

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE



**Risk management – Risk assessment techniques**

**Gestion des risques – Techniques d'évaluation des risques**

IEC/ISO 31010:2009

<https://standards.iteh.ai/catalog/standards/sis/6928b032-c4f2-42d2-a083-4fa2ea00ebb7/iec-iso-31010-2009>

Withdrawing



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2009 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland  
Email: [inmail@iec.ch](mailto:inmail@iec.ch)  
Web: [www.iec.ch](http://www.iec.ch)

### About the IEC

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

### About IEC publications

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

- Catalogue of IEC publications: [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: [www.iec.ch/online\\_news/justpub](http://www.iec.ch/online_news/justpub)

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: [www.iec.ch/webstore/custserv](http://www.iec.ch/webstore/custserv)

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: [csc@iec.ch](mailto:csc@iec.ch)

Tel.: +41 22 919 02 11

Fax: +41 22 919 03 00

### A propos de la CEI

La Commission Electrotechnique internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

### A propos des publications CEI

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

- Catalogue des publications de la CEI: [www.iec.ch/searchpub/cur\\_fut-f.htm](http://www.iec.ch/searchpub/cur_fut-f.htm)

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,...). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: [www.iec.ch/online\\_news/justpub](http://www.iec.ch/online_news/justpub)

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: [www.electropedia.org](http://www.electropedia.org)

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: [www.iec.ch/webstore/custserv/custserv\\_entry-f.htm](http://www.iec.ch/webstore/custserv/custserv_entry-f.htm)

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:

Email: [csc@iec.ch](mailto:csc@iec.ch)

Tél.: +41 22 919 02 11

Fax: +41 22 919 03 00

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE



**Risk management – Risk assessment techniques**

**Gestion des risques – Techniques d'évaluation des risques**

<https://standards.iteh.ai/catalog/standards/sis/5928b032-c4f2-42d2-a083-4fa2ea00ebb7/iec-iso-31010-2009>

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

PRICE CODE **XD**  
CODE PRIX

## CONTENTS

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**RISK MANAGEMENT –  
RISK ASSESSMENT TECHNIQUES**

FOREWORD

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

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

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

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

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

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

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

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

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

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

IEC ISO 31010:2009

<https://standards.iteh.ai/catalog/standards/sis/6928b032-c4f2-42d2-a083-4fa2ea00ebb7/iec-iso-31010-2009>

Witholdam

## INTRODUCTION

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

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

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

Risk management includes the application of logical and systematic methods for

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

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

Risk assessment attempts to answer the following fundamental questions:

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

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

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



# RISK MANAGEMENT – RISK ASSESSMENT TECHNIQUES

## 1 Scope

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

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

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

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

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

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

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

## 2 Normative references

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

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

ISO 31000, *Risk management – Principles and guidelines*

## 3 Terms and definitions

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

## 4 Risk assessment concepts

### 4.1 Purpose and benefits

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

Some of the principal benefits of performing risk assessment include:

- understanding the risk and its potential impact upon objectives;

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

#### **4.2 Risk assessment and the risk management framework**

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

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

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

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

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

#### **4.3 Risk assessment and the risk management process**

##### **4.3.1 General**

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

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

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

#### 4.3.2 Communication and consultation

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

Involving stakeholders in the risk management process will assist in

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

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

#### 4.3.3 Establishing the context

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

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

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

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

- defining the extent of the project, process, function or activity in terms of time and location,
- defining the relationships between a particular project or activity and other projects or activities of the organization,
- defining the risk assessment methodologies,
- defining the risk criteria,
- defining how risk management performance is evaluated,
- identifying and specifying the decisions and actions that have to be made, and
- identifying scoping or framing studies needed, their extent, objectives and the resources required for such studies.

d) Defining risk criteria involves deciding

- the nature and types of consequences to be included and how they will be measured,
- the way in which probabilities are to be expressed,
- how a level of risk will be determined,
- the criteria by which it will be decided when a risk needs treatment,
- the criteria for deciding when a risk is acceptable and/or tolerable,
- whether and how combinations of risks will be taken into account.

Criteria can be based on sources such as

- agreed process objectives,
- criteria identified in specifications,
- general data sources,
- generally accepted industry criteria such as safety integrity levels,
- organizational risk appetite,
- legal and other requirements for specific equipment or applications.

#### 4.3.4 Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risks can be assessed at an organizational level, at a departmental level, for projects, individual activities or specific risks. Different tools and techniques may be appropriate in different contexts.

Risk assessment provides an understanding of risks, their causes, consequences and their probabilities. This provides input to decisions about:

- whether an activity should be undertaken;
- how to maximize opportunities;
- whether risks need to be treated;
- choosing between options with different risks;
- prioritizing risk treatment options;
- the most appropriate selection of risk treatment strategies that will bring adverse risks to a tolerable level.

#### 4.3.5 Risk treatment

Having completed a risk assessment, risk treatment involves selecting and agreeing to one or more relevant options for changing the probability of occurrence, the effect of risks, or both, and implementing these options.

This is followed by a cyclical process of reassessing the new level of risk, with a view to determining its tolerability against the criteria previously set, in order to decide whether further treatment is required.

#### 4.3.6 Monitoring and review

As part of the risk management process, risks and controls should be monitored and reviewed on a regular basis to verify that

- assumptions about risks remain valid;
- assumptions on which the risk assessment is based, including the external and internal context, remain valid;
- expected results are being achieved;
- results of risk assessment are in line with actual experience;
- risk assessment techniques are being properly applied;
- risk treatments are effective.

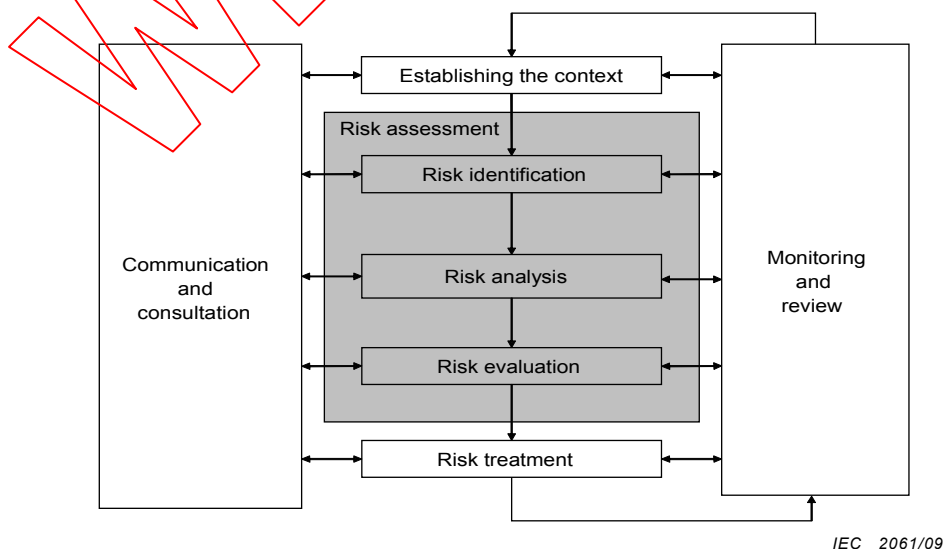
Accountability for monitoring and performing reviews should be established.

## 5 Risk assessment process

### 5.1 Overview

Risk assessment provides decision-makers and responsible parties with an improved understanding of risks that could affect achievement of objectives, and the adequacy and effectiveness of controls already in place. This provides a basis for decisions about the most appropriate approach to be used to treat the risks. The output of risk assessment is an input to the decision-making processes of the organization.

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation (see Figure 1). The manner in which this process is applied is dependent not only on the context of the risk management process but also on the methods and techniques used to carry out the risk assessment.



IEC 2061/09

**Figure 1 – Contribution of risk assessment to the risk management process**

Risk assessment may require a multidisciplinary approach since risks may cover a wide range of causes and consequences.

## 5.2 Risk identification

Risk identification is the process of finding, recognizing and recording risks.

The purpose of risk identification is to identify what might happen or what situations might exist that might affect the achievement of the objectives of the system or organization. Once a risk is identified, the organization should identify any existing controls such as design features, people, processes and systems.

The risk identification process includes identifying the causes and source of the risk (hazard in the context of physical harm), events, situations or circumstances which could have a material impact upon objectives and the nature of that impact

Risk identification methods can include:

- evidence based methods, examples of which are check-lists and reviews of historical data;
- systematic team approaches where a team of experts follow a systematic process to identify risks by means of a structured set of prompts or questions;
- inductive reasoning techniques such as HAZOP.

Various supporting techniques can be used to improve accuracy and completeness in risk identification, including brainstorming, and Delphi methodology.

Irrespective of the actual techniques employed, it is important that due recognition is given to human and organizational factors when identifying risk. Hence, deviations of human and organizational factors from the expected should be included in the risk identification process as well as "hardware" or "software" events.

## 5.3 Risk analysis

### 5.3.1 General

Risk analysis is about developing an understanding of the risk. It provides an input to risk assessment and to decisions about whether risks need to be treated and about the most appropriate treatment strategies and methods.

Risk analysis consists of determining the consequences and their probabilities for identified risk events, taking into account the presence (or not) and the effectiveness of any existing controls. The consequences and their probabilities are then combined to determine a level of risk.

Risk analysis involves consideration of the causes and sources of risk, their consequences and the probability that those consequences can occur. Factors that affect consequences and probability should be identified. An event can have multiple consequences and can affect multiple objectives. Existing risk controls and their effectiveness should be taken into account. Various methods for these analyses are described in Annex B. More than one technique may be required for complex applications.

Risk analysis normally includes an estimation of the range of potential consequences that might arise from an event, situation or circumstance, and their associated probabilities, in order to measure the level of risk. However in some instances, such as where the consequences are likely to be insignificant, or the probability is expected to be extremely low, a single parameter estimate may be sufficient for a decision to be made

In some circumstances, a consequence can occur as a result of a range of different events or conditions, or where the specific event is not identified. In this case, the focus of risk assessment is on analysing the importance and vulnerability of components of the system with a view to defining treatments which relate to levels of protection or recovery strategies.

Methods used in analysing risks can be qualitative, semi-quantitative or quantitative. The degree of detail required will depend upon the particular application, the availability of reliable data and the decision-making needs of the organization. Some methods and the degree of detail of the analysis may be prescribed by legislation.

Qualitative assessment defines consequence, probability and level of risk by significance levels such as “high”, “medium” and “low”, may combine consequence and probability, and evaluates the resultant level of risk against qualitative criteria.

Semi-quantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic, or have some other relationship; formulae used can also vary.

Quantitative analysis estimates practical values for consequences and their probabilities, and produces values of the level of risk in specific units defined when developing the context. Full quantitative analysis may not always be possible or desirable due to insufficient information about the system or activity being analysed, lack of data, influence of human factors, etc. or because the effort of quantitative analysis is not warranted or required. In such circumstances, a comparative semi-quantitative or qualitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.

In cases where the analysis is qualitative, there should be a clear explanation of all the terms employed and the basis for all criteria should be recorded.

Even where full quantification has been carried out, it needs to be recognized that the levels of risk calculated are estimates. Care should be taken to ensure that they are not attributed a level of accuracy and precision inconsistent with the accuracy of the data and methods employed.

Levels of risk should be expressed in the most suitable terms for that type of risk and in a form that aids risk evaluation. In some instances, the magnitude of a risk can be expressed as a probability distribution over a range of consequences.

### **5.3.2 Controls assessment**

The level of risk will depend on the adequacy and effectiveness of existing controls. Questions to be addressed include:

- what are the existing controls for a particular risk?
- are those controls capable of adequately treating the risk so that it is controlled to a level that is tolerable?
- in practice, are the controls operating in the manner intended and can they be demonstrated to be effective when required?

These questions can only be answered with confidence if there are proper documentation and assurance processes in place.

The level of effectiveness for a particular control, or suite of related controls, may be expressed qualitatively, semi-quantitatively or quantitatively. In most cases, a high level of accuracy is not warranted. However, it may be valuable to express and record a measure of risk control effectiveness so that judgments can be made on whether effort is best expended in improving a control or providing a different risk treatment.