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)

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 It also gives information on projects, replaced and withdrawn publications.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

CONTENTS

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;

- lack of knowledge which arises when uncertainty is recognized but not fully understood;
- unpredictability;
- uncertainty arising from the limitations of the human mind, for example in understanding complex data, predicting situations with long-term consequences or making bias-free judgments.

Not all uncertainty is able to be understood and the significance of uncertainty might be hard or impossible to define or influence. However, a recognition that uncertainty exists in a specific context enables early warning systems to be put in place to detect change in a proactive and timely manner and make arrangements to build resilience to cope with unexpected circumstances.

4.2 Risk

Risk includes the effects of any of the forms of uncertainty described in 4.1 on objectives. The uncertainty may lead to positive or negative consequences or both.

Risk is often described in terms of risk sources, potential events, their consequences and their likelihoods. An event can have multiple causes and lead to multiple consequences. Consequences can have a number of discrete values, be continuous variables or be unknown. Consequences may not be discernible or measurable at first, but may accumulate over time. Sources of risk can include inherent variability, or uncertainties related to a range of factors including human behaviour and organizational structures or societal influences for which it can be difficult to predict any particular event that might occur. It follows that risk cannot always be tabulated easily as a set of events, their consequences and their likelihoods.

Risk assessment techniques aim to help people understand uncertainty and the associated risk in this broad, complex and diverse context, for the purpose of supporting better-informed decisions and actions.

5 Uses of risk assessment techniques

The techniques described in this document provide a means to improve understanding of uncertainty and its implications for decisions and actions.

ISO 31000 describes principles for managing risk and the foundations and organizational arrangements that enable risk to be managed. It specifies a process that enables risk to be recognized, understood and modified as necessary, according to criteria that are established as part of the process. Risk assessment techniques can be applied within this structured approach which involves establishing context, assessing risk and treating risk, along with ongoing monitoring, review, communication and consultation, recording and reporting. This process is illustrated in Figure A.1 which also shows examples of where within the process techniques can be applied.

In the ISO 31000 process, risk assessment involves identifying risks, analysing them, and using the understanding gained from the analysis to evaluate risk by drawing conclusions about their comparative significance in relation to the objectives and performance thresholds of the organization. This process provides inputs into decisions about whether treatment is required, priorities for treatment and the actions intended to treat risk. In practice an iterative approach is applied.

Risk assessment techniques described in this document are used

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

In particular, the techniques can be used to:

- provide structured information to support decisions and actions where there is uncertainty;
- clarify the implications of assumptions on the achievement of objectives;
- compare multiple options, systems, technologies or approaches, etc. where there is multifaceted uncertainty around each option;
- assist in defining realistic strategic and operational objectives;
- help determine an organization's risk criteria, such as risk limits, risk appetite or risk bearing capacity;
- take risk into account when setting or reviewing priorities;
- recognize and understand risk, including risk that could have extreme outcomes;
- understand which uncertainties matter most to an organization's objectives and provide a rationale for what should be done about them;
- recognize and exploit opportunities more successfully;
- articulate the factors that contribute to risk and why they are important;
- identify effective and efficient risk treatment actions;
- determine the modifying effect of proposed risk treatments, including any change in the nature or magnitude of risk;
- communicate about risk and its implications;
- learn from failure and successes in order to improve the way risk is managed;
- demonstrate that regulatory and other requirements have been satisfied.

The way in which risk is assessed depends on the situation's complexity and novelty, and the level of relevant knowledge and understanding.

- In the simplest case, when there is nothing new or unusual about a situation, risk is well understood, with no major stakeholder implications or consequences are not significant, then actions are likely to be decided according to established rules and procedures and previous assessments of risk.
- For very novel, complex or challenging issues, where there is high uncertainty and little experience, there is little information on which to base assessment and conventional techniques of analysis might not be useful or meaningful. This also applies to circumstances where stakeholders hold strongly divergent views. In these cases, multiple techniques might be used to gain a partial understanding of risk, with judgements then made in the context of organizational and societal values, and stakeholder views.

The techniques described in this document have greatest application in situations between these two extremes where the complexity is moderate and there is some information available on which to base the assessment.

6 Implementing risk assessment

6.1 Plan the assessment

6.1.1 Define purpose and scope of the assessment

The purpose of the assessment should be established, including identifying the decisions or actions to which it relates, the decision makers, stakeholders, and the timing and nature of the output required (for example whether qualitative, semi-quantitative or quantitative information is required).

The scope, depth and level of detail of the assessment should be defined, with a description of what is included, and excluded. The types of consequence to be included in the assessment should be defined. Any conditions, assumptions, constraints or necessary resources relevant to the assessment activity should also be specified.

6.1.2 Understand the context

When undertaking a risk assessment those involved should be aware of the broader circumstances in which decisions and actions based on their assessment will be made. This includes understanding the internal and external issues that contribute to the context of the organization as well as wider societal and environmental aspects. Any relevant context statement should be reviewed and checked to see that it is current and appropriate. Understanding the bigger picture is particularly important where there is significant complexity.

6.1.3 Engage with stakeholders

Stakeholders and those who are likely to be able to contribute useful knowledge or relevant views should be identified and their perspectives considered, whether or not they are included as participants in the assessment. Appropriate involvement of stakeholders helps ensure that the information on which risk assessment is based is valid and applicable and that stakeholders understand the reasons behind decisions. Involvement of stakeholders can:

- provide information that enables the context of the assessment to be understood;
- bring together different areas of knowledge and expertise for more effectively identifying and understanding risk;
- provide relevant expertise for use of the techniques;
- enable stakeholder interests to be understood and considered;
- provide input to the process of determining whether risk is acceptable particularly when the stakeholders are impacted;
- fulfil any requirements for people to be informed or consulted;
- obtain support for the outputs and decisions arising from risk assessment;
- identify gaps in knowledge that need to be addressed prior to and/or during risk assessment.

It should be decided how outputs and outcomes of risk assessment are to be reliably, accurately and transparently communicated to relevant stakeholders.

Techniques for eliciting views from stakeholders and experts are described in Clause B.1.

6.1.4 Define objectives

The objectives of the specific system or process for which risk is to be assessed should be defined and where practicable documented. This will facilitate identification of risk and understanding its implications.

To the extent practicable the objectives should be:

- specific to the subject of the assessment;
- measurable either qualitatively or quantitatively;
- achievable within the constraints imposed by the context;
- relevant to the larger goals or context of the organization;
- achievable within a stated time frame.

6.1.5 Consider human, organizational and social factors

Human, organizational and social factors should be considered explicitly and taken into account as appropriate. Human aspects are relevant to risk assessment in the following ways: