# IEC/ISO 31010

Edition 1.0 2009-11

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

colour inside

## Risk management – Risk assessment techniques

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XD

ICS 03.100.01

ISBN 2-8318-1068-2

# CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

# RISK MANAGEMENT – RISK ASSESSMENT TECHNIQUES

## FOREWORD

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

International standard IEC/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.**

# 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*

# SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

# GESTION DES RISQUES – TECHNIQUES D'ÉVALUATION DES RISQUES

## AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI/ISO 31010 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement et le groupe de travail «Gestion des risques» de l'ISO TMB.

Le texte de cette norme est issu des documents suivants:

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

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme. A l'ISO, la norme a été approuvée par 17 comités membres sur 18 ayant votés.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

**IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.**

# INTRODUCTION

Les organisations de tout type et de toute taille font face à un éventail de risques susceptibles d'avoir un impact sur la réalisation de leurs objectifs.

Il peut s'agir de leurs activités (de leurs initiatives stratégiques à leurs opérations, processus et projets) qui peuvent avoir des conséquences en termes de résultats sociétaux, environnementaux, technologiques, de sécurité et sûreté, de mesures commerciales, financières et économiques, et avoir des impacts sociaux, culturels, politiques et toucher à la réputation de l'organisation.

Toute activité d'une organisation implique des risques qu'il convient de gérer. Le processus de gestion des risques facilite la prise de décision. Il s'agit en effet de tenir compte de l'incertitude, d'éventuels événements ou de certaines circonstances (prévus ou imprévus) et de leurs effets sur les objectifs fixés.

La gestion des risques comprend l'application de méthodes logiques et systématiques permettant:

- de communiquer et de consulter tout au long de ce processus;
- d'établir le contexte de l'organisation afin d'identifier, d'analyser, d'évaluer et de traiter le risque lié à une activité, un processus, une fonction ou un produit;
- de surveiller et d'examiner l'évolution des risques;
- de rapporter et de consigner les résultats de manière appropriée.

L'évaluation des risques fait partie intégrante de la gestion des risques. Elle consiste à fournir un processus structuré permettant d'identifier dans quelle mesure les objectifs peuvent être affectés, et d'analyser les conséquences et la probabilité d'occurrence des risques avant de décider s'il est nécessaire de procéder à un traitement supplémentaire.

L'évaluation des risques tente de répondre aux questions essentielles suivantes:

- que se passe-t-il et pourquoi (par identification des risques) ?
- quelles sont les conséquences ?
- quelle est la probabilité d'occurrence ?
- existe-t-il des facteurs permettant de limiter la conséquence du risque ou de réduire la probabilité d'occurrence du risque ?

Le niveau de risque est-il tolérable ou acceptable et nécessite-t-il un traitement supplémentaire ? La présente norme est destinée à refléter les bons usages actuels en matière de choix et d'utilisation des techniques d'évaluation des risques et ne fait pas référence à des notions nouvelles ou en cours de développement n'ayant pas atteint un niveau satisfaisant de consensus professionnel.

La présente norme est par nature générale de sorte qu'elle puisse servir de guide dans de nombreuses industries et pour différents types de systèmes. Il se peut que dans ces industries, il existe des normes plus spécifiques établissant les méthodologies et niveaux d'évaluation pour des applications particulières. Si ces normes ont été élaborées en harmonie avec la présente norme, les normes spécifiques seront généralement suffisantes.

# GESTION DES RISQUES – TECHNIQUES D'ÉVALUATION DES RISQUES

## 1 Domaine d’application

La présente Norme internationale est une norme d’accompagnement de l’ISO 31000 et fournit des lignes directrices permettant de choisir et d'appliquer des techniques systématiques d'évaluation des risques.

L'évaluation des risques réalisée conformément à la présente norme contribue aux autres activités de gestion des risques.

L'application de certaines techniques est présentée, avec des références spécifiques à d'autres normes internationales dans lesquelles la notion et l'application des techniques sont décrites plus en détail.

La présente norme n’est pas destinée à être utilisée à des fins de certification, de réglementation ou contractuelles.

La présente norme ne fournit pas de critères particuliers permettant d'identifier s'il est nécessaire de procéder à une évaluation des risques. Elle ne précise pas non plus la méthode d'évaluation des risques nécessaire pour une application donnée.

La présente norme ne spécifie pas toutes les techniques et de ce fait l’absence d’une technique n’implique pas qu’elle n’est pas valable. Le fait qu’une méthode soit applicable à une circonstance particulière n’implique pas qu’il convient nécessairement de l’appliquer.

NOTE La présente norme ne traite pas spécifiquement de la sécurité. C'est une norme générale de gestion des risques et toute référence à la sécurité est purement de nature informative. Les lignes directrices sur l'introduction des aspects de sécurité dans les normes CEI est définie dans le Guide ISO/CEI 51.

## 2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

Guide ISO/CEI 73, *Management du risque – Vocabulaire – Principes directeurs pour l'utilisation dans les normes*

ISO 31000, *Management du risque – Principes et lignes directrices*