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)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

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

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

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

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

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications, symboles graphiques et le glossaire. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

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*

3 Terms and definitions

For the purposes of this document, the following terms or definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

3.1
event
occurrence or change of a particular set of circumstances

Note 1 to entry: An event can have one or more occurrences, and can have several causes and several consequences.

Note 2 to entry: An event can also be something that is expected which does not happen, or something that is not expected which does happen.

Note 3 to entry: An event can be a risk source.

[SOURCE: ISO 31000:2018, 3.5]

3.2
opportunity
combination of circumstances expected to be favourable to objectives

Note 1 to entry: An opportunity is a positive situation in which gain is likely and over which one has a fair level of control.

Note 2 to entry: An opportunity to one party may pose a threat to another.

Note 3 to entry: Taking or not taking an opportunity are both sources of risk.

[SOURCE: IEC 31010:2019, 3.2 [2]]

3.3
project
temporary endeavour to achieve one or more defined objectives

Note 1 to entry: A project generally consists of a set of coordinated and controlled activities (3.1) with start and finish dates, conforming to specific requirements, including the constraints of time, cost and resources.

Note 2 to entry: An individual project can form part of a larger project structure and generally has a defined start and finish date.

Note 3 to entry: In some projects the objectives and scope are updated and the product or service characteristics defined progressively as the project proceeds.

Note 4 to entry: The output of a project can be one or several units of product or service.

Note 5 to entry: The project's organization is normally temporary and established for the lifetime of the project.

Note 6 to entry: The complexity of the interactions among project activities is not necessarily related to the project size.

[SOURCE: ISO 21502:2020, 3.20, modified – The Notes have been taken from ISO 10006:2017, 3.3. [3]]

3.4
project management
coordinated activities to direct and control the accomplishment of agreed objectives

[SOURCE: ISO 21502:2020, 3.24]

3.5
project plan
documented description of the technical and management baselines to be followed for a project

[SOURCE: ISO 21506:2024, 3.68 [4]]

3.6
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

[SOURCE: ISO 31000:2018, 3.1]

3.7
risk management
coordinated activities to direct and control an organization with regard to risk

[SOURCE: ISO 31000:2018, 3.2]

3.8
risk management framework
set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization

Note 1 to entry: The foundations include the policy, objectives, mandate and commitment to manage risk (3.6).

Note 2 to entry: The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.

Note 3 to entry: The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

[SOURCE: ISO Guide 73:2009, 2.1.1 [5]]

3.9
risk management policy
statement of the overall intentions and direction of an organization related to risk management

[SOURCE: ISO 31073:2022, 3.2.2 [6]]

3.10
risk management plan
scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk

Note 1 to entry: Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.

Note 2 to entry: The risk management plan can be applied to a particular product, process and project (3.3), and part or whole of the organization.

[SOURCE: ISO 31073:2022, 3.2.3]

3.11
risk management process
systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk

[SOURCE: ISO 31073:2022, 3.3.1]

3.12
risk treatment
process to modify risk

Note 1 to entry: Risk treatment can involve:

– avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk,

– taking or increasing risk in order to pursue an opportunity,

– removing the risk source,

– changing the likelihood,

– changing the consequences,

– sharing the risk with another party or parties (including contracts and risk financing), and

– retaining the risk by informed decision.

Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

Note 3 to entry: Risk treatment can create new risks or modify existing risks.

[SOURCE: ISO 31073:2022, 3.3.32]

3.13
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.

[SOURCE: IEC 31010:2019, 3.5]

3.14
uncertainty
state, even partial, of deficiency of information related to understanding or knowledge

Note 1 to entry: In some cases, uncertainty can be related to the organization’s context as well as to its objectives.

Note 2 to entry: Uncertainty is the root source of risk, namely any kind of “deficiency of information” that matters in relation to objectives (and objectives, in turn, relate to all relevant interested parties’ needs and expectations).

[SOURCE: ISO 31073:2022, 3.1.3]

3.15
work breakdown structure
decomposition of the defined scope of a project or programme into progressively lower levels consisting of elements of work

[SOURCE: ISO 21502:2020, 3.29]

4 Managing risks in projects

Every project involves uncertainties that can lead to risks. These uncertainties can relate to the objectives of the project itself (for example to complete the project within a specified time frame and budget) or to the requirements of the assets, products or services that the project creates (for example for a product to be safe, dependable and environmentally sustainable).

The consequences that could arise from uncertainty in a project can be beneficial as well as detrimental, so project risk management is directed not only to avoiding or reacting to problems but also to identifying and capturing opportunities. Taking account of project risks contributes to better decisions, better project outcomes and increased value for stakeholders.

This document is relevant to individuals and organizations concerned with any or all phases in the life cycle of projects. To obtain maximum benefit, risk management activities should be initiated at the outset when considering a project, and continued through subsequent phases (see Table 1). However, project risk management can be initiated successfully at any point in the life cycle. It is scalable, so it can be used with both small and large projects and with individual phases of projects. It can also be applied to sub-projects and to sets of inter-related projects and programmes.

Risk management should be integrated with project management activities and processes. It should not be separate or an afterthought.

A typical set of project phases and their characteristics is shown in Table 1. In practice, there can be iteration between the phases.

Table 1 – Typical phases in a project

	Phase 1	Phase 2	Phase 3	Phase 4	Additional activities	
Phase label	Identify Concept	Pre-feasibility Select	Feasibility Design and develop	Deliver Implement Install and commission	Operate and maintain	Abandon Dispose
Purpose	Appraising opportunities: determine whether the project could be worthwhile and its alignment with business strategy	Selecting options: identify and appraise project development options and select the preferred one	Defining the project: finalize the scope and detail of the preferred option	Delivering the project: produce an operating asset, product or service, consistent with the agreed scope	Realising the benefits: evaluate the project outcome to ensure performance	Closure: ensure safe and acceptable closure or disposal
Focus of risk management activities	Strategic threats and opportunities	Risk-based options selection	Design and delivery strategy	Project delivery, test and handover	Operation and maintenance	Disposal and rehabilitation
NOTE The additional activities in the two right-hand columns correspond to phases in the life cycle of an asset, product or service that is created by a project. They are not project phases, but they are included here because they are often considered by project managers as they proceed through phases 1 to 4.						

It is common for each phase to culminate in a decision point (sometimes called a gate) at which executive approval is provided for progression and entry to the next phase. Information on risks and risk management is an important part of the information provided to executives to support their decisions. Information on risks and controls in each phase should also be shared with other teams managing the next phase of the project.

All executives and people in the organizations associated with a project have a role in managing the risks associated with their decisions and activities. This document is intended for use by:

a) project directors and project managers who are part of an organization that owns or commissions the project or that will own or manage the assets, products or services the project will create,

b) members of project teams who are responsible for significant sub-projects, groups of activities or packages of work, and the associated risks,

c) risk managers and members of risk management groups, internal or external to the organization, who are responsible for overseeing, supporting or administering risk management activities in the project,

d) project owners or sponsors who are responsible for ensuring that the sponsoring organization's business interests in the project are maintained and that the expected outcomes and benefits are realized,

e) executives who have to approve the progression of the project at each decision point and the expenditure, resource allocation and objectives associated with the subsequent phase,

f) peer reviewers who provide assurance to the executives who make approval decisions that the supporting information is comprehensive, accurate, valid and reliable,

g) project directors and project managers who are part of a contracting organization, or a sub-contractor or supplier, that bids for or delivers some or all of the project and its associated assets, products or services,

h) financiers and insurers who provide financial and related support for the project,

i) regulators of project-related activities or the assets, products or services that can be created by the project, and

j) other stakeholders, including sub-contractors, suppliers, users or beneficiaries of the assets, products or services that can be created by the project, and other parties who could have an interest in the project and its outcomes (including the wider public).

5 Principles

For project risk management to be effective, efficient and consistent, an organization should at all levels comply with the principles shown below.

a) Risk management creates and protects value.

Risk management contributes to demonstrable progress towards organizational objectives and improvement of performance and quality in projects and the assets, products and services they create. The objectives shall be understood clearly by all parties.

c) Risk management is part of decision-making.

Risk management helps decision makers make informed choices about the project, within each stage of its life, prioritize actions and distinguish among alternative courses of action. This implies that all decisions should consider risk.

d) Risk management is an integral part of all organizational processes associated with a project.

Risk management is not a stand-alone activity that is separate from the main activities and processes of the project or the organization. Risk management is part of the responsibilities of project managers and of staff at all levels. It is an integral part of all the organizational processes associated with a project, including strategic project and investment planning, project management and management of project change.

e) Risk management explicitly addresses uncertainty.

All people in the organization should explicitly take account of uncertainty, the nature of that uncertainty, and how it can be addressed, particularly in critical processes.

f) Risk management is systematic, structured and timely.

A systematic, timely and structured approach to risk management contributes to consistent, comparable and reliable project decisions and their successful application, to the efficiency and effectiveness of project management processes and to the benefits the project aims to deliver. A sound framework for risk management should be applied from the beginning of a project.

g) Risk management is based on the best available information.

The inputs to the process of managing risk in a project are based on information sources such as technical and engineering analyses, physical site and equipment inspections, test results and progress reports, supplemented with historical data, experience, stakeholder feedback, forecasts and expert judgement. However, those involved with managing risks in a project should inform themselves of, and should take into account, any limitations of the data or modelling used, uncertainty in the information available or the possibility of divergence among experts.

h) Risk management is tailored.

Risk management activities are adapted to the kind of project, the project's external and internal context and those of the organizations involved, and the level of uncertainty and complexity associated with the project. The level of risk management effort is proportionate to the situation.

i) Risk management takes human and cultural factors into account.

The capabilities, perceptions and intentions of people and organizations that can facilitate or hinder achievement of the project's objectives are taken into account when managing risk, as are social and organizational changes brought about by the project.

j) Risk management is transparent and inclusive.

Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up to date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

k) Risk management is dynamic, iterative and responsive to change.

As a project progresses and as related external and internal events occur, context and knowledge change, monitoring and review take place, new risks emerge, some risks change, and other risks disappear. Therefore, risk management activities in a project help project decision-makers to continually identify, understand and respond to change.

l) Risk management facilitates continual improvement of the organization.

Organizations should develop and implement strategies to improve the maturity of their project risk management alongside all other aspects of their organizational processes.

6 Project risk management framework

6.1 General

Project risk management processes should be integrated with project management processes. The project management framework – the way in which the project management process will be organized, structured and controlled – should provide the foundations and arrangements that will embed project risk management throughout the project through all phases, at all levels and across all the organizations involved. The success of project risk management will depend in part on the effectiveness of the integration.

The project risk management framework assists in managing project risks. It does this through consistent and effective project risk management processes (see Clause 7), applied at varying levels and within the specific context of the project. The framework and processes ensure that information about project risk is adequately reported and used as a basis for governance, decision making and accountability at all relevant organizational and project levels. Organizations often adopt a common risk management framework, aligned with their corporate risk management framework, and they customize it in a similar way in many projects.

This Clause 6 describes the necessary components of the framework for managing project risk and the way in which they interrelate in an iterative manner. Figure 1 shows the risk management framework and process in ISO 31000 applied to managing risk in projects.

This framework is not intended to prescribe a management system, but rather to assist the organizations involved in a project to integrate project risk management into the overall project management framework. Therefore, organizations should adapt the components of the framework to their specific needs and the specific project requirements.

If an organization's existing project management practices and processes include components of risk management, or if the organization has already adopted a formal project risk management process for particular types of projects, risks or situations, then these should be critically reviewed and assessed against this document to determine their adequacy and effectiveness.

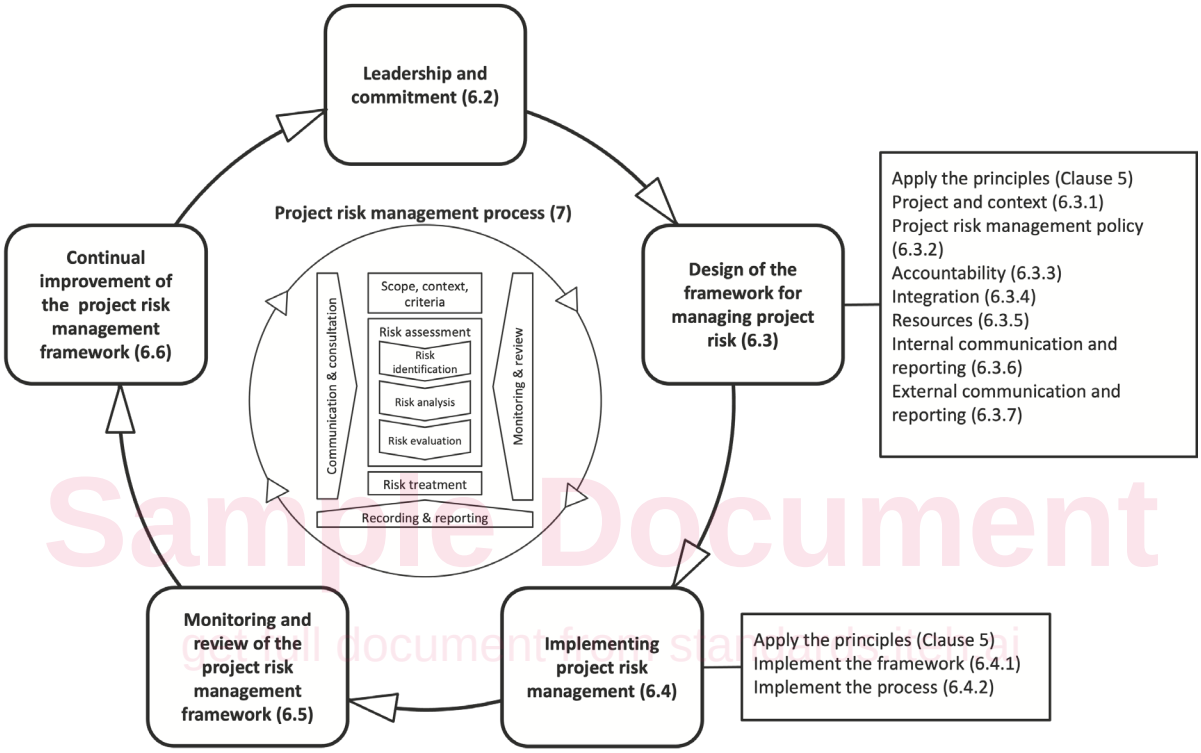

Figure 1 – Relationship between the components of the framework for managing risk, adapted from ISO 31000

6.2 Leadership and commitment

The introduction of risk management and ensuring its on-going effectiveness require sustained commitment by management of all the organizations involved in the project, including owners and key contractors. Strategic and rigorous planning is also necessary to achieve commitment at all levels. Management of owner, contractor and major sub-contractor or supplier organizations should:

a) define and endorse a common risk management policy for the project,

b) ensure that the cultures of the participating organizations and the project risk management policy are aligned as far as possible,

c) align project risk management objectives and criteria with the objectives and strategies of the organizations involved, and particularly those of the owner organization,

d) determine project risk management performance indicators that align with performance indicators for the project itself and the organizations involved,

e) inform employees about any legal, regulatory and organizational requirements that apply, and assess their understanding of those requirements,

f) assign accountabilities and responsibilities at appropriate levels within the organization structures and within the project organization,