISO Guide 73:2009, 3.5.1.3, modified — The original Note 2 entry has been modified; the original Notes 3 and 4 to entry have been deleted.]

3.6
consequence
outcome of an event (3.10) affecting objectives

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

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

Note 3 to entry: Initial consequences can escalate through cascading and cumulative effects.

[SOURCE: ISO Guide 73:2009, 3.6.1.3, modified — The original Note 1 to entry has been deleted.]

3.6
likelihood
chance of something happening

Note 1 to entry: In risk management 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).

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.

[SOURCE: ISO Guide 73:2009, 3.6.1.1]

3.7
control
measure that maintains or modifies risk

Note 1 to entry: Controls include any process, policy, device, practice, or other conditions and/or actions which maintain and modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO Guide 73:2009, 3.8.1.1, modified — The original definition and Note 1 to entry have been modified; Note 3 to entry has been added.]

4 Principles

These principles provide guidelines on the attributes of effective and efficient risk management, communicating its value and explaining its intention and purpose. These principles should enable an organization to manage the effects of uncertainty on its objectives. See Figure 2.

a) Value creation and protection

Risk management creates and protects value. It contributes to the achievement of objectives, encourages innovation and improves performance.

b) Integrated

Risk management is an integral part of all organizational activities, including decision making. It is not a stand-alone activity that is separate from the activities and processes of the organization. Everyone in an organization has responsibility for managing risk. Risk management improves decision making at all levels.

c) Structured

A systematic and structured approach to risk management contributes to efficiency and to consistent, comparable, and reliable results.

d) Customized

The risk management framework and processes should be customized to the organization's external and internal context and related to its objectives.

e) 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 and decision making.

f) Dynamic and responsive

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

g) Best available information

The inputs to risk management are based on historical and current information as well as future expectations, taking into account any limitations and uncertainties associated with the information.

h) Human and cultural factors

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

i) Continual improvement

Risk management improves organizational performance through increasing awareness and developing capabilities based on continuous learning and experience. These activities support organizational learning and resilience.

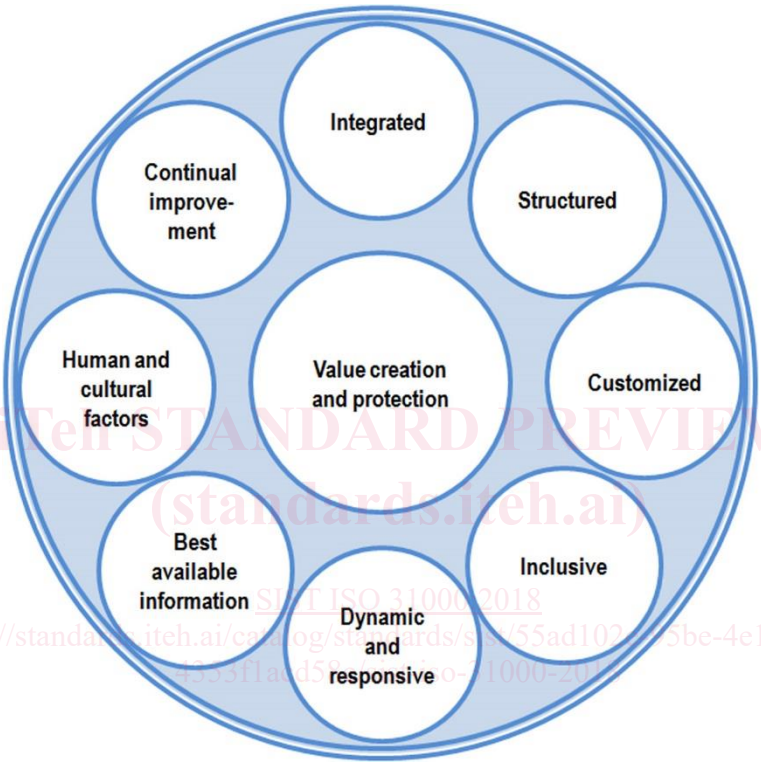

Figure 2— Principles