

RISKIJUHTIMINE. RISIKIHINDAMISMEETODID

Risk management - Risk assessment techniques

This document is a preview generated by EVS

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

See Eesti standard EVS-EN IEC 31010:2019 sisaldab Euroopa standardi EN IEC 31010:2019 ingliskeelset teksti.	This Estonian standard EVS-EN IEC 31010:2019 consists of the English text of the European standard EN IEC 31010:2019.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 16.08.2019.	Date of Availability of the European standard is 16.08.2019.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

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

ICS 03.100.01

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:  
Koduleht [www.evs.ee](http://www.evs.ee); telefon 605 5050; e-post [info@evs.ee](mailto:info@evs.ee)

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Homepage [www.evs.ee](http://www.evs.ee); phone +372 605 5050; e-mail [info@evs.ee](mailto:info@evs.ee)

EUROPEAN STANDARD

**EN IEC 31010**

NORME EUROPÉENNE

EUROPÄISCHE NORM

August 2019

ICS 03.100.01

Supersedes EN 31010:2010 and all of its amendments  
and corrigenda (if any)

English Version

## Risk management - Risk assessment techniques (IEC 31010:2019)

Management du risque - Techniques d'appréciation du  
risque  
(IEC 31010:2019)

Risikomanagement - Verfahren zur Risikobeurteilung  
(IEC 31010:2019)

This European Standard was approved by CENELEC on 2019-07-18. 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 CEN-CENELEC Management Centre 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 CEN-CENELEC Management Centre 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, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



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

**CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels**

## European foreword

The text of document 56/1837/FDIS, future edition 2 of IEC 31010, prepared by IEC/TC 56 "Dependability" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 31010:2019.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2020-04-18
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2022-07-18

This document supersedes EN 31010:2010.

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

## Endorsement notice

The text of the International Standard IEC 31010:2019 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 62740	NOTE	Harmonized as EN 62740
IEC 60812	NOTE	Harmonized as EN IEC 60812
IEC 61882	NOTE	Harmonized as EN 61882
ISO 22000	NOTE	Harmonized as EN ISO 22000
IEC 61508 (series)	NOTE	Harmonized as EN 61508 (series)
IEC 61511 (series)	NOTE	Harmonized as EN 61511 (series)
ISO 22301	NOTE	Harmonized as EN ISO 22301
IEC 62502	NOTE	Harmonized as EN 62502
IEC 62508	NOTE	Harmonized as EN 62508
IEC 61165	NOTE	Harmonized as EN 61165
IEC 60300-3-11	NOTE	Harmonized as EN 60300-3-11

## Annex ZA (normative)

### Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: [www.cenelec.eu](http://www.cenelec.eu).

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
ISO 31000	2018	Risk management_ - Guidelines	-	-
ISO Guide 73	2009	Risk management_ - Vocabulary	-	-

## CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	9
2 Normative references .....	9
3 Terms and definitions .....	9
4 Core concepts .....	10
4.1 Uncertainty .....	10
4.2 Risk .....	11
5 Uses of risk assessment techniques .....	11
6 Implementing risk assessment.....	12
6.1 Plan the assessment.....	12
6.1.1 Define purpose and scope of the assessment .....	12
6.1.2 Understand the context.....	13
6.1.3 Engage with stakeholders.....	13
6.1.4 Define objectives .....	13
6.1.5 Consider human, organizational and social factors .....	13
6.1.6 Review criteria for decisions .....	14
6.2 Manage information and develop models .....	16
6.2.1 General .....	16
6.2.2 Collecting information .....	16
6.2.3 Analysing data.....	16
6.2.4 Developing and applying models .....	17
6.3 Apply risk assessment techniques.....	18
6.3.1 Overview .....	18
6.3.2 Identifying risk .....	19
6.3.3 Determining sources, causes and drivers of risk .....	19
6.3.4 Investigating the effectiveness of existing controls.....	20
6.3.5 Understanding consequences, and likelihood .....	20
6.3.6 Analysing interactions and dependencies .....	22
6.3.7 Understanding measures of risk.....	22
6.4 Review the analysis .....	25
6.4.1 Verifying and validating results .....	25
6.4.2 Uncertainty and sensitivity analysis .....	25
6.4.3 Monitoring and review.....	26
6.5 Apply results to support decisions.....	26
6.5.1 Overview .....	26
6.5.2 Decisions about the significance of risk .....	27
6.5.3 Decisions that involve selecting between options.....	27
6.6 Record and report risk assessment process and outcomes .....	28
7 Selecting risk assessment techniques.....	28
7.1 General.....	28
7.2 Selecting techniques.....	29
Annex A (informative) Categorization of techniques .....	31
A.1 Introduction to categorization of techniques .....	31
A.2 Application of categorization of techniques .....	31
A.3 Use of techniques during the ISO 31000 process.....	37

Annex B (informative) Description of techniques .....	40
B.1 Techniques for eliciting views from stakeholders and experts.....	40
B.1.1 General .....	40
B.1.2 Brainstorming .....	40
B.1.3 Delphi technique.....	42
B.1.4 Nominal group technique .....	43
B.1.5 Structured or semi-structured interviews .....	44
B.1.6 Surveys .....	45
B.2 Techniques for identifying risk.....	46
B.2.1 General .....	46
B.2.2 Checklists, classifications and taxonomies.....	47
B.2.3 Failure modes and effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA) .....	49
B.2.4 Hazard and operability (HAZOP) studies.....	50
B.2.5 Scenario analysis .....	52
B.2.6 Structured what if technique (SWIFT) .....	54
B.3 Techniques for determining sources, causes and drivers of risk .....	55
B.3.1 General .....	55
B.3.2 Cindynic approach .....	56
B.3.3 Ishikawa analysis (fishbone) method .....	58
B.4 Techniques for analysing controls .....	60
B.4.1 General .....	60
B.4.2 Bow tie analysis.....	60
B.4.3 Hazard analysis and critical control points (HACCP).....	62
B.4.4 Layers of protection analysis (LOPA).....	64
B.5 Techniques for understanding consequences and likelihood .....	66
B.5.1 General .....	66
B.5.2 Bayesian analysis.....	66
B.5.3 Bayesian networks and influence diagrams.....	68
B.5.4 Business impact analysis (BIA).....	70
B.5.5 Cause-consequence analysis (CCA).....	72
B.5.6 Event tree analysis (ETA).....	74
B.5.7 Fault tree analysis (FTA) .....	76
B.5.8 Human reliability analysis (HRA).....	78
B.5.9 Markov analysis.....	79
B.5.10 Monte Carlo simulation .....	81
B.5.11 Privacy impact analysis (PIA) / data protection impact analysis (DPIA) .....	83
B.6 Techniques for analysing dependencies and interactions .....	85
B.6.1 Causal mapping.....	85
B.6.2 Cross impact analysis.....	87
B.7 Techniques that provide a measure of risk .....	89
B.7.1 Toxicological risk assessment.....	89
B.7.2 Value at risk (VaR) .....	91
B.7.3 Conditional value at risk (CVaR) or expected shortfall (ES) .....	93
B.8 Techniques for evaluating the significance of risk .....	94
B.8.1 General .....	94
B.8.2 As low as reasonably practicable (ALARP) and so far as is reasonably practicable (SFAIRP).....	94

B.8.3	Frequency-number (F-N) diagrams .....	96
B.8.4	Pareto charts .....	98
B.8.5	Reliability centred maintenance (RCM) .....	100
B.8.6	Risk indices .....	102
B.9	Techniques for selecting between options .....	103
B.9.1	General .....	103
B.9.2	Cost/benefit analysis (CBA) .....	104
B.9.3	Decision tree analysis .....	106
B.9.4	Game theory .....	107
B.9.5	Multi-criteria analysis (MCA) .....	109
B.10	Techniques for recording and reporting .....	111
B.10.1	General .....	111
B.10.2	Risk registers .....	112
B.10.3	Consequence/likelihood matrix (risk matrix or heat map) .....	113
B.10.4	S-curves .....	117
Bibliography	.....	119
Figure A.1	– Application of techniques in the ISO 31000 risk management process [3] .....	37
Figure B.1	– Example Ishikawa (fishbone) diagram .....	59
Figure B.2	– Example of Bowtie .....	61
Figure B.3	– A Bayesian network showing a simplified version of a real ecological problem: modelling native fish populations in Victoria, Australia .....	69
Figure B.4	– Example of cause-consequence diagram .....	73
Figure B.5	– Example of event tree analysis .....	75
Figure B.6	– Example of fault tree .....	77
Figure B.7	– Example of Markov diagram .....	80
Figure B.8	– Example of dose response curve .....	89
Figure B.9	– Distribution of value .....	91
Figure B.10	– Detail of loss region VaR values .....	91
Figure B.11	– VaR and CVaR for possible loss portfolio .....	93
Figure B.12	– ALARP diagram .....	95
Figure B.13	– Sample F-N diagram .....	97
Figure B.14	– Example of a Pareto chart .....	98
Figure B.15	– Part example of table defining consequence scales .....	114
Figure B.16	– Part example of a likelihood scale .....	114
Figure B.17	– Example of consequence/likelihood matrix .....	115
Figure B.18	– Probability distribution function and cumulative distribution function .....	117
Table A.1	– Characteristics of techniques .....	31
Table A.2	– Techniques and indicative characteristics .....	32
Table A.3	– Applicability of techniques to the ISO 31000 process .....	38
Table B.1	– Examples of basic guidewords and their generic meanings .....	51



Table B.2 – Table of deficits for each stakeholder .....	57
Table B.3 – Table of dissonances between stakeholders .....	57
Table B.4 – Example of Markov matrix .....	80
Table B.5 – Examples of systems to which Markov analysis can be applied .....	81
Table B.6 – An example of RCM task selection .....	101
Table B.7 – Example of a game matrix .....	108

This document is a preview generated by EVS

## 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 31010 has been prepared by IEC technical committee 56: Dependability, in co-operation with ISO technical committee 262: Risk management.

It is published as a double logo standard.

This second edition cancels and replaces the first edition published in 2009. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- more detail is given on the process of planning, implementing, verifying and validating the use of the techniques;
- the number and range of application of the techniques has been increased;
- the concepts covered in ISO 31000 are no longer repeated in this standard.

The text of this International Standard is based on the following documents of IEC:

FDIS	Report on voting
56/1837/FDIS	56/1845/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table. In ISO, the standard has been approved by 44 P members out of 46 having cast a vote.

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

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

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- 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.**

## INTRODUCTION

This document provides guidance on the selection and application of various techniques that can be used to help improve the way uncertainty is taken into account and to help understand risk.

The techniques are used:

- where further understanding is required about what risk exists or about a particular risk;
- within a decision where a range of options each involving risk need to be compared or optimized;
- within a risk management process leading to actions to treat risk.

The techniques are used within the risk assessment steps of identifying, analysing and evaluating risk as described in ISO 31000, and more generally whenever there is a need to understand uncertainty and its effects.

The techniques described in this document can be used in a wide range of settings, however the majority originated in the technical domain. Some techniques are similar in concept but have different names and methodologies that reflect the history of their development in different sectors. Techniques have evolved over time and continue to evolve, and many can be used in a broad range of situations outside their original application. Techniques can be adapted, combined and applied in new ways or extended to satisfy current and future needs.

This document is an introduction to selected techniques and compares their possible applications, benefits and limitations. It also provides references to sources of more detailed information.

The potential audience for this document is:

- anyone involved in assessing or managing risk;
- people who are involved in developing guidance that sets out how risk is to be assessed in specific contexts;
- people who need to make decisions where there is uncertainty including:
  - those who commission or evaluate risk assessments,
  - those who need to understand the outcomes of assessments, and
  - those who have to choose assessment techniques to meet particular needs.

Organizations that are required to conduct risk assessments for compliance or conformance purposes would benefit from using appropriate formal and standardized risk assessment techniques.