BS EN IEC 31010:2019

BSI Standards Publication

Risk management – Risk assessment techniques (IEC 31010:2019)

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

National foreword

This British Standard is the UK implementation of EN IEC 31010:2019. It is identical to IEC 31010:2019. It supersedes BS EN 31010:2010, which will be withdrawn on 18 July 2022.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2019
Published by BSI Standards Limited 2019

ISBN 978 0 580 95443 6

ICS 03.100.01

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2019.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 31010

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

© 2019 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 31010:2019 E

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 31010:2019

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

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

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.

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 31010:2019

This page deliberately left blank

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

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 31

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 31010:2019

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 31010:2019

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

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

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.

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

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.

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

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.

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

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.

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

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;

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

- 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.

AVA Documents
Document Sharing Hub

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).

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

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:

AVA Documents
Document Sharing Hub

- as a source of uncertainty;
- through influences on the way in which techniques are selected and applied;
- in the ways that information is interpreted and used (for example because of differing perceptions of risk).

Human performance (whether above or below expectation) is a source of risk and can also affect the effectiveness of controls. The potential for deviation from expected or assumed behaviours should be specifically considered when assessing risk. Human performance considerations are frequently complex and expert advice can be required to identify and analyse human aspects of risk.

Human factors also influence the selection and use of techniques, particularly where judgements have to be made or team approaches are used. Skilled facilitation is needed to minimize these influences. Biases such as groupthink and over-confidence (for example in estimates or perceptions) should be addressed. Expert opinion should be informed by evidence and data wherever possible and efforts made to avoid or minimize cognitive biases.

People's personal objectives and values can vary and differ from those of the organization. This can result in different perceptions about the level of a risk and different criteria by which individuals make decisions. An organization should endeavour to achieve a common understanding of risk internally and take account of the differing perceptions of stakeholders.

Social aspects, including socioeconomic position, race ethnicity and culture, gender, social relationships and residential and community context can affect risk both directly and indirectly. Impacts may be long term and not immediately visible and can require a long-term planning perspective.

6.1.6 Review criteria for decisions

6.1.6.1 General

Criteria, including risk criteria, which need to be taken into account when making decisions, should be reviewed prior to undertaking the assessment. Criteria can be qualitative, semi-quantitative or quantitative. In some cases there might be no explicit criteria specified and stakeholders use their judgement to respond to the results of analysis.

Relevant criteria to review are:

- how it will be decided whether risk is acceptable;
- how the relative significance of risks will be determined;
- how risk will be taken into account in decisions on options, where each option is associated with multiple risks that might have positive or negative consequences, or both;
- how the relationships between risks will be taken into account.

6.1.6.2 Criteria for deciding whether risk can be accepted

Criteria for defining the nature and extent of risk that can be accepted in pursuit of objectives, sometimes referred to as risk appetite, can be defined by specifying a technique to determine the magnitude of risk, or a parameter related to risk, together with a limit beyond which risk becomes unacceptable. The limit set for unacceptable adverse risk can depend on potential rewards.

The acceptability of risk can also be defined by specifying the acceptable variation in specific performance measures linked to objectives.

Different criteria might be specified according to the type of consequence. For example, an organization's criteria for accepting financial risk may differ from those defined for risk to human life.

AVA Documents
Document Sharing Hub

The following are examples of considerations used when defining whether risk can be accepted.

- Risk bearing capacity (RBC) (also called risk capacity): An organization's RBC is usually defined in terms of risk capital, which is available for absorbing adverse effects from risks. For a commercial firm capacity might be specified in terms of maximum retention capacity covered by assets, or the largest financial loss the company could bear without having to declare bankruptcy. The estimated RBC should be reasonably tested by stress testing scenarios to provide a reliable confidence level. An organization's risk appetite reflects management's willingness to utilize its RBC.
- ALARP/ALARA and SFAIRP: In some jurisdictions legislated criteria for decisions about treating safety related risk involve ensuring the risk of injury or ill health is "as low as is reasonably practicable" (ALARP), "as low as reasonably achievable" (ALARA) or demonstrating that controls minimize risk "so far as is reasonably practicable" (SFAIRP) (see B.8.2).
- "Globally at least equivalent" (GALE) [*globalement au moins équivalent (GAME)* [1]]: it is considered acceptable for risks with adverse consequences from a particular source to increase if it can be demonstrated that risks from other sources have decreased by an equivalent or greater amount.
- Cost/benefit criteria such as price per life saved or return on investment (ROI).

6.1.6.3 Criteria for evaluating the significance of risk

Risk criteria (the terms of reference against which the significance of risk is determined) can be expressed in terms that involve any of the characteristics and measures of risk elaborated in 6.3.5 and 6.3.7. Ethical, cultural, legal, social, reputational, environmental, contractual, financial and other considerations can also be relevant.

An evaluation of the significance of a risk compared to other risks is often based on an estimate of the magnitude of risk compared with criteria which are directly related to thresholds set around the objectives of the organization. Comparison with these criteria can inform an organization which risks should be focused on for treatment, based on their potential to drive outcomes outside of thresholds set around objectives.

The magnitude of risk is seldom the only criterion relevant to decisions about the significance of risk. Other relevant factors can include sustainability (e.g. triple bottom line) and resilience, ethical and legal criteria, the effectiveness of controls, the maximum impact if controls are not present or fail, the timing of the consequences, the costs of controls and stakeholder views.

Techniques for evaluating the significance of risk are described in Clause B.8

6.1.6.4 Criteria for deciding between options

An organization will be faced with many decisions where several, often competing, objectives are potentially affected, and there are both potential adverse outcomes and potential benefits to consider. For such decisions several criteria might need to be met and trade-offs between competing objectives might be required. Criteria relevant to the decision should be identified and the way in which criteria are to be weighted or trade-offs otherwise made should be decided and accounted for and the information recorded and shared. In setting criteria, the possibility that costs and benefits may differ for different stakeholders should be considered. The way in which different forms of uncertainty are to be taken into account should be decided.

Techniques in Clause B.9 address selecting between options.

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

6.2 Manage information and develop models

6.2.1 General

Prior to and during a risk assessment, relevant information should be obtained. This information provides an input to statistical analysis, models or to the techniques described in Annexes A and B. In some cases, the information can be used by decision makers without further analysis.

The information needed at each point depends on the results of earlier information gathering, the purpose and scope of the assessment, and the method or methods to be used for analysis. The way information is to be collected, stored, and made available should be decided.

The records of the outputs of the assessment that are to be kept should be decided, along with how those records are to be made, stored, updated and provided to those who might need them. Sources of information should always be indicated.

6.2.2 Collecting information

Information can be gathered from sources such as literature reviews, observations, and expert opinion. Data can be collected or derived, for example, from measurements, experiments, interviews and surveys.

Typically, data directly or indirectly represent past losses or benefits. Examples include project failures or successes, the number of complaints, financial gains or losses, health impacts, injuries and fatalities, etc. Additional information might also be available such as the causes of failures or successes, sources of complaints, the nature of injuries, etc. Data can also include the output from models or other analysis techniques.

The following should be decided:

- the source of information and its reliability;
- type (e.g. whether it is qualitative, quantitative or both (see 6.3.7.1));
- level (e.g. strategic, tactical, operational);
- quantity and quality of the data needed;
- collection methodology;
- level of confidentiality.

When the data to be analysed are obtained from sampling, the statistical confidence that is required should be stated so that sufficient data is collected. Where no statistical analysis is needed this should be stated.

If the data or results from previous assessments are available, it should first be established whether there has been any change in context and, if so, whether the earlier data or results remain relevant.

The validity, reliability and limitations of any information to be used in the assessment should be assessed, taking into account:

- the age and relevance of information;
- the source of information, and the methods used to collect it;
- uncertainties and gaps in the information;
- the authority or provenance of information, data sets, algorithms and models.

6.2.3 Analysing data

Analysis of data can provide:

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

- an understanding of past consequences and their likelihood in order to learn from experience;
- trends and patterns, including periodicities, that provide an indication of what might influence the future;
- correlations that can give indications of possible causal relationships for further validation.

Limitations and uncertainties in data should be identified and understood.

Past data cannot be assumed to continue to apply into the future, but they can give an indication to decision makers of what is more or less likely to occur in the future.

6.2.4 Developing and applying models

6.2.4.1 General

A model is an approximate representation of reality. Its purpose is to transform what might be an inherently complex situation into simpler terms that can be analysed more easily. It can be used to help understand the meaning of data and to simulate what might happen in practice under different conditions. A model may be physical, represented in software or be a set of mathematical relationships.

Modelling generally includes the following steps:

- describing the problem;
- describing the purpose of building a model and the outcomes desired;
- developing a conceptual model of the problem;
- building a physical, software or mathematical representation of the conceptual model;
- developing software or other tools to analyse how the model behaves;
- processing data;
- validating or calibrating the model by reviewing outputs for known situations;
- drawing conclusions from the model about the real world problem.

Each of these steps can involve approximations, assumptions and expert judgement and (if possible) they should be validated by people independent of the developers. Critical assumptions should be reviewed against available information to assess their credibility.

To achieve reliable results when using models, the following should be validated:

- the conceptual model adequately represents the situation being assessed;
- the model is being used within the contextual limits for which it was designed;
- theoretical concepts underlying the model and any associated calculations are well understood;
- the selection of parameters and mathematical representations of the concepts is sound;
- the mathematics underlying calculations are well understood;
- input data is accurate and reliable, or the nature of the model takes into account the reliability of the input data used;
- the model operates as planned with no internal errors or bugs;
- the model is stable and not overly sensitive to small changes in key inputs.

This can be achieved by:

- performing a sensitivity analysis to check how sensitive the model is to changes in input parameters;

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

- stress testing the model with particular scenarios, often extreme scenarios;
- comparing outputs with past data (other than those from which it was developed);
- verifying that similar results are obtained when the model is run by different people;
- checking the outputs against actual performance.

Comprehensive documentation of the model and the theories and assumptions on which it is based should be kept, sufficient to enable validation of the model.

6.2.4.2 Using software for analysis

Software programmes can be used to represent and organize data or to analyse it. Software programmes used for modelling and analysis often provide a simple user interface and a rapid output, but these characteristics might lead to invalid results that are unnoticed by the user. Invalid results can arise because of:

- inadequacies in the algorithms used to represent the situation;
- assumptions made in the design and use of the model underlying the software;
- errors in data input including misunderstandings of their meaning;
- data conversion issues when new software is used;
- poor interpretation of outputs.

Commercial software is often black box (commercial in confidence) and might contain any of these errors.

New software should be tested using a simple model with inputs that have a known output, before progressing to test more complex models. The testing details should be retained for use on future version updates or for new software analysis programmes.

Errors in the constructed model can be checked by increasing or decreasing an input value to determine whether the output responds as expected. This can be applied to each of the various inputs. Data input errors are often identified when varying the data inputs. This approach also provides information on the sensitivity of the model to data variations.

A good understanding of the mathematics relevant to the particular analysis is recommended to avoid erroneous conclusions. Not only are the above errors likely, but also the selection of a particular programme might not be appropriate. It is easy to follow a programme and assume that the answer will therefore be right. Evidence should be gathered to check that the outputs are reasonable.

6.3 Apply risk assessment techniques

6.3.1 Overview

The techniques described in Annexes A and B are used to develop an understanding of risk as an input to decisions where there is uncertainty, including decisions about whether and how to treat risk.

Assessment techniques can be used for:

- identifying risk (see 6.3.2);
- determining causes, sources and drivers of risk, and the level of exposure to them (see 6.3.3);
- investigating the overall effectiveness of controls and the modifying effect of proposed risk treatments (see 6.3.4);
- understanding consequences and likelihood (see 6.3.5);

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

- analysing interactions and dependencies (see 6.3.6);
- providing a measure of risk (see 6.3.7).

Factors to consider when selecting a particular technique for these activities are described in Clause 7.

In general, analysis can be descriptive (such as a report of a literature review, a scenario analysis or a description of consequences) or quantitative, where data are analysed to produce numerical values. In some cases, rating scales can be applied to compare particular risks.

The way in which risk is assessed and the form of the output should be compatible with any defined criteria. For example, quantitative criteria require a quantitative analysis technique which produces an output with the appropriate units.

Mathematical operations should be used only if the chosen metrics allow. In general, mathematical operations should not be used with ordinal scales. Even with fully quantitative analysis, input values are usually estimates. A level of accuracy and precision should not be attributed to results beyond that which is consistent with the data and methods employed.

6.3.2 Identifying risk

Identifying risk enables uncertainty to be explicitly taken into account. All sources of uncertainty and both beneficial and detrimental effects might be relevant, depending on the context and scope of the assessment.

Techniques for identifying risk usually make use of the knowledge and experience of a variety of stakeholders (see B.1.1). They include considering:

- what uncertainty exists and what its effects might be;
- what circumstances or issues (either tangible or intangible) have the potential for future consequences;
- what sources of risk are present or might develop;
- what controls are in place and whether they are effective;
- what, how, when, where, and why events and consequences might occur;
- what has happened in the past and how this might reasonably relate to the future;
- which human aspects and organizational factors might apply.

Physical surveys can also be useful in identifying sources of risk or early warning signs of potential consequences.

The output from risk identification can be recorded as a list of risks with events, causes and consequences specified, or using other suitable formats.

Whatever techniques are used, risk identification should be approached methodically and iteratively so that it is thorough and efficient. Risk should be identified early enough to allow actions to be taken whenever possible. However there are occasions when some risks cannot be identified during a risk assessment. A mechanism should therefore be put in place for capturing emerging risks and recognizing early warning signs of potential success or failure.

Techniques for identifying risk are described in Clause B.2.

6.3.3 Determining sources, causes and drivers of risk

Identifying causes, sources and drivers of risk can:

- contribute towards estimating the likelihood of an event or consequence;

Documents
Document Sharing Hub
Full document details: BS EN IEC 31010:2019

- help to identify treatments that will modify risk;
- assist in determining early warning indicators and their detection thresholds;
- determine common causes which can help develop priorities for treating risk.

Sources of risk can include events, decisions, actions and processes, both favourable and unfavourable, as well as situations that are known to exist but where outcomes are uncertain. Any form of uncertainty described in 4.1 can be a source of risk.

Events and consequences can have multiple causes or causal chains.

Risk can often only be controlled by modifying risk drivers. They influence the status and development of risk exposures, and often affect more than one risk. As a result, risk drivers often need more and closer attention than sources of individual risks.

Techniques for determining sources, causes and drivers of risk are described in Clause B.3.

6.3.4 Investigating the effectiveness of existing controls

Risk is affected by the overall effectiveness of any controls that are in place. The following aspects of controls should be considered:

- the mechanism by which the controls are intended to modify risk;
- whether the controls are in place, are capable of operating as intended, and are achieving the expected results;
- whether there are shortcomings in the design of controls or the way they are applied;
- whether there are gaps in controls;
- whether controls function independently, or if they need to function collectively to be effective;
- whether there are factors, conditions, vulnerabilities or circumstances that can reduce or eliminate control effectiveness including common cause failures;
- whether controls themselves introduce additional risks.

NOTE A risk can have more than one control and controls can affect more than one risk.

A distinction should be made between controls that change likelihood, consequences or both, and controls that change how the burden of risk is shared between stakeholders. For example, insurance and other forms of risk financing do not directly affect the likelihood of an event or its outcomes but can make some of the consequences more tolerable to a particular stakeholder by reducing their extent or smoothing cash flow.

Any assumptions made during risk analysis about the actual effect and reliability of controls should be validated where possible, with a particular emphasis on individual or combinations of controls that are assumed to have a substantial modifying effect. This should take into account information gained through routine monitoring and review of controls.

Techniques for analysing controls are described in Clause B.4

6.3.5 Understanding consequences, and likelihood

6.3.5.1 Analysing the type, magnitude and timing of consequences

Consequence analysis can vary from a description of outcomes to detailed quantitative modelling or vulnerability analysis. Consequential effects (domino or knock-on effects) where one consequence leads to another should be considered where relevant.

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

Risk can be associated with a number of different types of consequences, impacting different objectives. The types of consequence to be analysed should have been decided when planning the assessment. The context statement should be checked to ensure that the consequences to be analysed align with the purpose of the assessment and the decisions to be made. This can be revisited during the assessment as more is learned.

The magnitude of consequences can be expressed quantitatively as a point value or as a distribution. A distribution can be appropriate where:

- the value for the consequence is uncertain;
- the consequences vary depending on circumstances;
- the parameters that affect consequences vary.

Consideration of the full distribution associated with a consequence provides complete information. It is possible to summarize the distribution in the form of a point value such as the expected value (mean), variation (variance) or the percentage in the tail or some other relevant part of the distribution (percentile).

For any method of obtaining a point value or values to represent a distribution of consequences, there are underlying assumptions and uncertainties about:

- the form of the distribution chosen to fit the data (e.g. continuous or discrete, normal or highly skewed);
- the most appropriate way of representing that distribution as a point value;
- the value of the point estimate because of inherent uncertainties in the data from which the distribution was produced.

It should not be assumed that data relevant to risk necessarily follows a normal distribution.

In some cases information can be summarized as a qualitative or semi-quantitative rating which can be used when comparing risks.

The magnitude of consequences might also vary according to other parameters. For example, the health consequences of exposure to a chemical generally depend on the dose to which the person or other species is exposed. For this example, the risk is usually represented by a dose response curve which depicts the probability of a specified end point (e.g. death) as a function of a short-term or an accumulated dose.

Consequences might also change over time. For example, the adverse impacts of a fault might become more severe the longer the fault exists. Appropriate techniques should be selected to take this into account.

Sometimes consequences result from exposures to multiple sources of risk: for example, environmental or human health effects from the exposure to biological, chemical, physical, and psychosocial sources of risk. In considering multiple exposures the possibility of synergistic effects should be taken into account as well as the influence of the duration and extent of exposure.

6.3.5.2 Analysing likelihood

Likelihood can refer to the likelihood of an event or to the likelihood of a specified consequence. The parameter to which a likelihood value applies should be explicitly stated and the event or consequence whose likelihood is being stated should be clearly and precisely defined. It can be necessary to include a statement about exposure and duration to fully define likelihood.

Likelihood can be described in a variety of ways, including as an expected probability or frequency or in descriptive terms (e.g. "highly likely"). Where a descriptive term is used, its

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

meaning should be defined. There can be uncertainty in the likelihood which can be shown as a distribution of values representing the degree of belief that a particular value will occur.

Where a percentage is used as a measure of likelihood the nature of the ratio to which the percentage applies should be stated.

EXAMPLE 1 The statement that the chance of a supplier failing to deliver is 5 % is vague in terms of both time period and population. It is also unclear whether the percentage refers to 5 % of projects or 5 % of suppliers. A more explicit statement would be "the probability of one or more suppliers failing to deliver the required goods or services to a project within the life of a project is 5 % of projects".

To minimize misinterpretations when expressing likelihood, either qualitatively or quantitatively, the time period and population concerned should be explicit and consistent with the scope of the particular assessment.

EXAMPLE 2 The probability of one or more suppliers failing to deliver the required goods or services to a project within the next two months is 1 % of projects whereas within a six-month time scale failure can occur in 3 % of projects.

There are many possible biases which can influence estimates of likelihood. Furthermore, interpretation of the likelihood estimate can vary depending on the context within which it is framed. Care should be taken to understand the possible effects of individual (cognitive) and cultural biases.

Techniques for understanding consequences and likelihood are described in Clause B.5.

6.3.6 Analysing interactions and dependencies

There are usually many interactions and dependencies between risks. For example, multiple consequences can arise from a single cause or a particular consequence might have multiple causes. The occurrence of some risks may make the occurrence of others more or less likely, and these causal links can form cascades or loops.

To achieve a more reliable assessment of risk where causal links between risks are significant, it can be useful to create a causal model that incorporates the risks in some form. Common themes can be sought within the risk information such as common causes or drivers of risk, or common outcomes.

Interactions between risks can have a range of impacts on decision making, for example, escalating the importance of activities which span multiple connected risks or increasing the attractiveness of one option over others. Risks might be susceptible to common treatments, or there can be situations such that treating one risk has positive or negative implications elsewhere. Treatment actions can be consolidated at times to significantly reduce the amount of work and more effectively balance available resources. A coordinated treatment plan should take account of these factors rather than assuming that each risk should be treated independently.

Techniques for analysing interactions and dependencies are described in Clause B.6.

6.3.7 Understanding measures of risk

6.3.7.1 Determining measures of risk

In some situations it is useful to provide a measure of risk as some combination of the magnitude of potential consequences and the likelihood of those consequences. This can involve qualitative, semi-quantitative or quantitative measures.

- Qualitative approaches are usually based on descriptive (nominal) or ranking (ordinal) scales for consequences and likelihoods.
- Semi-quantitative approaches include where:

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

  - one parameter (usually likelihood) is expressed quantitatively and the other described or expressed on a rating scale;
  - scales are divided into discrete bands, the limits of which are expressed quantitatively. Points on the scale are often set up to have a logarithmic relationship to fit with data;
  - numeric descriptors are added to scale points, the meanings of which are described qualitatively.

  The use of semi-quantitative scales can lead to misinterpretations if the basis for any calculations is not explained carefully. Therefore, semi-quantitative approaches should be validated and used with caution.

- Quantitative approaches use measures of consequences and likelihoods that are expressed on numerical (ratio) scales. Where a risk is analysed in quantitative terms, it should be ensured that appropriate units and dimensions are used and carried over through the assessment.

Qualitative and semi-quantitative techniques can be used only to compare risks with other risks measured in the same way or with criteria expressed in the same terms. They cannot be used for directly combining or aggregating risks and they are very difficult to use in situations where there are both positive and negative consequences or when trade-offs are to be made between risks.

When quantitative estimates for a consequence and its likelihood are combined as a simple product to provide a magnitude for a risk, information can be lost. In particular, there is no distinction between risks with high consequence and low likelihood and those with low consequences that occur frequently. To compensate for this, a weighting factor may be applied to either the consequence or likelihood; but this should be used with care.

Risk cannot always be adequately described or estimated as a single value representing the likelihood of a specific consequence. Examples where this applies include situations in which:

- consequences are best expressed as a probability distribution of consequences;
- an event has a number of different causes and leads to a range of outcomes and possible consequential effects;
- consequences arise cumulatively from on-going exposure to a source of risk;
- sources of risk (such as systemic problems) are identifiable, but it is very difficult to specify the nature and or likelihood of the consequences that might arise. (In this case estimating a valid magnitude for risk in terms of likelihood and consequence becomes impossible.).

When a risk has a distribution of possible consequences, a measure of risk can be obtained as the probability weighted average of the consequences (i.e. the expectation value). However, this might not always be a good measure of risk because it reflects the mean consequence of the distribution. This results in loss of information about less likely consequences that can be severe and hence important for understanding risk. Techniques for dealing with extreme values are not included in this document.

NOTE An expectation value or expected value is equivalent to summing every consequence/likelihood pair across a distribution, which is equivalent to using the mean consequence of the distribution.

Examples of quantitative metrics of the magnitude of a risk include:

- an expected frequency of occurrence of a specified consequence such as the number of vehicle accidents per thousand kilometres travelled in a region;
- the expected time between events of interest such as the mean up time of an item;
- a probability of a specified end point over a defined period of exposure (relevant when consequences accumulate over a period of exposure) such as the probability of contracting cancer in a life time as a result of exposure to a specified dose of a chemical;

Documents
Document Sharing Hub
Full document details: BS EN IEC 31010:2019

- an expected value, such as the expected returns or financial gains over an investment period, or the expected public health burden in terms of disability adjusted life years per million people per year;
- a statistic representing the shape of a distribution of consequences such as the variance or volatility of returns on an investment;
- a value at or above or below a specified percentile in a consequence distribution;

  EXAMPLE The profit from a project that there is a 90 % chance of achieving; or the Value at Risk (VaR) of a portfolio which measures the loss that might arise in a portfolio over a specified time period with a specified probability.

- an extreme measure associated with the distribution of consequences such as the expected maximum consequences.

Consequence based metrics such as the maximum credible loss or probable maximum loss are mainly used when it is difficult to define which controls have the capability of failing or where there is insufficient data on which to base estimates of likelihood.

The magnitude of risk depends on the assumptions made about the presence and effectiveness of relevant controls. Terms such as inherent or gross risk (for the situation where those controls which can fail are assumed to do so) and residual or net risk for the level of a risk when controls are assumed to operate as intended are often used by practitioners. However, it is difficult to define these terms unambiguously and it is therefore advisable to always state explicitly the assumptions made about controls.

When reporting a magnitude of risk, either qualitatively or quantitatively, the uncertainties associated with assumptions and with the input and output parameters should be described.

6.3.7.2 Aggregating measures of risk

In some cases (such as for capital allocation) it can be useful to combine values for a set of risks to produce a single value. Provided the risks are characterized by a single consequence, measured in the same units, such as monetary value, they can in principle be combined. That is, they can be combined only when consequences and likelihood are stated quantitatively and the units are consistent and correct. In some situations, a measure of utility can be used as a common scale to quantify and combine consequences that are measured in different units.

Developing a single consolidated value for a set of more complex risks loses information about the component risks. In addition, unless great care is taken, the consolidated value can be inaccurate and has the potential to be misleading. All methods of aggregating risks to a single value have underlying assumptions which should be understood before being applied. Data should be analysed to seek correlations and dependencies which will affect how risks combine. Modelling techniques used to produce an aggregate level of risk should be supported by scenario analysis and stress testing.

Where models incorporate calculations involving distributions, they should include correlations between those distributions in an appropriate manner. If correlation is not taken into account appropriately the outcomes will be inaccurate and may be grossly misleading. Consolidating risks by simply adding them up is not a reliable basis for decision making and could lead to undesired results. Monte Carlo simulation can be used to combine distributions (see B.5.10).

Qualitative or semi-quantitative measures of risk cannot be directly aggregated. Equally, only general qualitative statements can be made about the relative effectiveness of controls based on qualitative or semi-quantitative measures of changes in level of risk.

Relevant data about different risks can be brought together in a variety of ways to assist decision makers. It is possible to conduct a qualitative aggregation based on expert opinion, taking into account more detailed risk information. The assumptions made and information used to conduct qualitative aggregations of risk should be clearly articulated.

Documents
Document Sharing Hub
Full document details: BS EN IEC 31010:2019

6.3.7.3 Societal risk

Where a population is exposed to risk, a simple aggregation of the individual level of risk by multiplying by the population exposed, in most cases, does not adequately represent the true impact of the consequences. For example, an individual's risk of a fatality from an event such as a dam failure might need to be considered differently from the same event affecting a group of individuals together.

Societal risk is typically expressed and evaluated in terms of the relationship between the frequency of occurrence of a consequence (F) and the number of people bearing the consequences (N). (See F-N diagrams in B.8.3).

Techniques that provide a measure of risk are described in Clause B.7.

6.4 Review the analysis

6.4.1 Verifying and validating results

Where practicable, results of analysis should be verified and validated. Verification involves checking that the analysis was done correctly. Validation involves checking that the right analysis was done to achieve the required objectives. For some situations verification and validation can involve independent review processes.

Validation can include:

- checking that the scope of the analysis is appropriate for the stated goals;
- reviewing all critical assumptions to ensure they are credible in the light of available information;
- checking that appropriate methods, models and data were used;
- using multiple methods, approximations and sensitivity analysis to test and validate conclusions.

Verification can include:

- checking the validity of mathematical manipulations and calculations;
- checking that the results are insensitive to the way data or results are displayed or presented;
- comparing results with past experience where data exists or by comparison with outcomes after they occur;
- establishing whether the results are sensitive to the way data or results are displayed or presented and to identify input parameters that have a significant effect on the results of the assessment;
- comparing results with past or subsequent experience including explicitly obtaining feedback as time progresses.

6.4.2 Uncertainty and sensitivity analysis

Those analysing risk should understand the uncertainties in the analysis and appreciate the implications for the reliability of the results. Uncertainties and their implications should always be communicated to decision makers.

Uncertainty in analysis outputs can arise because:

- there is variability in the system being considered;
- the data is from an unreliable source, inconsistent or insufficient – for example, the type of data collected or methods of collection might have changed;

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

- there might be ambiguity, for example in the way that qualitative descriptors are stated or understood;
- the analysis method does not adequately represent the complexity of the system;
- there is a high reliance on people's expert opinion or judgement;
- relevant data might not exist or the organization might not have collected the data needed;
- data from the past might not provide a reliable basis from which to forecast the future because something within the context or circumstances has changed;
- there are uncertainties or approximations in the assumptions that are made.

When a lack of reliable data is recognized during the analysis, further data should be collected, if practicable. This can involve implementing new monitoring arrangements. Alternatively, the analysis process should be adjusted to take account of the data limitations.

A sensitivity analysis can be carried out to evaluate the significance of uncertainties in data or in the assumptions underlying the analysis. Sensitivity analysis involves determining the relative change to the results brought about by changes in individual input parameters. It is used to identify data that need to be accurate, and those that are less sensitive and hence have less effect upon overall accuracy. Parameters to which the analysis is sensitive and the degree of sensitivity should be stated where appropriate.

Parameters that are critical to the assessment and that are subject to change should be identified for on-going monitoring, so that the risk assessment can be updated, and, if necessary, decisions reconsidered.

6.4.3 Monitoring and review

Monitoring can be used:

- to compare actual outcomes with the results predicted by risk assessment and hence improve future assessments;
- to look for precursors and early indicators of potential consequences that were identified by the assessment;
- to collect data needed for a good understanding of risk;
- to scan for new risk and unexpected changes that can indicate a need to update assessment.

Where a sensitivity analysis indicates parameters of particular importance to the outcome of an analysis, these should also be considered for monitoring.

Assessments should be reviewed periodically to identify whether change has occurred, including changes in the context or in assumptions, and whether there is new information or new methods available.

6.5 Apply results to support decisions

6.5.1 Overview

The outcomes from risk analysis provide an input to decisions that need to be made and actions that are taken.

NOTE An understanding of risk can inform actions even where no explicit decision-making process is followed.

The factors to consider when making decisions and any specific criteria should have been defined as part of establishing the context for the assessment (see 6.1.6).

Two types of decisions can be distinguished:

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

- decisions about the significance of risk and whether and how to treat risk;
- decisions that involve comparing options where each has uncertainties (such as which of several opportunities to pursue).

6.5.2 Decisions about the significance of risk

The information from risk identification and analysis can be used to draw conclusions about whether the risk should be accepted and the comparative significance of the risk relative to the objectives and performance thresholds of the organization. This provides an input into decisions about whether risk is acceptable or requires treatment, and any priorities for treatment.

Some risks may be accepted for a finite time (for example, to allow time to actually implement treatments). The assessor should be clear about the mechanisms for temporarily accepting risks and the process to be used for subsequent reconsideration.

Priorities for treatment, for monitoring or for more detailed analysis are often based on a magnitude of risk obtained by combining a representative consequence and its likelihood, and displayed using a consequence/likelihood matrix (B.10.3). This method has some limitations (see B.10.3.5 and 6.3.7.1). Factors other than the magnitude of risk that can be taken into account in deciding priorities include:

- other measures associated with the risk such as the maximum or expected consequences or the effectiveness of controls;
- the qualitative characteristics of events or their possible consequences;
- the views and perceptions of stakeholders;
- the cost and practicability of further treatment compared with the improvement gained;
- interactions between risks including the effects of treatments on other risks.

Once risks have been evaluated and treatments decided, the risk assessment process can be repeated to check that proposed treatments have not created additional adverse risks and that the risk remaining after treatment is within the organization's risk appetite.

Techniques for evaluating the significance of risk are described in Clause B.8.

6.5.3 Decisions that involve selecting between options

Selecting between options normally involves weighing the potential advantages and disadvantages of each option taking into account uncertainties including:

- uncertainties associated with the potential outcomes of the options and estimates of costs and benefits;
- potential events and developments that may affect outcomes;
- the varied values that different stakeholders place on costs and benefits;
- uncertainty around judgements made from the outputs of risk analysis, including considerations such as whether objectives and criteria will continue unchanged into the future.

This type of decision is often made using expert judgement based on the understanding from an analysis of the options concerned and the risk associated with each, taking into account:

- trade-offs that may need to be made between competing objectives;
- the organization's appetite for risk;
- the different attitudes and beliefs of stakeholders.

Techniques that can be used when comparing options that involve uncertainty are described in Clause B.9.

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

6.6 Record and report risk assessment process and outcomes

The results of risk assessment, the methodologies used and the rationale for assumptions and any recommendations should be documented and a decision made about what information needs to be communicated and to whom. The way in which records are to be reviewed and updated should be defined.

The purpose of records is to:

- communicate information about risk to decision makers and other stakeholders including regulators;
- provide a record and justification of the rationale for decisions made;
- preserve the results of assessment for future use and reference;
- track performance and trends;
- provide confidence that risks are understood and are being managed appropriately;
- enable verification of the assessment;
- provide an audit trail.

It follows that any documentation or records should be provided in a timely manner and be in a form that can be understood by those who will read it. Documents should also provide the necessary technical depth for validation, and sufficient detail to preserve the assessment for future use. The information provided should be sufficient to allow both the processes followed and the outcomes to be reviewed and validated. Assumptions made, limitations in data or methods, and reasons for any recommendations made should be clear.

Risk should be expressed in understandable terms, and the units in which quantitative measures are expressed should be clear and correct.

Those presenting the results should characterize their confidence or that of their team in the accuracy and completeness of the results. Uncertainties should be adequately communicated so that the report does not imply a level of certainty beyond the reality.

Techniques for recording and reporting are described in Clause B.10.

7 Selecting risk assessment techniques

7.1 General

Clause 7 describes factors to consider when selecting a technique or techniques for a particular purpose. Annexes A and B list and further explain some commonly used techniques. They describe the characteristics of each technique and its possible range of application, together with its inherent strengths and weaknesses.

Many of the techniques described in this document were originally developed for particular industries seeking to manage particular types of unwanted outcomes. Several of the techniques are similar, but use different terminologies, reflecting their independent development for a similar purpose in different sectors. Over time the application of many of the techniques has broadened, for example extending from technical engineering applications to financial or managerial situations, or to consider positive as well as negative outcomes. New techniques have emerged and old ones have been adapted to new circumstances. The techniques and their applications continue to evolve. There is potential for enhanced understanding of risk by using techniques outside their original application. Annexes A and B therefore indicate the characteristics of techniques that can be used to determine the range of circumstances to which they can be applied.

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

7.2 Selecting techniques

The choice of technique and the way it is applied should be tailored to the context and use, and provide information of the type and form needed by the stakeholders. In general terms, the number and type of technique selected should be scaled to the significance of the decision, and take into account constraints on time and other resources, and opportunity costs.

In deciding whether a qualitative or quantitative technique is more appropriate, the main criteria to consider are the form of output of most use to stakeholders and the availability and reliability of data. Quantitative techniques generally require high quality data if they are to provide meaningful results. However, in some cases where data is not sufficient, the rigour needed to apply a quantitative technique can provide an improved understanding of the risk, even though the result of the calculation might be uncertain.

There is often a choice of techniques relevant for a given circumstance. Several techniques might need to be considered, and applying more than one technique can sometimes provide useful additional understanding. [2] Different techniques can also be appropriate as more information becomes available.

In selecting a technique or techniques the following should therefore be considered:

- the purpose of the assessment;
- the needs of stakeholders;
- any legal, regulatory and contractual requirements;
- the operating environment and scenario;
- the importance of the decision (e.g. the consequences if a wrong decision is made);
- any defined decision criteria and their form;
- the time available before a decision must be made;
- information that is available or can be obtained;
- the complexity of the situation;
- the expertise available or that can be obtained.

The characteristics of the techniques relevant to these requirements are listed in Table A.1. Table A.2 provides a list of techniques, classified according to these characteristics.

As the degree of uncertainty, complexity and ambiguity of the context increases then the need to consult a wider group of stakeholders will increase, with implications for the combination of techniques selected.

NOTE For example, IEC TR 63039:2016 [50] guides how to use ETA, FTA and Markov techniques in a complementary way so that the combined use is an efficient way to analyse risk of complex systems.

Some of the techniques described in this document can be applied during steps of the ISO 31000 risk management process in addition to their usage in risk assessment. Application of the techniques to the risk management process is illustrated in Figure A.1. Table A.3 illustrates their application specifically to assessment.

Annex B contains an overview of each technique, its use, its inputs and outputs, its strengths and limitations and, where applicable, a reference for where further detail can be found. It categorizes techniques according to their primary application in assessing risk, namely:

- eliciting views from stakeholders and experts, (Clause B.1);
- identifying risk (Clause B.2);
- determining sources, causes and drivers of risk (Clause B.3);
- analysing existing controls (Clause B.4);

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

- understanding consequences and likelihood (Clause B.5);
- analysing dependencies and interactions (Clause B.6);
- providing measures of risk (Clause B.7);
- evaluating the significance of risk (Clause B.8);
- selecting between options (Clause B.9);
- recording and reporting (Clause B.10).

Within each grouping, techniques are arranged alphabetically and no order of importance is implied.

The majority of techniques in Annex B assume that risks or sources of risk can be identified. There are also techniques which can be used to indirectly assess residual risk by considering controls and requirements that are in place (see for example IEC 61508 [36]).

While this document discusses and provides example techniques, the techniques described are non-exhaustive and no recommendation is made as to the efficacy of any given technique in any given circumstance. Care should be taken in selecting any technique to ensure that it is appropriate, reliable and effective in the given circumstance.

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

Annex A
(informative)

Categorization of techniques

A.1 Introduction to categorization of techniques

Table A.1 explains the characteristics of techniques that can be used for selecting which technique or techniques to use.

Table A.1 – Characteristics of techniques

Characteristic	Description	Details (e.g. features indicators)
Application	How the technique is used in risk assessment (see titles of Clauses B.1 to B.10)	Elicit views, identify, analyse cause, analyse controls, etc.
Scope	Applies to risk at organizational level, departmental or project level or individual processes or equipment level	organization (org) project/department (dep) equipment/process (equip/proc)
Time horizon	Looks at short-, medium- or long-term risk or is applicable to any time horizon	Short, medium, long, any
Decision level	Applies to risk at a strategic, tactical or operational level	Strategic (1), tactical (2), operational (3)
Starting info/data needs	The level of starting information or data needed	High, medium, low
Specialist expertise	Level of expertise required for correct use	low: intuitive or one to two days' training moderate: training course of more than two days high: requires significant training or specialist expertise
Qualitative – quantitative	Whether the method is qualitative, semi-quantitative or quantitative	quantitative (quant) qualitative (qual) semi-quantitative (semi-quant) can be used qualitatively or quantitatively (either)
Effort to apply	Time and cost required to apply technique	high, medium, low

A.2 Application of categorization of techniques

Table A.2 lists a range of techniques classified according to these characteristics. The techniques described represent structured ways of looking at the problem in hand that have been found useful in particular contexts. The list is not intended to be comprehensive but covers a range of commonly used techniques from a variety of sectors. For simplicity the techniques are listed in alphabetical order without any priority.

Each technique is described in more detail in Annex B, as referenced in column 1 of Table A.2.

Documents
Document Sharing Hub

Full document details: BS EN IEC 31010:2019

Table A.2 – Techniques and indicative characteristics

Sub-clause	Technique	Description	Application	Scope	Time horizon	Decision level	Starting info/data needs	Specialist expertise	Qual/quant/ semi-quant	Effort to apply
B.8.2	ALARP/SFAIRP	Criteria for deciding significance of risk and means of evaluating tolerability of risk.	evaluate. risk	1	any	1/2	high	high	qual/quant	high
B.5.2	Bayesian analysis	A means of making inference about model parameters using Bayes' theorem which has the capability of incorporating empirical data into prior judgements about probabilities.	analyse likelihood	any	any	any	medium	high	quant	medium
B.5.3	Bayesian networks/ Influence diagrams	A graphical model of variables and their cause-effect relationships expressed using probabilities. A basic Bayesian network has variables representing uncertainties. An extended version, known as an influence diagram, includes variables representing uncertainties, consequences and actions.	identify risk estimate risk decide between options	any	any	any	medium	high	quant	medium/ high
B.4.2	Bow tie analysis	A diagrammatic way of describing the pathways from sources of risk to outcomes, and of reviewing controls.	Analyse risk analyse controls describe risk	2/3	short/ medium	any	low	low/ moderate	qual/semi-quant	low
B.1.2	Brainstorming	Technique used in workshops to encourage imaginative thinking.	elicit views	any	any	any	none	low/ moderate	qual	low
B.5.4	Business impact analysis	The BIA process analyses the consequences of a disruptive incident on the organization which determines the recovery priorities of an organization's products and services and, thereby, the priorities of the activities and resources which deliver them.	analyse conseq. analyse controls	1	short/ medium	2	medium	low	quant/qual	medium
B.6.1	Causal mapping	A network diagram representing events, causes and effects and their relationships.	analyse causes	2/3	any	2/3	medium	moderate	qual	medium
B.5.5	Cause-consequence analysis	A combination of fault and event tree analysis that allows inclusion of time delays. Both causes and consequences of an initiating event are considered.	analyse causes and conseq.	2/3	any	2/3	medium/ high	moderate/ high	quant	medium/ high

Documents
Document Sharing Hub
Full document details: BS EN IEC 31010:2019

Sub-clause	Technique	Description	Application	Scope	Time horizon	Decision level	Starting info/data needs	Specialist expertise	Qual/quant/ semi-quant	Effort to apply
B.2.2	Checklists classifications, taxonomies	Lists based on experience or on concepts and models that can be used to help identify risks or controls.	identify risk or controls	2/3	any	any	high to develop, low to use	low/ moderate	qual	low/medium
B.3.2	Cindynic approach	Considers goals, values, rules, data and models of stakeholders and identifies inconsistencies, ambiguities, omissions and ignorance. These form systemic sources and drivers of risk.	identify risk drivers	1/2	short or medium	1	low	moderate	qual	high
B.7.3	Conditional value at risk CVaR	Also called expected shortfall (ES), is a measure of the expected loss from a financial portfolio in the worst *a* % of cases.	measure of risk	any	short/ medium	3	high	high	quant	medium
B.10.3	Consequence/ likelihood matrix	Compares individual risks by selecting a consequence/likelihood pair and displaying them on a matrix with consequence on one axis and likelihood on the other.	report risks evaluate	any	any	any	medium	low to use, moderate to develop	qual/ semi-quant/ quant	low
B.9.2	Cost/benefit analysis	Uses money as a scale for estimating positive and negative, tangible and intangible, consequences of different options.	compare options	any	short/ medium	any	medium /high	moderate/ high	quant	medium/ high
B.6.2	Cross impact analysis	Evaluates changes in the probability of the occurrence of a given set of events consequent on the actual occurrence of one of them.	analyse likelihood and cause	any	short/ medium	any	low to high	moderate/ high	quant	medium/ high
B.9.3	Decision tree analysis	Uses a tree-like representation or model of decisions and their possible consequences. Outcomes are usually expressed in monetary terms or in terms of utility. An alternative representation of a decision tree is an influence diagram (see B.5.3).	compare options	any	any	2	low/ medium	moderate	quant	medium
B.1.3	Delphi technique	Collects judgements through a set of sequential questionnaires. People participate individually but receive feedback on the responses of others after each set of questions.	elicit views	any	any	any	none	moderate	qual	medium

Documents
Document Sharing Hub
Full document details: BS EN IEC 31010:2019

Sub-clause	Technique	Description	Application	Scope	Time horizon	Decision level	Starting info/data needs	Specialist expertise	Qual/quant/ semi-quant	Effort to apply
B.5.6	Event tree analysis (ETA)	Models the possible outcomes from a given initiating event and the status of controls thus analysing the frequency or probability of the various possible outcomes.	analyse conseq. and controls	2/3	any	any	low/medium	moderate	qual/quant	medium
B.5.7	Fault tree analysis (FTA)	Analyses causes of a focus event using Boolean logic to describe combinations of faults. Variations include a success tree where the top event is desired and a cause tree used to investigate past events.	analyse likelihood analyse causes	2/3	medium	2/3	high for quant analysis	depends on complexity	qual/quant	medium/ high
B.2.3	Failure modes and effects (and criticality) analysis FME(C)A	Considers the ways in which each component of a system might fail and the failure causes and effects. FMEA can be followed by a criticality analysis which defines the significance of each failure mode (FMECA).	identify risks	2/3	any	2/3	depends on application	moderate	qual/semi-quant/quant	low /high
B.8.3	Frequency / number (F/N) diagrams	Special case of quantitative consequence/likelihood graph applied to consideration of tolerability of risk to human life.	evaluate risk	1	any	any	high	high	quant	high
B.9.4	Game theory	The study of strategic decision making to model the impact of the decisions of different players involved in the game. Example application area can be risk based pricing.	decide between options	1	medium	1/2	high	high	quant	medium/ high
B.4.3	Hazard analysis and critical control points (HACCP)	Analyses the risk reduction that can be achieved by various layers of protection.	analyse controls monitor	2/3	short/ medium	2/3	medium	moderate	qual	medium
B.2.4	Hazard and operability studies (HAZOP)	A structured and systematic examination of a planned or existing process or operation in order to identify and evaluate problems that might represent risk to personnel or equipment, or prevent efficient operation.	identify and analyse risks	3	medium/ long	2/3	medium	facilitator: high, participants: moderate	qual	medium/ high
B.5.8	Human reliability analysis (HRA)	A set of techniques for identifying the potential for human error and estimating the likelihood of failure.	analyse risk and sources of risk	2/3	any	2/3	medium	high	qual/quant	medium to high
B.1.5	Interviews	Structured or semi- structured one-to-one conversations to elicit views.	elicit views	any	any	any	none	moderate	qual	high

Documents
Document Sharing Hub
Full document details: BS EN IEC 31010:2019