IEC 62198

Edition 3.0 2025-06

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

## Managing risk in projects – Application guidelines

## Gestion des risques liés à un projet – Lignes directrices pour l'application

ICS 03.100.01

ISBN 978-2-8327-0501-8

IEC 62198:2025-06(en-fr)

# CONTENTS

FOREWORD ..... 3
INTRODUCTION ..... 5
1 Scope ..... 6
2 Normative references ..... 6
3 Terms and definitions ..... 6
4 Managing risks in projects ..... 9
5 Principles ..... 11
6 Project risk management framework ..... 12
6.1 General ..... 12
6.2 Leadership and commitment ..... 13
6.3 Design of the framework for managing project risk ..... 14
6.3.1 Understanding the project and its context ..... 14
6.3.2 Establishing the project risk management policy ..... 14
6.3.3 Accountability ..... 15
6.3.4 Integration into project management processes ..... 16
6.3.5 Resources ..... 16
6.3.6 Establishing internal project communication and reporting mechanisms ..... 16
6.3.7 Establishing external project communication and reporting mechanisms ..... 17
6.4 Implementing project risk management ..... 17
6.4.1 Implementing the framework for managing project risk ..... 17
6.4.2 Implementing the project risk management process ..... 17
6.5 Monitoring and review of the project risk management framework ..... 18
6.6 Continual improvement of the project risk management framework ..... 18
7 Project risk management process ..... 18
7.1 General ..... 18
7.2 The project risk management plan ..... 19
7.3 Communication and consultation ..... 20
7.4 Scope, context and criteria ..... 21
7.4.1 General ..... 21
7.4.2 Defining the scope ..... 21
7.4.3 Establishing the external context ..... 21
7.4.4 Establishing the internal context ..... 22
7.4.5 Establishing the context of the project risk management process ..... 22
7.4.6 Defining risk criteria ..... 23
7.4.7 Key elements ..... 23
7.5 Risk assessment ..... 24
7.5.1 General ..... 24
7.5.2 Risk identification ..... 24
7.5.3 Risk analysis ..... 25
7.5.4 Risk evaluation ..... 26
7.6 Risk treatment ..... 26
7.6.1 General ..... 26
7.6.2 Selection of risk treatment options ..... 27
7.6.3 Risk treatment plans ..... 28
7.7 Monitoring and review ..... 28
7.7.1 General ..... 28

7.7.2 Management meetings ..... 29
7.8 Recording and reporting the project risk management process ..... 29
7.8.1 Reporting ..... 29
7.8.2 Records and data storage ..... 30
7.8.3 The project risk register ..... 30
Annex A (informative) Examples ..... 32
A.1 General ..... 32
A.2 Project risk management process ..... 32
A.2.1 Stakeholder analysis (see 7.3) ..... 32
A.2.2 External and internal context (see 7.4.3 and 7.4.4) ..... 33
A.2.3 Risk management context (see 7.4.5) ..... 35
A.2.4 Risk criteria (see 7.4.6) ..... 36
A.2.5 Key elements (see 7.4.7) ..... 37
A.2.6 Risk analysis (see 7.5.3) ..... 38
A.2.7 Risk evaluation (see 7.5.4) ..... 41
A.2.8 Risk treatment (see 7.6) ..... 42
A.2.9 Risk register (see 7.5.2 and 7.8.3) ..... 42
Bibliography ..... 44

Figure 1 – Relationship between the components of the framework for managing risk, adapted from ISO 31000 ..... 13
Figure 2 – Project risk management process, adapted from ISO 31000 ..... 19
Figure A.1 – Risk management scope for an open pit mine project ..... 36
Figure A.2 – Distribution of cost estimate using simulation (example only) ..... 41

Table 1 – Typical phases in a project ..... 10
Table A.1 – Stakeholders for a government project ..... 32
Table A.2 – Stakeholders and objectives for a ship upgrade ..... 33
Table A.3 – Stakeholders and communication needs for a civil engineering project ..... 33
Table A.4 – External context for an energy project ..... 34
Table A.5 – Internal context for a private sector infrastructure project ..... 35
Table A.6 – Example risk management context for a power enhancement project ..... 35
Table A.7 – Criteria for a high-technology project ..... 36
Table A.8 – Key elements for a communications system project ..... 37
Table A.9 – Key elements for establishing a new health service organization ..... 38
Table A.10 – Example consequence scale ..... 39
Table A.11 – Example likelihood scale ..... 39
Table A.12 – Example of a matrix for determining the level of risk ..... 40
Table A.13 – Example of priorities for attention ..... 42
Table A.14 – Example of a treatment options worksheet ..... 42
Table A.15 – Simple risk register structure ..... 43
Table A.16 – Example scale for control effectiveness (CE) ..... 43

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

# Managing risk in projects - Application guidelines

## 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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62198 has been prepared by IEC technical committee 56: Dependability. It is an International Standard.

This third edition cancels and replaces the second edition, published in 2013, and constitutes a technical revision.

This edition includes the following technical changes with respect to the previous edition:

a) now aligned with ISO 31000, *Risk management – Guidelines* and ISO 21502, *Project, programme and portfolio management – Guidance on project management* [1][1].

b) the principles and generic guidelines on managing risk in projects have been updated to take into account developments in risk management and leadership, with particular reference to implementing risk management within the broad scope of project management envisaged by ISO 21502, including project-related oversight and direction by the sponsoring organization.

The text of this International Standard is based on the following documents:

| Draft | Report on voting |
|---|---|
| 56/2058/FDIS | 56/2081/RVD |

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

[1] Numbers in square brackets refer to the Bibliography.

# INTRODUCTION

Every project involves risk. Project risks can be related to the objectives of the project itself or to the objectives of the assets, products or services the project creates. This document provides guidelines for managing risks in a project in a systematic, effective, efficient and consistent way.

Risk management includes the coordinated activities to direct and control an organization with regard to risk. ISO 31000, *Risk management – Guidelines*, describes:

a) the principles for effective risk management,

b) the framework that provides the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout an organization, and

c) a process for managing risk that can be applied to all types of risk in any organization.

This document shows how those general principles and guidelines apply to managing uncertainty, threats and opportunities in projects. It applies to all kinds of projects and project management processes. When applying this document in conjunction with flexible or agile project management processes, the project's objectives, requirements and specifications are expected to evolve as the project progresses. The application of this document can be adjusted in these circumstances.

This document is relevant to individuals and organizations concerned with any or all phases in the life cycle of projects. It can also be applied to sub-projects and to sets of inter-related projects and programmes.

The application of this document can be tailored to each specific project by taking into consideration factors such as context, objectives and requirements. Therefore, it is not in the scope of this document to impose a certification system for risk management practitioners.

The guidance provided in this document is not intended to override existing industry-specific standards, although the guidance can be helpful in such instances.

## 1 Scope

This document provides principles and generic guidelines on managing risk in projects. In particular it describes a systematic approach to managing risk in projects based on ISO 31000.

Guidance is provided on the principles for managing risk in projects, the framework and organizational requirements for implementing risk management, and the process for conducting effective risk management.

## 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 31000, *Risk management – Guidelines*

# SOMMAIRE

AVANT-PROPOS ..... 48
INTRODUCTION ..... 50
1 Domaine d'application ..... 51
2 Références normatives ..... 51
3 Termes et définitions ..... 51
4 Management du risque dans les projets ..... 54
5 Principes ..... 56
6 Cadre organisationnel du management du risque lié à un projet ..... 58
6.1 Généralités ..... 58
6.2 Leadership et engagement ..... 59
6.3 Conception du cadre organisationnel pour le management du risque lié à un projet ..... 60
6.3.1 Compréhension du projet et de son contexte ..... 60
6.3.2 Etablissement d'une politique de management du risque lié à un projet ..... 60
6.3.3 Responsabilité ..... 61
6.3.4 Intégration aux processus de management de projet ..... 62
6.3.5 Ressources ..... 62
6.3.6 Mise en place de mécanismes de communication et d'élaboration de rapports sur le projet, en interne ..... 63
6.3.7 Mise en place de mécanismes de communication et d'élaboration de rapports sur le projet, en externe ..... 63
6.4 Mise en œuvre du management du risque lié à un projet ..... 64
6.4.1 Mise en œuvre du cadre organisationnel de management du risque lié à un projet ..... 64
6.4.2 Mise en œuvre d'un processus de management du risque lié à un projet ..... 64
6.5 Surveillance et revue du cadre organisationnel du management du risque lié à un projet ..... 64
6.6 Amélioration continue du cadre organisationnel du management du risque lié à un projet ..... 65
7 Processus de management du risque lié à un projet ..... 65
7.1 Généralités ..... 65
7.2 Plan de management du risque lié à un projet ..... 66
7.3 Communication et concertation ..... 67
7.4 Contenu, contexte et critères ..... 68
7.4.1 Généralités ..... 68
7.4.2 Définition du contenu ..... 68
7.4.3 Établissement du contexte externe ..... 69
7.4.4 Établissement du contexte interne ..... 69
7.4.5 Établissement du contexte du processus de management du risque lié au projet ..... 69
7.4.6 Définition des critères de risque ..... 70
7.4.7 Éléments essentiels ..... 71
7.5 Appréciation du risque ..... 71
7.5.1 Généralités ..... 71
7.5.2 Identification du risque ..... 71
7.5.3 Analyse du risque ..... 73
7.5.4 Évaluation du risque ..... 74
7.6 Traitement du risque ..... 74

7.6.1 Généralités ..... 74
7.6.2 Choix des options de traitement du risque ..... 75
7.6.3 Plans de traitement du risque ..... 76
7.7 Surveillance et revue ..... 76
7.7.1 Généralités ..... 76
7.7.2 Réunions de management ..... 77
7.8 Consignation et élaboration de rapports concernant le processus de management du risque lié à un projet ..... 77
7.8.1 Élaboration de rapports ..... 77
7.8.2 Enregistrements et stockage des données ..... 78
7.8.3 Registre des risques liés au projet ..... 78
Annexe A (informative) Exemples ..... 80
A.1 Généralités ..... 80
A.2 Processus de management du risque lié à un projet ..... 80
A.2.1 Analyse des parties prenantes (voir 7.3) ..... 80
A.2.2 Contextes externe et interne (voir 7.4.3 et 7.4.4) ..... 81
A.2.3 Contexte du management du risque (voir 7.4.5) ..... 83
A.2.4 Critères de risque (voir 7.4.6) ..... 84
A.2.5 Éléments essentiels (voir 7.4.7) ..... 85
A.2.6 Analyse du risque (voir 7.5.3) ..... 86
A.2.7 Évaluation du risque (voir 7.5.4) ..... 90
A.2.8 Traitement du risque (voir 7.6) ..... 91
A.2.9 Registre des risques (voir 7.5.2 et 7.8.3) ..... 91
Bibliographie ..... 93

Figure 1 – Relations entre les composantes du cadre organisationnel de management du risque (figure adaptée de l'ISO 31000) ..... 59
Figure 2 – Processus de management du risque lié au projet (figure adaptée de l'ISO 31000) ..... 66
Figure A.1 – Contenu du management du risque dans le cadre d'un projet de mine à ciel ouvert ..... 84
Figure A.2 – Distribution de l'estimation des coûts par simulation (uniquement à titre d'exemple) ..... 90

Tableau 1 – Phases types d'un projet ..... 55
Tableau A.1 – Parties prenantes d'un projet gouvernemental ..... 80
Tableau A.2 – Parties prenantes et objectifs pour une modernisation de navire ..... 81
Tableau A.3 – Parties prenantes et besoins en communication dans le cadre d'un projet de génie civil ..... 81
Tableau A.4 – Contexte externe dans le cadre d'un projet énergétique ..... 82
Tableau A.5 – Contexte interne dans le cadre d'un projet d'infrastructure dans le secteur privé ..... 83
Tableau A.6 – Contexte exemple du management du risque dans le cadre d'un projet d'augmentation de capacité énergétique ..... 83
Tableau A.7 – Critères d'un projet de haute technologie ..... 84
Tableau A.8 – Éléments essentiels pour un projet de système de communication ..... 85
Tableau A.9 – Éléments essentiels pour l'établissement d'un nouvel organisme de services de santé ..... 86

Tableau A.10 – Exemple d’échelle de conséquence ..... 87
Tableau A.11 – Exemple d’échelle de vraisemblance ..... 88
Tableau A.12 – Exemple de matrice permettant de déterminer le niveau de risque ..... 88
Tableau A.13 – Exemple de priorités d’attention ..... 90
Tableau A.14 – Exemple de feuille de calcul pour l’évaluation des options de traitement ..... 91
Tableau A.15 – Structure simplifiée de registre des risques ..... 92
Tableau A.16 – Exemple d’échelle d’efficacité des moyens de maîtrise (CE) ..... 92

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

# Gestion des risques liés à un projet - Lignes directrices pour l'application

## AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC 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 l'IEC. L'IEC 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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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'IEC attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'IEC ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de propriété revendiqué à cet égard. À la date de publication du présent document, l'IEC n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse https://patents.iec.ch. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevet.

L'IEC 62198 a été établie par le comité d'études 56 de l'IEC: Sûreté de fonctionnement. Il s'agit d'une Norme internationale.

Cette troisième édition annule et remplace la deuxième édition, parue en 2013, et constitue une révision technique.

Cette édition inclut les modifications techniques suivantes par rapport à l'édition précédente:

a) alignement avec l'ISO 31000, *Management du risque – Lignes directrices* et l'ISO 21502, *Management de projets, programmes et portefeuilles – Recommandations sur le management de projets* [1][1];

b) mise à jour des principes et lignes directrices génériques concernant le management du risque dans les projets, afin de tenir compte des développements en matière de management du risque et de leadership, avec une référence particulière à la mise en œuvre du management du risque dans le domaine d'application étendu du management de projet envisagé par l'ISO 21502, comprenant la supervision et la direction liées au projet proposées par l'organisme commanditaire.

Le texte de cette Norme internationale est issu des documents suivants:

| Projet | Rapport de vote |
|---|---|
| 56/2058/FDIS | 56/2081/RVD |

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site Web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé, ou
- révisé.

[1] Les chiffres entre crochets se réfèrent à la Bibliographie.

# INTRODUCTION

Chaque projet implique des risques. Les risques d'un projet peuvent être liés aux objectifs du projet lui-même ou aux objectifs des actifs, produits ou services que crée le projet. Le présent document donne les lignes directrices pour manager les risques au sein d'un projet de façon systématique, efficace, efficiente et cohérente.

Le management du risque comprend les activités coordonnées dans le but de diriger et maîtriser un organisme vis-à-vis du risque. L'ISO 31000, *Management du risque – Lignes directrices*, décrit:

a) les principes pour un management efficace du risque;

b) le cadre qui fournit les fondements et dispositions organisationnelles présidant à la conception, la mise en œuvre, la surveillance, la revue et l'amélioration continue du management du risque au à travers tout l'organisme; et

c) un processus de management du risque applicable à tous les types de risque, pour tout organisme.

Le présent document montre comment ces principes et lignes directrices à caractère général s'appliquent à la gestion de l'incertitude, des menaces et des opportunités dans les projets. Ils s'appliquent à tous les types de projets et de processus de management de projet. Lorsque le présent document est appliqué conjointement avec des processus flexibles ou agiles de management de projet, les objectifs, exigences et spécifications inhérents au projet ont vocation à évoluer à mesure de l'avancée du projet. L'application du présent document peut être ajustée en pareilles circonstances.

Le présent document s'adresse aux individus et organismes concernés par tout ou partie des phases du cycle de vie d'un projet. Il peut également s'appliquer à des sous-projets et à des ensembles de projets et de programmes en interrelation.

L'application du présent document peut être ajustée à chaque projet spécifique, en considérant des facteurs tels que le contexte, les objectifs et les exigences. Par conséquent, il n'est pas dans le domaine d'application du présent document d'imposer une procédure de certification aux praticiens du management du risque.

Les lignes directrices fournies dans le présent document n'ont pas pour objet de remplacer les normes existantes spécifiques à un secteur industriel, même si elles peuvent s'avérer utiles dans ces cas.

## 1 Domaine d’application

Le présent document donne les principes et lignes directrices génériques concernant le management du risque dans les projets. Il présente en particulier une démarche systématique de management du risque s’appuyant sur l’ISO 31000.

Les lignes directrices concernent les principes de management du risque dans les projets, le cadre et les exigences organisationnelles de mise en œuvre du management du risque, et le processus visant à assurer un management efficace du risque.

## 2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu’ils constituent, pour tout ou partie de leur contenu, des exigences 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).

ISO 31000, *Management du risque – Lignes directrices*