



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

<https://standards.iteh.ai/catalog/standards/sist/55ad102e-95be-4e1d-8991-4353f1acd58e/sist-iso-31000-2018>

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:
2017-02-17Voting terminates on:
2017-05-11

Risk management — Guidelines

Management du risque — Lignes directrices

ICS: 03.100.01

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST ISO 31000:2018

<https://standards.iteh.ai/catalog/standards/sist/55ad102e-95be-4e1d-8991-4353f1acd58e/sist-iso-31000-2018>

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.



Reference number
ISO/DIS 31000:2017(E)

© ISO 2017

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST ISO 31000:2018

<https://standards.iteh.ai/catalog/standards/sist/55ad102e-95be-4e1d-8991-4353f1acd58e/sist-iso-31000-2018>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
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

14	Contents	Page
15	Foreword	3
16	Introduction	3
17	1 Scope	5
18	2 Normative references	5
19	3 Terms and definitions	5
20	4 Principles	7
21	5 Framework	9
22	5.1. General.....	9
23	5.2. Leadership and commitment.....	10
24	5.2.1. General.....	10
25	5.2.2. Integrating risk management.....	10
26	5.3. Design	11
27	5.3.1. Understanding the organization and its context	11
28	5.3.2. Articulate risk management commitment(s).....	11
29	5.3.3. Assigning organizational roles, accountabilities, responsibilities and authorities	12
30	5.3.4. Allocating resources	12
31	5.3.5. Establishing communication and consultation	12
32	5.4. Implementation	13
33	5.5. Evaluation.....	13
34	5.6. Improvement	13
35	5.6.1. Adapting	13
36	5.6.2. Continually improving	13
37	6 Process	14
38	6.1. General.....	14
39	6.2. Communication and consultation.....	14
40	6.3. Establishing the context	15
41	6.3.1. General.....	15
42	6.3.2. Defining the purpose and scope of the process.....	15
43	6.3.3. Internal and external context.....	15
44	6.3.4. Defining risk criteria	16
45	6.4. Risk assessment.....	16
46	6.4.1. General.....	16
47	6.4.2. Risk identification.....	16
48	6.4.3. Risk analysis	17
49	6.4.4. Risk evaluation.....	18
50	6.5. Risk treatment.....	18
51	6.5.1. General.....	18
52	6.5.2. Selection of risk treatment options	19
53	6.5.3. Preparing and implementing risk treatment plans	19
54	6.6. Monitoring and review	20
55	6.7. Recording and reporting	20
56	Bibliography	21
57		

58 **Foreword**

59 ISO (the International Organization for Standardization) is a worldwide federation of national
60 standards bodies (ISO member bodies). The work of preparing International Standards is normally
61 carried out through ISO technical committees. Each member body interested in a subject for which a
62 technical committee has been established has the right to be represented on that committee.
63 International organizations, governmental and non-governmental, in liaison with ISO, also take part in
64 the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all
65 matters of electrotechnical standardization.

66 The procedures used to develop this document and those intended for its further maintenance are
67 described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the
68 different types of ISO documents should be noted. This document was drafted in accordance with the
69 editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

70 Attention is drawn to the possibility that some of the elements of this document may be the subject of
71 patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of
72 any patent rights identified during the development of the document will be in the Introduction and/or
73 on the ISO list of patent declarations received (see www.iso.org/patents).

74 Any trade name used in this document is information given for the convenience of users and does not
75 constitute an endorsement.

76 For an explanation on the meaning of ISO specific terms and expressions related to conformity
77 assessment, as well as information about ISO's adherence to the World Trade Organization (WTO)
78 principles in the Technical Barriers to Trade (TBT) see the following URL:
79 www.iso.org/iso/foreword.html.

80 The committee responsible for this document is ISO/TC 262

81 **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.

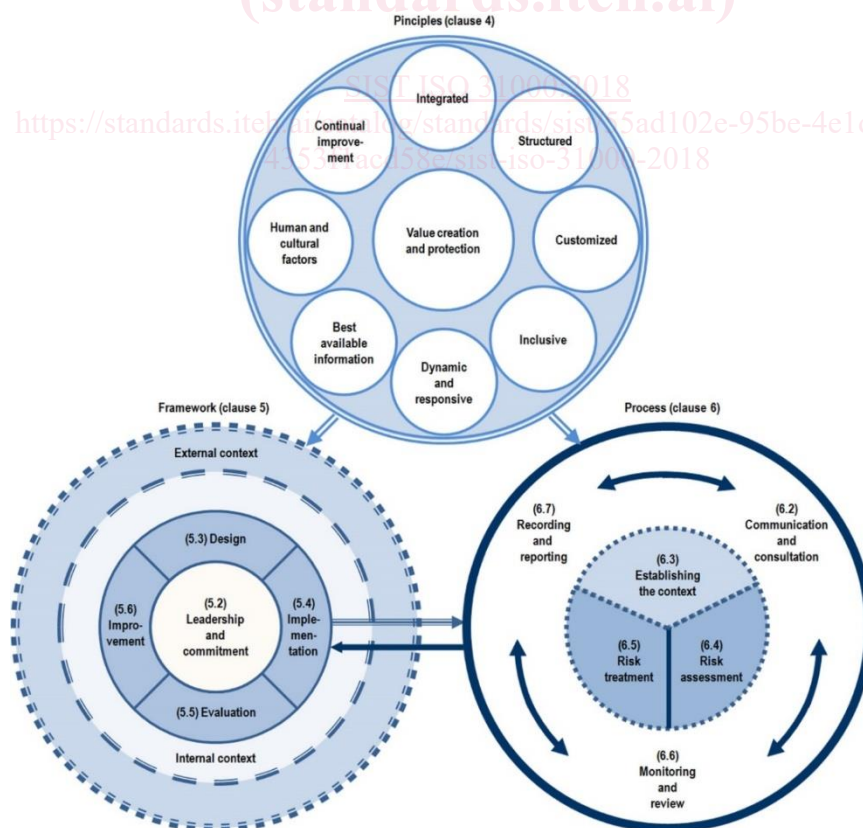


Figure 1 — Relationship between the principles, framework and process

99 Risk Management — Guidelines

100 1 Scope

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

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

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

106 2 Normative references

107 There are no normative references in this document.

108 3 Terms and definitions

109 For the purposes of this document, the terms and definitions given in ISO Guide 73 and the following
110 apply.

111 ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- 112 • ISO Online browsing platform: available at <http://www.iso.org/obp>
- 113 • IEC Electropedia: available at <http://www.electropedia.org>

114 3.1

115 risk

116 effect of uncertainty on objectives

117 Note 1 to entry: An effect is a deviation from the expected. It can be positive (sometimes expressed as
118 opportunities), negative (sometimes expressed as threats) or both.

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

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

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

124 3.2

125 risk management

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

127 [SOURCE: ISO Guide 73:2009, 3.1]

128 3.3

129 stakeholder

130 person or organization that can affect, be affected by, or perceive themselves to be affected by a
131 decision or activity

ISO/DIS 31000 :2017(E)

132 Note 1 to entry: A decision maker can be a stakeholder.

133 [SOURCE: ISO Guide 73:2009, 3.2.1.1]

134 3.4

135 risk source

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

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

138 3.5

139 event

140 occurrence or change of a particular set of circumstances

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

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

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

145 3.6

146 consequence

147 outcome of an event (3.10) affecting objectives

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

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

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

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

153 3.6

154 likelihood

155 chance of something happening

156 Note 1 to entry: In risk management terminology, the word “likelihood” is used to refer to the chance of
157 something happening, whether defined, measured or determined objectively or subjectively, qualitatively or
158 quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a
159 given time period).

160 Note 2 to entry: The English term “likelihood” does not have a direct equivalent in some languages; instead, the
161 equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted
162 as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it
163 should have the same broad interpretation as the term “probability” has in many languages other than English.

164 [SOURCE: ISO Guide 73:2009, 3.6.1.1]

165 3.7

166 control

167 measure that maintains or modifies risk

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

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

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

173 **4 Principles**

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

177 **a) Value creation and protection**

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

180 **b) Integrated**

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

185 **c) Structured**

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

188 **d) Customized**

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

191 **e) Inclusive**

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

195 **f) Dynamic and responsive**

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

199 **g) Best available information**

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

202 **h) Human and cultural factors**

ISO/DIS 31000:2017(E)

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.

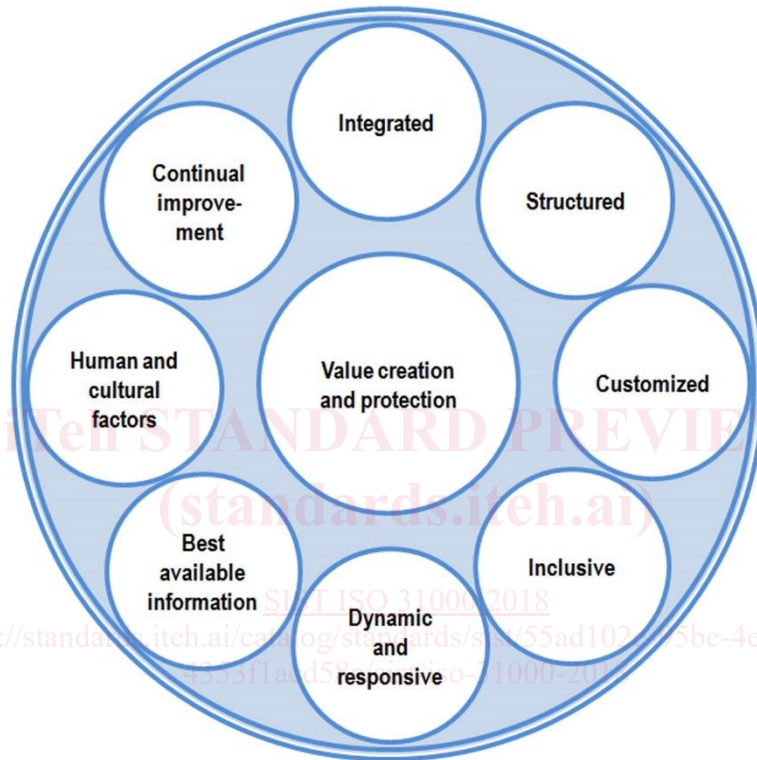


Figure 2— Principles