IEC 31010

Edition 2.0 2019-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Risk management – Risk assessment techniques

Management du risque – Techniques d'appréciation du risque



IEC 31010:2019-06(en-fr)



THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2019 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

IEC 31010

Edition 2.0 2019-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Risk management – Risk assessment techniques

Management du risque – Techniques d'appréciation du risque

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.100.01

ISBN 978-2-8322-6989-3

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

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

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.

RISK MANAGEMENT – RISK ASSESSMENT TECHNIQUES

1 Scope

This International Standard provides guidance on the selection and application of techniques for assessing risk in a wide range of situations. The techniques are used to assist in making decisions where there is uncertainty, to provide information about particular risks and as part of a process for managing risk. The document provides summaries of a range of techniques, with references to other documents where the techniques are described in more detail.

2 Normative references

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.

ISO Guide 73:2009, *Risk management – Vocabulary*

ISO 31000:2018, *Risk management – Guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 31000:2018, ISO Guide 73:2009 and the following apply.

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

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
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 31000:2018, 3.7]

3.2
opportunity
combination of circumstances expected to be favourable to objectives

Note 1 to entry: An opportunity is a positive situation in which gain is likely and over which one has a fair level of control.

Note 2 to entry: An opportunity to one party may pose a threat to another.

Note 3 to entry: Taking or not taking an opportunity are both sources of risk.

3.3
probability
measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty

Note 1 to entry: See definition 3.1, Note 2 to entry.

3.4
risk driver
driver of risk
factor that has a major influence on risk

3.5
threat
potential source of danger, harm, or other undesirable outcome

Note 1 to entry: A threat is a negative situation in which loss is likely and over which one has relatively little control.

Note 2 to entry: A threat to one party may pose an opportunity to another.

4 Core concepts

4.1 Uncertainty

Uncertainty is a term which embraces many underlying concepts. Many attempts have been made, and continue to be developed, to categorize types of uncertainty including:

- uncertainty which recognizes the intrinsic variability of some phenomena, and that cannot be reduced by further research; for example, throwing dice (sometimes referred to as aleatory uncertainty);
- uncertainty which generally results from a lack of knowledge and that therefore can be reduced by gathering more data, by refining models, improving sampling techniques, etc. (sometimes referred to as epistemic uncertainty).

Other commonly recognized forms of uncertainty include:

- linguistic uncertainty, which recognizes the vagueness and ambiguity inherent in spoken languages;
- decision uncertainty, which has particular relevance to risk management strategies, and which identifies uncertainty associated with value systems, professional judgement, company values and societal norms.

Examples of uncertainty include:

- uncertainty as to the truth of assumptions, including presumptions about how people or systems might behave;
- variability in the parameters on which a decision is to be based;
- uncertainty in the validity or accuracy of models which have been established to make predictions about the future;
- events (including changes in circumstances or conditions) whose occurrence, character or consequences are uncertain;
- uncertainty associated with disruptive events;
- the uncertain outcomes of systemic issues, such as shortages of competent staff, that can have wide ranging impacts which cannot be clearly defined;