



SLOVENSKI STANDARD
SIST EN 31010:2010
01-september-2010

Upravljanje tveganja - Tehnike ocenjevanja tveganja (IEC/ISO 31010:2009)

Risk management - Risk assessment techniques (IEC/ISO 31010:2009)

Risikomanagement - Verfahren zur Risikobeurteilung (IEC/ISO 31010:2009)

Gestion des risques - Techniques d'évaluation des risques (CEI/ISO 31010:2009)

Ta slovenski standard je istoveten z: EN 31010:2010

[SIST EN 31010:2010](https://standards.iteh.ai/catalog/standards/sist/bcbf9ae7-901a-4e76-9900-1ffccd62cdd7/sist-en-31010-2010)

<https://standards.iteh.ai/catalog/standards/sist/bcbf9ae7-901a-4e76-9900-1ffccd62cdd7/sist-en-31010-2010>

ICS:

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

SIST EN 31010:2010

en

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 31010:2010

<https://standards.iteh.ai/catalog/standards/sist/bcbf9ae7-901a-4e76-9900-1ffcd62cdd7/sist-en-31010-2010>

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 31010

May 2010

ICS 03.100.01

English version

**Risk management -
Risk assessment techniques
(IEC/ISO 31010:2009)**

Gestion des risques -
Techniques d'évaluation des risques
(CEI/ISO 31010:2009)

Risikomanagement -
Verfahren zur Risikobeurteilung
(IEC/ISO 31010:2009)

This European Standard was approved by CENELEC on 2010-05-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 56/1329/FDIS, future edition 1 of IEC/ISO 31010, prepared by IEC TC 56, Dependability, together with the ISO TMB "Risk management" working group, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 31010 on 2010-05-01.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

- latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2011-02-01
- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2013-05-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC/ISO 31010:2009 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60300-3-11	NOTE Harmonized as EN 60300-3-11. https://standards.iteh.ai/catalog/standards/sist/bcbf9ae7-901a-4e76-9900-1ffc62cdd7/sist-en-31010-2010
IEC 61078	NOTE Harmonized as EN 61078.
IEC 61165	NOTE Harmonized as EN 61165.
IEC 61508 series	NOTE Harmonized in EN 61508 series (not modified)
IEC 61511 series	NOTE Harmonized in EN 61511 series (not modified)
IEC 61649	NOTE Harmonized as EN 61649.
ISO 22000	NOTE Harmonized as EN ISO 22000.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
ISO/IEC Guide 73	-	Risk management - Vocabulary - Guidelines for use in standards	-	-
ISO 31000	-	Risk management - Principles and guidelines	-	-

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN 31010:2010

<https://standards.iteh.ai/catalog/standards/sist/bcbf9ae7-901a-4e76-9900-1ffcd62cdd7/sist-en-31010-2010>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 31010:2010

<https://standards.iteh.ai/catalog/standards/sist/bcbf9ae7-901a-4e76-9900-1ffcd62cdd7/sist-en-31010-2010>



IEC/ISO 31010

Edition 1.0 2009-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Risk management – Risk assessment techniques

Gestion des risques – Techniques d'évaluation des risques

[SIST EN 31010:2010](https://standards.iteh.ai/catalog/standards/sist/bcbf9ae7-901a-4e76-9900-1ffcd62cdd7/sist-en-31010-2010)

<https://standards.iteh.ai/catalog/standards/sist/bcbf9ae7-901a-4e76-9900-1ffcd62cdd7/sist-en-31010-2010>

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XD

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references.....	7
3 Terms and definitions.....	7
4 Risk assessment concepts.....	7
4.1 Purpose and benefits.....	7
4.2 Risk assessment and the risk management framework.....	8
4.3 Risk assessment and the risk management process.....	8
4.3.1 General.....	8
4.3.2 Communication and consultation.....	9
4.3.3 Establishing the context.....	9
4.3.4 Risk assessment.....	10
4.3.5 Risk treatment.....	10
4.3.6 Monitoring and review.....	11
5 Risk assessment process.....	11
5.1 Overview.....	11
5.2 Risk identification.....	12
5.3 Risk analysis.....	12
5.3.1 General.....	12
5.3.2 Controls Assessment.....	13
5.3.3 Consequence analysis.....	14
5.3.4 Likelihood analysis and probability estimation.....	14
5.3.5 Preliminary Analysis.....	15
5.3.6 Uncertainties and sensitivities.....	15
5.4 Risk evaluation.....	15
5.5 Documentation.....	16
5.6 Monitoring and Reviewing Risk Assessment.....	17
5.7 Application of risk assessment during life cycle phases.....	17
6 Selection of risk assessment techniques.....	17
6.1 General.....	17
6.2 Selection of techniques.....	17
6.2.1 Availability of Resources.....	18
6.2.2 The Nature and Degree of Uncertainty.....	18
6.2.3 Complexity.....	19
6.3 Application of risk assessment during life cycle phases.....	19
6.4 Types of risk assessment techniques.....	19
Annex A (informative) Comparison of risk assessment techniques.....	21
Annex B (informative) Risk assessment techniques.....	27
Bibliography.....	90
Figure 1 – Contribution of risk assessment to the risk management process.....	11
Figure B.1 – Dose-response curve.....	37
Figure B.2 – Example of an FTA from IEC 60-300-3-9.....	49
Figure B.3 – Example of an Event tree.....	52

Figure B.4 – Example of Cause-consequence analysis	55
Figure B.5 – Example of Ishikawa or Fishbone diagram	57
Figure B.6 – Example of tree formulation of cause-and-effect analysis.....	58
Figure B.7 – Example of Human reliability assessment	64
Figure B.8 – Example Bow tie diagram for unwanted consequences	66
Figure B.9 – Example of System Markov diagram	70
Figure B.10 – Example of State transition diagram.....	71
Figure B.11 – Sample Bayes' net	77
Figure B.12 – The ALARP concept.....	79
Figure B.13 – Part example of a consequence criteria table.....	84
Figure B.14 – Part example of a risk ranking matrix	84
Figure B.15 – Part example of a probability criteria matrix	85
Table A.1 – Applicability of tools used for risk assessment	22
Table A.2 – Attributes of a selection of risk assessment tools	23
Table B.1 – Example of possible HAZOP guidewords	34
Table B.2 – Markov matrix	70
Table B.3 – Final Markov matrix.....	72
Table B.4 – Example of Monte Carlo Simulation	74
Table B.5 – Bayes' table data	77
Table B.6 – Prior probabilities for nodes A and B	77
Table B.7 – Conditional probabilities for node C with node A and node B defined	77
Table B.8 – Conditional probabilities for node D with node A and node C defined	78
Table B.9 – Posterior probability for nodes A and B with node D and Node C defined	78
Table B.10 – Posterior probability for node A with node D and node C defined	78

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**RISK MANAGEMENT –
RISK ASSESSMENT TECHNIQUES**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International standard IEC/ISO 31010 has been prepared by IEC technical committee 56: Dependability together with the ISO TMB “Risk management” working group.

The text of this standard is based on the following documents:

FDIS	Rapport de vote
56/1329/FDIS	56/1346/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table. In ISO, the standard has been approved by 17 member bodies out of 18 having cast a vote.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition;
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN 31010:2010

<https://standards.iteh.ai/catalog/standards/sist/bcbf9ae7-901a-4e76-9900-1ffc62cdd7/sist-en-31010-2010>

INTRODUCTION

Organizations of all types and sizes face a range of risks that may affect the achievement of their objectives.

These objectives may relate to a range of the organization's activities, from strategic initiatives to its operations, processes and projects, and be reflected in terms of societal, environmental, technological, safety and security outcomes, commercial, financial and economic measures, as well as social, cultural, political and reputation impacts.

All activities of an organization involve risks that should be managed. The risk management process aids decision making by taking account of uncertainty and the possibility of future events or circumstances (intended or unintended) and their effects on agreed objectives.

Risk management includes the application of logical and systematic methods for

- communicating and consulting throughout this process;
- establishing the context for identifying, analysing, evaluating, treating risk associated with any activity, process, function or product;
- monitoring and reviewing risks;
- reporting and recording the results appropriately.

Risk assessment is that part of risk management which provides a structured process that identifies how objectives may be affected, and analyses the risk in term of consequences and their probabilities before deciding on whether further treatment is required.

Risk assessment attempts to answer the following fundamental questions:

- what can happen and why (by risk identification)?
- what are the consequences?
- what is the probability of their future occurrence?
- are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?

Is the level of risk tolerable or acceptable and does it require further treatment? This standard is intended to reflect current good practices in selection and utilization of risk assessment techniques, and does not refer to new or evolving concepts which have not reached a satisfactory level of professional consensus.

This standard is general in nature, so that it may give guidance across many industries and types of system. There may be more specific standards in existence within these industries that establish preferred methodologies and levels of assessment for particular applications. If these standards are in harmony with this standard, the specific standards will generally be sufficient.

RISK MANAGEMENT – RISK ASSESSMENT TECHNIQUES

1 Scope

This International Standard is a supporting standard for ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment.

Risk assessment carried out in accordance with this standard contributes to other risk management activities.

The application of a range of techniques is introduced, with specific references to other international standards where the concept and application of techniques are described in greater detail.

This standard is not intended for certification, regulatory or contractual use.

This standard does not provide specific criteria for identifying the need for risk analysis, nor does it specify the type of risk analysis method that is required for a particular application.

This standard does not refer to all techniques, and omission of a technique from this standard does not mean it is not valid. The fact that a method is applicable to a particular circumstance does not mean that the method should necessarily be applied.

NOTE This standard does not deal specifically with safety. It is a generic risk management standard and any references to safety are purely of an informative nature. Guidance on the introduction of safety aspects into IEC standards is laid down in ISO/IEC Guide 51.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC Guide 73, *Risk management – Vocabulary – Guidelines for use in standards*

ISO 31000, *Risk management – Principles and guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions of ISO/IEC Guide 73 apply.

4 Risk assessment concepts

4.1 Purpose and benefits

The purpose of risk assessment is to provide evidence-based information and analysis to make informed decisions on how to treat particular risks and how to select between options.

Some of the principal benefits of performing risk assessment include:

- understanding the risk and its potential impact upon objectives;

- providing information for decision makers;
- contributing to the understanding of risks, in order to assist in selection of treatment options;
- identifying the important contributors to risks and weak links in systems and organizations;
- comparing of risks in alternative systems, technologies or approaches;
- communicating risks and uncertainties;
- assisting with establishing priorities;
- contributing towards incident prevention based upon post-incident investigation;
- selecting different forms of risk treatment;
- meeting regulatory requirements;
- providing information that will help evaluate whether the risk should be accepted when compared with pre-defined criteria;
- assessing risks for end-of-life disposal.

4.2 Risk assessment and the risk management framework

This standard assumes that the risk assessment is performed within the framework and process of risk management described in ISO 31000.

A risk management framework provides the policies, procedures and organizational arrangements that will embed risk management throughout the organization at all levels.

As part of this framework, the organization should have a policy or strategy for deciding when and how risks should be assessed.

In particular, those carrying out risk assessments should be clear about

- the context and objectives of the organization,
- the extent and type of risks that are tolerable, and how unacceptable risks are to be treated,
- how risk assessment integrates into organizational processes,
- methods and techniques to be used for risk assessment, and their contribution to the risk management process,
- accountability, responsibility and authority for performing risk assessment,
- resources available to carry out risk assessment,
- how the risk assessment will be reported and reviewed.

4.3 Risk assessment and the risk management process

4.3.1 General

Risk assessment comprises the core elements of the risk management process which are defined in ISO 31000 and contain the following elements:

- communication and consultation;
- establishing the context;
- risk assessment (comprising risk identification, risk analysis and risk evaluation);
- risk treatment;
- monitoring and review.

Risk assessment is not a stand-alone activity and should be fully integrated into the other components in the risk management process.

4.3.2 Communication and consultation

Successful risk assessment is dependent on effective communication and consultation with stakeholders.

Involving stakeholders in the risk management process will assist in

- developing a communication plan,
- defining the context appropriately,
- ensuring that the interests of stakeholders are understood and considered,
- bringing together different areas of expertise for identifying and analysing risk,
- ensuring that different views are appropriately considered in evaluating risks,
- ensuring that risks are adequately identified,
- securing endorsement and support for a treatment plan.

Stakeholders should contribute to the interfacing of the risk assessment process with other management disciplines, including change management, project and programme management, and also financial management.

4.3.3 Establishing the context

Establishing the context defines the basic parameters for managing risk and sets the scope and criteria for the rest of the process. Establishing the context includes considering internal and external parameters relevant to the organization as a whole, as well as the background to the particular risks being assessed.

In establishing the context, the risk assessment objectives, risk criteria, and risk assessment programme are determined and agreed.

For a specific risk assessment, establishing the context should include the definition of the external, internal and risk management context and classification of risk criteria:

- a) Establishing the external context involves familiarization with the environment in which the organization and the system operates including :
 - cultural, political, legal, regulatory, financial, economic and competitive environment factors, whether international, national, regional or local;
 - key drivers and trends having impact on the objectives of the organization; and
 - perceptions and values of external stakeholders.
- b) Establishing the internal context involves understanding
 - capabilities of the organization in terms of resources and knowledge,
 - information flows and decision-making processes,
 - internal stakeholders,
 - objectives and the strategies that are in place to achieve them,
 - perceptions, values and culture,
 - policies and processes,
 - standards and reference models adopted by the organization, and
 - structures (e.g. governance, roles and accountabilities).
- c) Establishing the context of the risk management process includes
 - defining accountabilities and responsibilities,
 - defining the extent of the risk management activities to be carried out, including specific inclusions and exclusions,