IEC 62198

Edition 2.0 2013-11

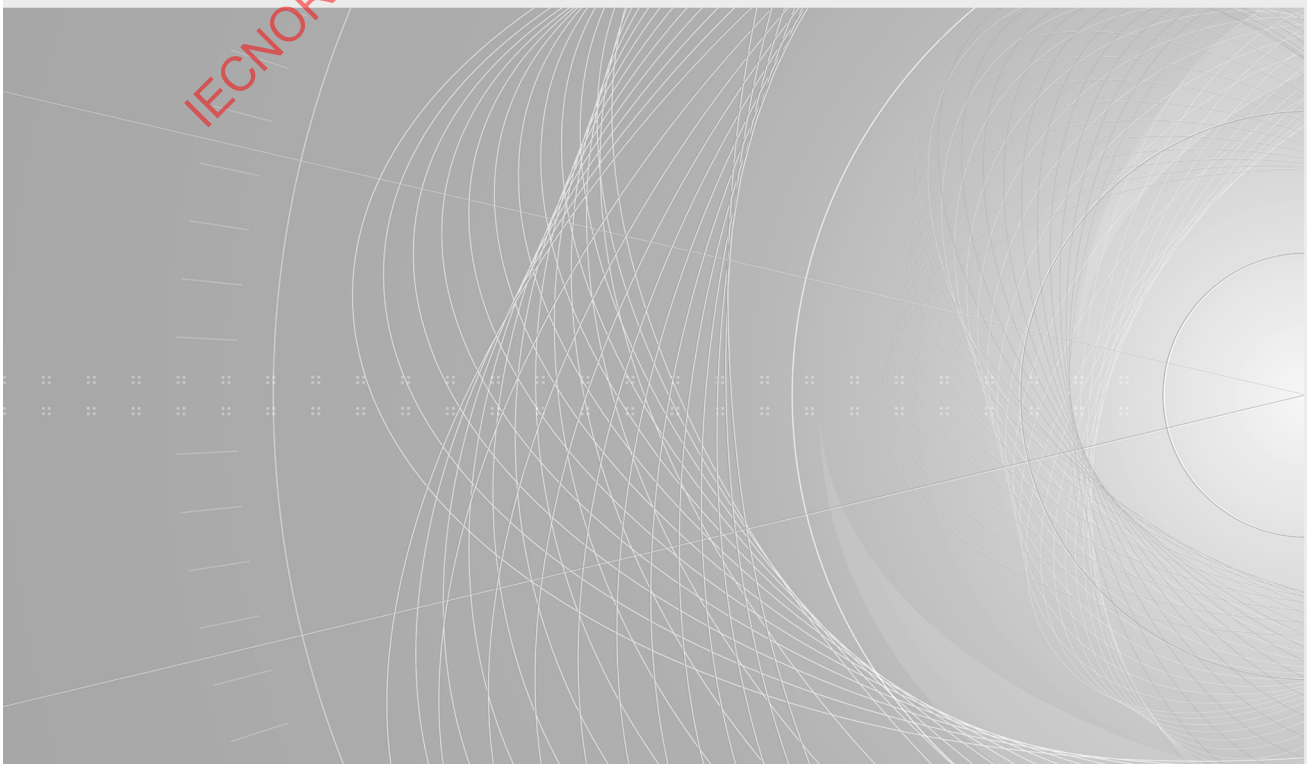
INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Managing risk in projects – Application guidelines

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



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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you 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It also gives information on projects, replaced and withdrawn publications.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 on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

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: csc@iec.ch.

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.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI 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.

Just Published CEI - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

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

IEC 62198

Edition 2.0 2013-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Managing risk in projects – Application guidelines

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX X

ICS 03.100.01

ISBN 978-2-8322-1192-2

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) 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 62198 has been prepared by IEC technical committee 56: Dependability.

This second edition cancels and replaces the first edition, published in 2001, and constitutes a technical revision.

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

a) major restructure and rewrite of the first version;

b) now aligned with ISO 31000, *Risk management – Principles and guidelines.*

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

FDIS	Report on voting
56/1529/FDIS	56/1539/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.

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 stability 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, or
- amended.

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

INTRODUCTION

Every project involves uncertainty and 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 International Standard provides guidelines for managing risks in a project in a systematic and consistent way.

Risk management includes the coordinated activities to direct and control an organization with regard to risk. ISO 31000, *Risk management – Principles and guidelines*, describes the principles for effective risk management, the framework that provides the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout an organization and a process for managing risk that can be applied to all types of risk in any organization. This standard shows how those general principles and guidelines apply to managing uncertainty in projects.

This standard 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 standard needs to be tailored to each specific project. Therefore, it is considered inappropriate to impose a certification system for risk management practitioners.

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

MANAGING RISK IN PROJECTS – APPLICATION GUIDELINES

1 Scope

This International Standard provides principles and generic guidelines on managing risk and uncertainty in projects. In particular it describes a systematic approach to managing risk in projects based on ISO 31000, *Risk management – Principles and guidelines*.

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.

This standard is not intended for the purpose of certification.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 – Principles and guidelines*

3 Terms and definitions

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

3.1
project
unique process consisting of a set of coordinated and controlled activities, with start and finish dates, undertaken to achieve an objective conforming to specific requirements, including the constraints of time, cost and resources

Note 1 to entry: An individual project may form part of a larger project structure.

Note 2 to entry: In some projects the objectives are updated and the product characteristics defined progressively as the project proceeds.

Note 3 to entry: The project's product is generally defined in the project scope. It may be one or several units of product and may be tangible or intangible.

Note 4 to entry: The project's organization is normally temporary and established for the lifetime of the project.

Note 5 to entry: The complexity of the interactions among project activities is not necessarily related to the project size.

[SOURCE: ISO 10006:2003, 3.5] [1][1]

3.2
project management
planning, organizing, monitoring, controlling and reporting of all aspects of a project and the motivation of all those involved in it to achieve the project objectives

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

[SOURCE: ISO 10006:2003, 3.6]

3.3
project management plan
document specifying what is necessary to meet the objective(s) of the project

Note 1 to entry: A project management plan should include or refer to the project's quality plan.

Note 2 to entry: The project management plan also includes or references such other plans as those relating to organizational structures, resources, schedule, budget, risk management (3.5), environmental management, health and safety management and security management, as appropriate.

[SOURCE: ISO 10006:2003, 3.7]

3.4
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected — positive and/or negative.

Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project (3.1), product and process).

Note 3 to entry: Risk is often characterized by reference to potential events and consequences, or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to understanding or knowledge of an event, its consequence, or likelihood.

[SOURCE: ISO Guide 73:2009, 1.1] [2]

3.5
risk management
coordinated activities to direct and control an organization with regard to risk

[SOURCE: ISO Guide 73:2009, 2.1]

3.6
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 (3.4).

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]

3.7
risk management policy
statement of the overall intentions and direction of an organization related to risk management

[SOURCE: ISO Guide 73:2009, 2.1.2]

3.8
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 (3.1), and part or whole of the organization.

[SOURCE: ISO Guide 73:2009, 2.1.3]

3.9
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 Guide 73:2009, 3.1]

3.10
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 Guide 73:2009, 3.8.1]

4 Managing risks in projects

Every project involves uncertainty that can lead to risk. These risks 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 the stakeholders.

This standard 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 are initiated at the earliest possible phase of a project and continued through subsequent phases. However, project risk management can be initiated successfully at any point in the life cycle, providing appropriate preliminary work is undertaken. The process is scalable, so it can be

used with both small and large projects and to individual phases of projects. It can also be applied to sub-projects and to sets of inter-related projects and programmes.

A typical set of project phases and their characteristics is shown in Table 1.

Table 1 – Typical phases in a project

Phase	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6
Phase label	Identify Concept	Select pre-feasibility	Design and develop feasibility	Deliver Implement Install	Operate and maintain	Abandon Dispose
Purpose	Appraising opportunities: determine whether the project could be worthwhile and 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 or service, consistent with the agreed scope	Realising the benefits: evaluate the project outcomes to ensure performance	Closure: ensure safe and acceptable closure
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

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 at each decision point. Information on risks and controls in each phase should also be handed over to the team managing the next phase of the project.

All executives and managers in the organizations associated with a project have a role in managing the risks associated with their decisions (Figure 1). This standard 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;

c) 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 realised;

d) executives who have to approve the progression of the project through each gate and the expenditure associated with the subsequent phase;

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

f) 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;

g) financiers and insurers who provide financial and related support for the project;

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

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

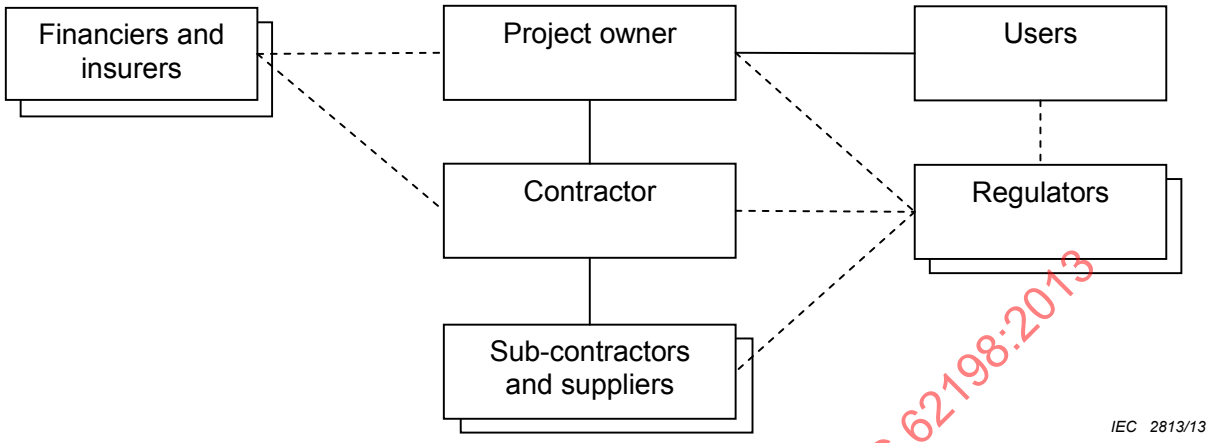


Figure 1 – Principal stakeholders in a project

5 Principles

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

a) Risk management creates and protects value

Risk management contributes to the demonstrable achievement of 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.

b) 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.

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 explicitly addresses uncertainty

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

e) Risk management is systematic, structured and timely

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

f) 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.

g) 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.

h) 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.

i) 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.

j) 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.

k) 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 through the application of the consistent and effective project risk management process (see Clause 7) at varying levels and within the specific context of the project. The framework ensures that information about project risk derived from these processes is adequately reported and used as a basis for decision making and accountability at all relevant organizational and project levels.

This clause describes the necessary components of the framework for managing project risk and the way in which they interrelate in an iterative manner. Figure 2 shows the risk management framework specified 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 standard to determine their adequacy and effectiveness.

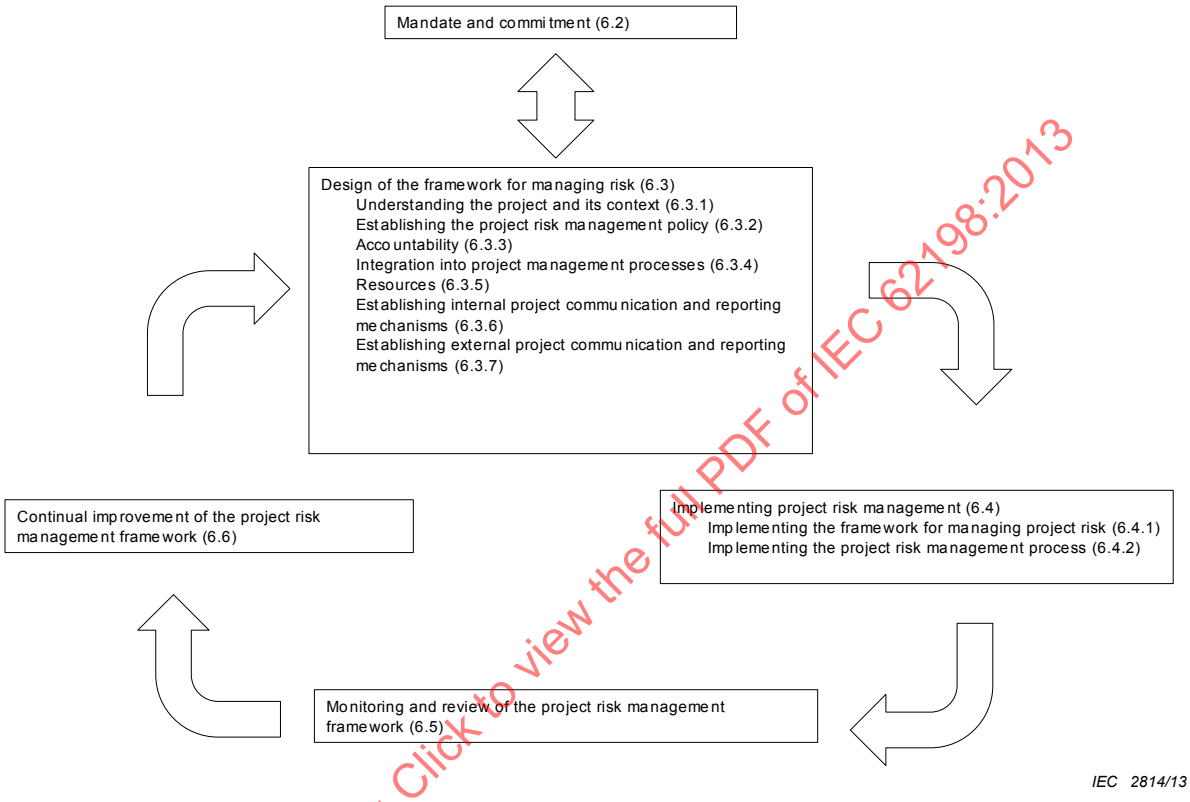


Figure 2 – Relationship between the components of the framework for managing risk, adapted from ISO 31000

6.2 Mandate and commitment

The introduction of risk management and ensuring its on-going effectiveness require strong and sustained commitment by management of all the organizations involved in the project, including owners and key contractors, as well as strategic and rigorous planning 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 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) ensure legal and regulatory compliance,

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

g) ensure that the necessary resources are allocated to project risk management,

h) ensure systems are in place to provide necessary resources in a timely manner,

i) communicate the benefits of risk management to all project stakeholders, and

j) ensure that the framework for managing risk continues to remain appropriate as the project progresses through the phases in its life cycle.

In some instances requirements for risk management can be included in contracts.

6.3 Design of the framework for managing project risk

6.3.1 Understanding the project and its context

Before starting the design and implementation of the framework for managing risk, it is important to evaluate and understand both the external and internal context of the project, since these can significantly influence the design of the framework.

Evaluating the project's external context can include, but is not limited to

a) the social and cultural, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local,

b) key drivers and trends having impact on the objectives or conduct of the project, and

c) relationships with, and perceptions and values of, external stakeholders, including all the organizations associated with the project (Figure 1).

Evaluating the project's internal context can include, but is not limited to

d) the purpose and objectives of the project and the way they align with the purpose and objectives of the project owner and the users of the asset, products or services the project creates,

e) governance, organizational structures, roles and accountabilities for the project and its performance,

f) policies, objectives and the strategies that are in place to achieve them,

g) capabilities of the organizations associated with the project, including the availability and capability of their resources and knowledge (e.g. capital, time, people, processes, systems and technologies),

h) information systems, information flows and decision-making processes (both formal and informal), and particularly the information systems that are to be used to support project management, control and reporting,

i) relationships between, and perceptions and values of, internal stakeholders,

j) standards, guidelines and models adopted by the organizations for the project, and

k) the form and extent of the contractual relationships between the parties.

6.3.2 Establishing the project risk management policy

The project risk management policy should clearly state the objectives for, and commitment to, risk management within all the main organizations associated with the project. The policy typically addresses the following:

a) the rationale for managing risk in the project;

b) links between the organizations' objectives and policies and the project risk management policy;

c) accountabilities and responsibilities for managing project risk in all of the organizations involved;

d) the way in which conflicting interests are dealt with;

e) commitment to make the necessary resources for risk management available to assist those accountable and responsible for managing risk;

f) the way in which project risk management performance will be measured and reported, and how it will be linked to overall project performance; and

g) commitment to review and improve the project risk management policy and framework periodically and in response to events or changes in circumstances as the project progresses.

The risk management policy should be communicated appropriately to project stakeholders.

The risk management policy for a particular project can be part of the organization's broader set of policies.

6.3.3 Accountability

Accountability refers to the obligation to deliver specific commitments and outcomes. The organizations involved in a project should ensure that there is accountability, authority and appropriate competence for managing risk across the project and in all of its phases. This should include implementing and maintaining the project risk management process and ensuring the adequacy, effectiveness and efficiency of any controls. This can be facilitated by

a) identifying the organizations and individual risk owners within them who have the accountability and authority to manage project risks,

b) identifying who is accountable for the development, implementation and maintenance of the framework for managing project risk,

c) identifying other responsibilities of people at all levels in each organization for the project risk management process,

d) establishing performance measures and external and internal reporting and escalation processes for risks in projects.

In most projects a project manager is appointed with a specific mandate and delegated authorities, commonly including responsibility for project risk management. Depending upon the size and complexity of the project, risk management tasks can be performed by the project manager or can be delegated. The tasks include:

1) defining responsibilities for managing risks associated with different project activities;

2) establishing communication mechanisms within the project and coordinating risk management information and activities;

3) establishing the context for project risk management process;

4) managing and reporting risk assessment activities;

5) recommending, initiating, allocating responsibilities for and monitoring the effective implementation of risk treatment activities;

6) seeking executive decisions on conflicting risk issues;

7) communicating information about risk issues in an appropriate and timely fashion throughout the project;

8) ensuring contingency plans are in place;

9) identifying and recording any problems relating to the management of risk;

10) monitoring the risk management process and implementing corrective action where necessary;

11) providing documentation to ensure traceability.

The authority for project risk management and interfaces with other functions should be defined and documented. The main accountabilities that cross organizational boundaries should be specified in contract documents.

6.3.4 Integration into project management processes

Risk management should be embedded in all project management practices and processes in a way that it is relevant, timely, effective and efficient. The project risk management process should become an integrated part of, and not separate from, those project management processes.

Risk management should also be embedded into broader organizational processes, including the project policy development, business and strategic planning and review, and change management processes.

There should be a project risk management plan to ensure that the risk management policy is implemented and that risk management is embedded in all of project management practices and processes. The project risk management plan can be integrated into other project plans, such as the project execution plan for a project phase.

6.3.5 Resources

The organizations involved in a project should allocate appropriate resources for project risk management.

Consideration should be given to the following:

a) people, skills, experience and competence;

b) resources needed for each step of the project risk management process;

c) the risk processes, methods, tools and supporting systems to be used for managing project risk;

d) documented project management processes and procedures;

e) information and knowledge management systems;

f) training programmes; and

g) contractual allocation of risk between the organizations involved.

The project budget should take into account the cost of the risk management function, and the cost of risk treatment activities.

6.3.6 Establishing internal project communication and reporting mechanisms

The organizations involved in a project should establish project communication and reporting mechanisms that support and encourage ownership of risk at each phase of the project life. These mechanisms should ensure that:

a) key components of the project risk management framework, and any subsequent modifications, are communicated appropriately;

b) there is adequate reporting on the project risk management framework, its effectiveness and the outcomes;

c) relevant information derived from the application of project risk management is available at appropriate levels and times and across all the organizations involved, including between phases as the project progresses; and

d) there are processes for consultation with stakeholders.

These mechanisms should include processes to consolidate project risk information where appropriate from a variety of sources, taking into account its sensitivity. In most circumstances, project risk management reporting should be integrated with regular project management reports.

6.3.7 Establishing external project communication and reporting mechanisms

The organizations involved in a project should develop and implement a coordinated plan for how they will communicate with external stakeholders. This should involve:

a) engaging appropriate external stakeholders and ensuring an effective exchange of information about the project;

b) external reporting to comply with legal, regulatory, and governance requirements;

c) providing feedback and reporting on communication and consultation;

d) using communication to build confidence in the organizations involved; and

e) communicating with stakeholders in the event of a crisis or contingency.

These mechanisms should include processes to consolidate project risk information where appropriate from a variety of sources in a timely manner, taking into account its sensitivity. In most circumstances, external communication should be coordinated and controlled by the project owner, unless there are specific regulatory requirements for contractors and suppliers.

6.4 Implementing project risk management

6.4.1 Implementing the framework for managing project risk

In implementing the framework for managing project risk, the organizations involved in a project should

a) define the appropriate timing and strategy for implementing the framework in the project, taking advantage where possible of synergies with each organization's own risk management policies and processes,

b) integrate the project risk management policy and process into project management processes,

c) comply with legal and regulatory requirements,

d) ensure that project decision-making, including the development and setting of objectives, is aligned with the outcomes of project risk management processes,

e) hold information and training sessions, and

f) communicate and consult with stakeholders to ensure that the project risk management framework remains appropriate.

6.4.2 Implementing the project risk management process

Project risk management should be implemented by ensuring that the project risk management process outlined in Clause 7 is applied through a project risk management plan (see 7.7.2) at all relevant levels and functions of the organizations involved as part of their project management practices and processes.

The project risk management plan should be developed early in the project and should be integrated into the project management plan. The scope of risk management processes and the amount of effort that should be put in at different stages of the project should be defined.

6.5 Monitoring and review of the project risk management framework

In order to ensure that project risk management is effective and continues to support project performance, the organizations involved in a project should

a) measure project risk management performance against indicators that are reviewed periodically for appropriateness and aligned with project performance indicators,

b) periodically measure progress against, and deviation from, the project risk management plan,

c) periodically review whether the project risk management framework, policy and plan are still appropriate, given the project's external and internal context and progress in the current project phase,

d) report on project risk, progress with the project risk management plan and how well the project risk management policy is being followed, as part of regular project reporting, and

e) review the effectiveness of the project risk management framework.

Performance indicators for risk management can relate to

– project success indicators that measure the extent to which objectives are achieved,

– process indicators that measure the extent to which risk management processes are followed, and

– risk indicators that measure how effectively treatments are being actioned.

6.6 Continual improvement of the project risk management framework

Based on results of monitoring and reviews, decisions should be made on how the project risk management framework, policy and plan can be improved. These decisions should lead to improvements in the management of project risk and the project risk management culture. A formal 'lessons learned' process can provide supporting information for this.

7 Project risk management process

7.1 General

The project risk management process should be

– an integral part of project management,

– embedded in the culture and practices of the organizations involved with a project, and

– tailored to and integrated with the business and project management processes of the organizations involved.

It comprises the activities described in 7.2 to 7.7. The project risk management process is shown in Figure 3.

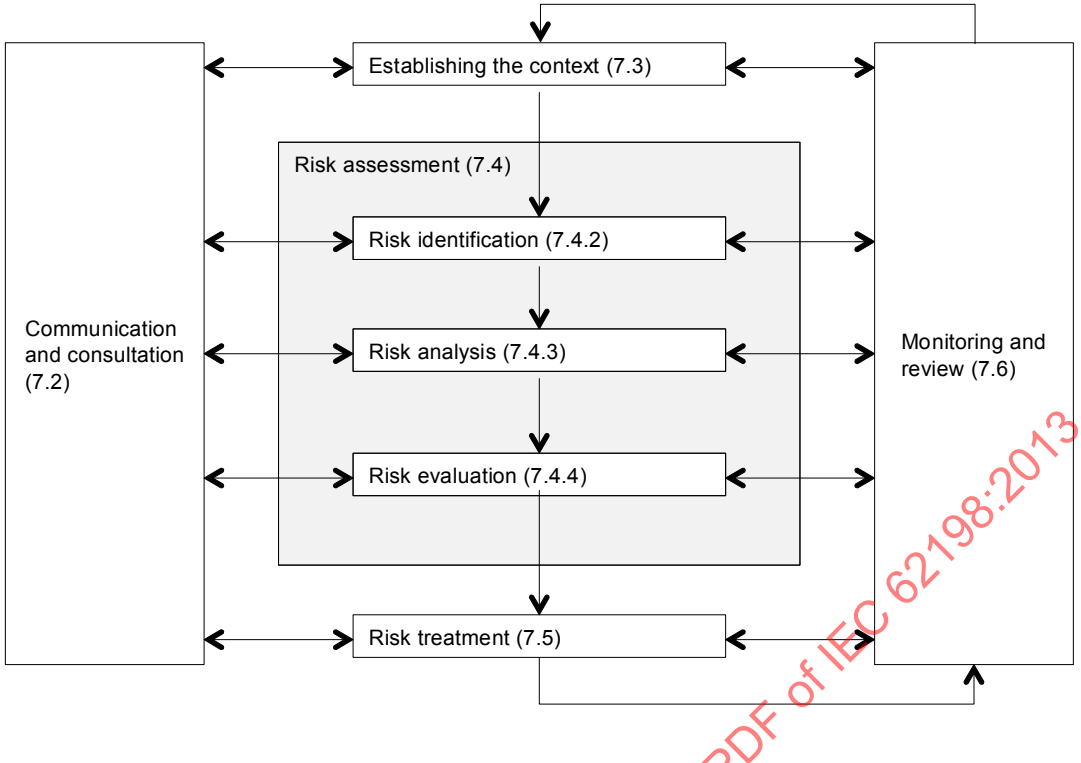


Figure 3 – Project risk management process, adapted from ISO 31000

7.2 Communication and consultation

Communication and consultation with external and internal stakeholders should take place during all stages of the project risk management process. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the project risk management process and relevant stakeholders understand the purpose and objectives of the project risk management process, the basis on which project risk information is incorporated into project decisions, and the reasons why particular actions are required.

Communication and consultation with stakeholders is important as they make judgements about risk based on their perceptions of risk. These perceptions can vary due to differences in their culture, values, needs, assumptions, concepts and concerns. As their views can have a significant impact on the decisions to be made, the stakeholders' perceptions should be identified, recorded, and taken into account in the decision making process.

Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information, taking into account confidential and personal integrity aspects.

The outcomes from communication and consultation between the main organizations involved in a project (Figure 1) can be reflected in various documents, including contracts, memoranda of understanding and heads of agreement, and in agreed allocations of responsibilities for specific risks and controls to individuals and participating organizations.

Plans for communication and consultation should be developed at an early project phase.

A consultative team approach can

a) help establish the context appropriately,

b) ensure that the interests of project stakeholders are understood and considered,

c) help ensure that risks are adequately identified,

d) bring different areas of expertise together for analysing risks,

e) ensure that different views are appropriately considered when defining risk criteria and in evaluating risks,

f) secure endorsement and support for a treatment plan,

g) enhance appropriate change management during the project risk management process, and

h) develop an appropriate external and internal communication and consultation plan.

Effective risk management relies on the timely availability of information from various areas over the life of the project. Interfaces and lines of communication should be formally established and maintained between project risk management and areas such as

1) design and development,

2) commercial and project control functions,

3) configuration control,

4) quality and dependability,

5) post-project support, including support for users and maintainers.

These interfaces should be defined at a sufficient level of authority and detail that a rapid reaction is possible.

7.3 Establishing the context

7.3.1 General

By establishing the context, the organizations involved in the project articulate their objectives and define the external and internal parameters to be taken into account when managing project risk. The context needs to be understood in order to set the scope, risk criteria and structure for steps in the project risk management process that follow.

While many factors here are similar to those addressed in the design of the project risk management framework (see 6.3), when establishing the context for the project risk management process they should be considered in greater detail. Their implications and how they relate to the scope of the project and the project management process are particularly important.

7.3.2 Establishing the external context

The external context is the external environment in which the project will be undertaken.

Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing project risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the project.

The external context can include, but is not limited to

– the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment of the project, whether international, national, regional or local,

– key drivers and trends having an impact on project objectives, and

– relationships with, perceptions and values of external stakeholders.

7.3.3 Establishing the internal context

The internal context is the internal environment in which the organizations involved in the project seek to achieve project objectives. It is anything within the organizations that can influence the way in which risk will be managed in the project. It should be established because

– project risk management takes place in the context of the objectives the organizations have for the project,
– the project risk management process should be aligned with the organizations' cultures, processes, structures and strategies, and
– some organizations fail to recognize opportunities to achieve their strategic, project or business objectives, and this affects continuing commitment, credibility, trust and value.

The internal context can include, but is not limited to

a) governance, organizational structures, roles and accountabilities,
b) policies, objectives, and the strategies that are in place to achieve them,
c) capabilities and resources, such as capital, time, people, processes, systems, technologies, expertise and knowledge,
d) relationships with, perceptions and values of internal stakeholders,
e) information systems, information flows and decision making processes (both formal and informal),
f) standards, guidelines and models adopted by the organizations, and
g) the form and extent of contractual and other relationships between the organizations involved.

7.3.4 Establishing the context of the project risk management process

The objectives, scope and deliverables of the project, or those parts of the project where the risk management process is being applied, should be established. The management of project risk should be undertaken with full consideration of the need to justify the resources used in carrying out risk management. The resources required, responsibilities and authorities, and the records to be kept should also be specified.

The context of the risk management process will vary according to the needs of the project. It can involve, but is not limited to

a) defining the project in terms of the activities and processes to be undertaken, the assets, products or services to be created, the resources to be committed, and the cost, time and location,
b) identifying and specifying the decisions that have to be made,
c) defining the scope, as well as the depth and breadth of the project risk management activities to be carried out, including specific inclusions and exclusions and, where appropriate, the kinds of risks to be addressed,
d) defining the relationships between the specific project and other projects, processes or activities of the organizations involved,
e) defining the goals and objectives of the project risk management activities,
f) defining responsibilities for and within the project risk management process,
g) identifying any scoping or framing studies needed, their extent and objectives, and the resources required for such studies,
h) defining project risk assessment methodologies,
i) defining the method for evaluating the performance and effectiveness of the risk management process.

Attention to these and other relevant factors should help ensure that the risk management approach adopted is appropriate to the circumstances, to the project and to the risks affecting the achievement of project objectives.

7.3.5 Defining risk criteria

The organizations involved in a project should agree criteria to be used to evaluate the significance of risk. The criteria should reflect the organizations' values and objectives in relation to the project. Some criteria can be imposed by, or derived from, legal and regulatory requirements, or by policies or other requirements to which the organizations subscribe. Risk criteria should be consistent with the project risk management policy (see 6.3.2), be defined at the beginning of the project risk management process and be reviewed regularly.

When defining risk criteria, factors to be considered should include the following:

a) the nature and types of causes or sources of risk, and how likelihood will be defined;

b) the nature and types of consequences that can occur and how their impacts will be measured;

c) the time frames within which the consequences could arise;

d) how the level of risk is to be determined;

e) the level at which risk becomes acceptable or tolerable; and

f) whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

The views of stakeholders should be considered when setting criteria.

Measures for the impact of risks should take into account all project objectives, which can relate to

1) commercial and business objectives of the organizations involved in the project,

2) achievement of cost and schedule targets for the project,

3) quality, dependability and performance of the assets, products or services the project creates,

4) health and safety of project stakeholders,

5) environmental protection and enhancement, and

6) statutory and regulatory compliance.

Criteria for acceptability and tolerability of risks should be developed. These are used for evaluating the risks in later stages of the process.

7.3.6 Key elements

To provide more confidence that risk identification is comprehensive and no important risks are overlooked, it is common to divide the project into a set of key elements that are used to organize the risk identification activity.

There are many ways of generating a key element structure, depending on the nature of the project and the purpose, scope and setting of the assessment. For example, key elements can be based on one or more of the following:

a) the project work breakdown structure (WBS), a general risk breakdown structure, functional breakdown structure, deliverables breakdown structure or cost breakdown structure for the project;

b) the remaining phases of the project life;

c) the main headings for the project information to be provided to decision-makers at the next stage-gate;

d) components of an asset, product or service to be created by a project;

e) areas of a project site;

f) contracts and sub-contracts, or contract clauses;

g) components of an organizational structure.

The key element structure allows those performing risk identification to focus their thoughts on each key element in turn and go into more depth than they would if they tried to deal with the whole project at once. A well-designed set of key elements will stimulate creative thought.

Development of key elements also helps identify whether there are any areas of special expertise needed to understand specific elements, allowing that expertise to be included in the risk identification team when it deals with that element.

7.4 Risk assessment

7.4.1 General

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. Its purpose is to identify risks that could affect project objectives, in a positive or negative way, understand how they could occur and develop priorities for attending to them.

7.4.2 Risk identification

The purpose of risk identification is to find, list and characterize risks that can affect the achievement of agreed project objectives, either positively or negatively.

Risk identification should consider sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events, circumstances or changes that could create, enhance, prevent, degrade, accelerate or delay the achievement of project objectives. It is also important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage cannot be included in the analysis until a further iteration is undertaken.

Risk identification should consider the impact of risks upon all project objectives.

Effective project risk management is fundamentally dependent upon the comprehensive identification of risks. This requires a systematic process.

There are many methods for risk identification. Tools and techniques should be selected that are best suited to the project objectives, organizational capabilities and the kinds of risks expected. These can include

a) brainstorming within the key element structure,

b) expert opinion,

c) interviews and questionnaires,

d) check lists,

e) historical data,

f) previous experience of participants and from other projects,

g) testing and modelling,

h) formal techniques such as failure modes and effects analysis (FMEA) or hazard and operability studies (HAZOP).

Identification should include risks whether or not their source is under the control of any of the organizations involved in the project, and whether or not the risk source or cause is immediately evident. Risk identification should include examination of the cascade and

cumulative effects of particular consequences. All significant causes and consequences should be considered.

Relevant and up-to-date information is important in identifying risks. This should include appropriate background information where possible. People with appropriate knowledge should be involved in identifying risks. All practicable information sources should be used when identifying risks.

The focus of risk identification varies according to the phase of the project. In the early phases, risk identification is often directed to high-level, general and strategic risks and the identification of 'fatal flaws' that can make successful project completion infeasible. In later project phases, risk identification focuses on specific risks in far greater detail.

Risk identification should consider the remaining phases in the project life cycle, and the life cycle of the asset, product or service the project delivers. Stakeholders and technical experts with relevant knowledge about these matters should be involved in the risk identification process.

As a project progresses, some risks will be resolved and new ones will arise, so risk identification should be a continuing process. Some risks identified in early project phases remain relevant in later phases; it is important that such risks are retained as the project progresses.

Risks should be recorded. This is normally in a project risk register (see 7.7.4).

7.4.3 Risk analysis

Risk analysis involves developing an understanding of each risk, its causes and consequences and how and why they could occur. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk analysis can also provide an input to decisions where choices have to be made and the options involve different types and levels of risk.

Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences for project objectives, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified. Existing project controls and their effectiveness and efficiency should be taken into account.

A risk can have multiple consequences that relate to several project objectives.

The way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk should reflect the type of risk, the information available and the purpose for which the risk assessment output is to be used. These should all be consistent with the risk criteria. It is also important to consider the interdependence of different risks and their sources.

The confidence in determination of the level of risk and its sensitivity to preconditions and assumptions should be considered in the analysis, and communicated effectively to decision makers and, as appropriate, other stakeholders. Factors such as divergence of opinion among experts, uncertainty, availability, quality, quantity and continuing relevance of information, or limitations on modelling should be stated and can be highlighted.

Risks can be analysed with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data and resources available. It can be necessary to re-visit the risk identification process during risk analysis to further clarify project risks.

Analysis can be qualitative or quantitative, or a combination of these, depending on the circumstances. Qualitative and quantitative analysis approaches can be used in all phases of

the project, but they make different contributions in different phases. For example, qualitative risk analysis can be undertaken early in the project life cycle to support strategic decisions, and quantitative risk analysis can be applied later to support the development of detailed cost and time budgets. Further analyses of uncertainty in such areas as dependability and life cycle cost can be undertaken as part of the selection of project options and detailed design at relevant phases of the project.

7.4.4 Risk evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.

Risk evaluation involves comparing the outcomes of the analysis with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

Evaluation can involve balancing a range of different kinds of risks with both positive and negative outcomes, in order to make decisions about such matters as whether or not a project should proceed or what approach to follow within a project.

In some circumstances, the risk evaluation can lead to a decision to undertake further analysis. For example, in the early phases of a project, risk analysis can assist in developing work plans for investigations and studies to be undertaken in subsequent phases.

7.5 Risk treatment

7.5.1 General

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide new controls or modify existing ones.

Some risks can be accepted without treatment in any way other than maintaining existing controls. These risks should be included in the project risk register so that effective monitoring can be carried out. Risks that are not accepted should be treated.

Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organization that benefits from the risk. Decisions should be made in accordance with legal, regulatory and other requirements.

Risk treatment follows a cyclical process: following initial treatment actions, risks are reassessed to see whether they are acceptable with the new treatments and, if not, further treatment is undertaken.

7.5.2 Selection of risk treatment options

Risk treatment options can include the following:

a) avoiding a risk with negative consequences by removing the source of risk or deciding not to start or continue with the activity that gives rise to the risk (or even discontinuing the project);

b) engaging in an activity that can lead to risks with positive consequences in order to pursue an opportunity (including changing the project scope or objectives);

c) taking an action that changes the likelihood of the risk, to enhance the likelihood of positive consequences and reduce the likelihood of negative ones;

d) taking an action that changes the consequences of the risk, to enhance the size of positive consequences and reduce the size of negative ones;

e) sharing the risk with another party or parties (including through contracts, insurance or risk financing); and

f) retaining the risk by informed decision.

Decisions about risk treatment follow a simple sequence:

1) if the consequences of a risk breach legal or regulatory requirements, action is required;
2) if the consequences of a risk breach organizational policy or exceed risk criteria developed when establishing the context, action is generally required;
3) if the consequences of a risk have adverse implications for the health and safety of people, then risk treatment must be undertaken and the appropriate criterion for selecting treatment tasks is 'as low as reasonably practicable' (ALARP);
4) in all other circumstances, actions should be undertaken only if the aggregate benefits and advantages for the project exceed the aggregate costs and disadvantages, taking into account all the advantages and disadvantages across the entire project.

Risk treatment options are not necessarily mutually exclusive, nor do they all apply to only one risk. A number of treatment options can be considered and applied either individually or in combination. The project can often benefit from the adoption of a combination of treatment options.

When selecting risk treatment options, the values and perceptions of stakeholders and the most appropriate ways to communicate with them can be important practical considerations. Though equally effective for the project, some risk treatments can be more acceptable to some stakeholders than to others.

The implementation of risk treatment actions can introduce new risks that should also be considered. Such secondary risks should be assessed, treated, monitored and reviewed.

7.5.3 Risk treatment plans

The purpose of risk treatment plans is to document the selected treatment options and how they will be implemented. The information provided in treatment plans should include:

a) the reasons for selection of treatment options, including expected benefits to be gained;
b) those who are accountable for approving the plan and those responsible for implementing the plan;
c) proposed actions and their priority;
d) resource requirements including contingencies;
e) performance measures and constraints;
f) reporting and monitoring requirements; and
g) timing and schedule.

For each risk treatment a person should be nominated to have responsibility for that treatment (the task owner). The most appropriate person could be:

1) the person who is responsible for the activity from which the risk arises;
2) the person who can best control the likelihood of the risk occurring;
3) the person best positioned to respond the occurrence of the risk or change its consequences;
4) the person with the appropriate level of authority to deal with the risk.

Treatment plans should be integrated with the project management plan.

7.6 Monitoring and review

Monitoring and review should be a planned part of the project risk management process and integrated with other aspects of regular project monitoring and control.

Responsibilities for monitoring and review should be clearly defined.

Monitoring and review should encompass all aspects of the project risk management process for the purposes of

a) detecting changes in the external and internal context, including changes to the project scope, objectives or risk criteria that can require revision of risks, risk treatments and priorities,
b) obtaining further information to improve risk assessment,
c) ensuring that controls are effective and efficient in both design and operation,
d) analysing and learning lessons from successes and failures (including incidents and near-misses), changes and trends, and
e) identifying emerging risks.

Risk treatment activities should be included in the project plan and monitored as part of regular project control activities. Progress in implementing risk treatment tasks should be incorporated into the project's overall performance management, measurement and external and internal reporting activities.

At the end of the project, it is desirable that there is a post-project review of control effectiveness, lessons learned and feedback of learning into future projects. It is important that this activity is started during the project, so that it is not left until the end when everyone who knew what happened has already left and moved onto the next project.

The results of monitoring and review should be recorded and reported as appropriate. They should also be used as an input to the review of the risk management framework (see 6.5).

7.7 Recording and reporting the project risk management process

7.7.1 Reporting

Reporting on risk matters is necessary as an input to management decision-making and to provide confidence that project objectives are achievable. All project meetings provide an opportunity for discussing and resolving risk matters. Project meetings can be formal or informal, but all discussions and decisions concerning risks should be recorded and reported.

Discussions of risk matters can include the following:

a) identifying and assessing new or emerging risks;
b) reviewing the project risk register;
c) reviewing the status of risks, the effectiveness of associated controls and the implementation of risk treatment activities;
d) identifying and agreeing any changes to information about the risks, re-analysing the changes and updating the risk register;
e) assessing the effectiveness of the risk management process;
f) discussing the relationship between contracted parties, including the allocation of risks.

Specific performance indicators can be developed for many of the items noted above.

Reporting requirements should be specified in the project risk management plan. Where feasible, project risk management reporting should be integrated with other forms of project management reporting.

7.7.2 The project risk management plan

The project risk management plan describes the structured process of risk management to be applied to the project.

The project risk management plan can be part of the project management plan or it may be a separate document. It can include or refer to

a) the context and boundaries of project risk management including the objectives of project risk management,
b) the project risk management framework, processes and interfaces,
c) responsibilities for risk management activities, authorities and lines of reporting,
d) internal and external interfaces,
e) schedule of project risk management meetings (often aligned with or part of regular project management meetings),
f) project risk review processes,
g) relationship with other project documents and plans,
h) relevant organizational procedures,
i) interfaces with risk management plans from other sources as appropriate (for example, suppliers and subcontractors),
j) project risk register format.

The project risk management plan should be reviewed regularly and updated as required.

7.7.3 Documentation

Documentation is required to facilitate the implementation and control of the risk management process, particularly at the hand over of different project phases.

Documentation aids planning, progress evaluation and traceability. The risk management process, the risks and their treatment should all be documented. In the project risk management process, records provide the foundation for improvement in methods and tools, as well as in the overall process.

Decisions concerning the creation of records should take into account

a) the organizations' needs for continuous learning,
b) benefits of re-using information for project management purposes,
c) costs and efforts involved in creating and maintaining records,
d) legal, regulatory and operational requirements for records,
e) method of access, ease of retrievability and storage media,
f) retention period, and
g) sensitivity of information.

7.7.4 The project risk register

The project risk register is a particularly important form of documentation. It is the medium for recording changes to risk status. Its content is the basis for regular reporting at project management level and for discussion of risks and their treatment at project meetings.

A project risk register should be initiated at the earliest phase in the life of a project (Table 1) and be reviewed and updated throughout the project's life. The register can consist of a data base that includes all the information relating to identified risks. It should contain at least a list of the risks and risk owners (the people responsible for each risk), the causes and

consequences of each risk for the objectives, relevant controls and control owners (the people responsible for each control) and the outcomes from risk analysis and risk evaluation. It can also contain additional information as required, including the names of people responsible for further analysis (usually the risk owners or people who report to them) or treatment (task owners). A unique identification number should be allocated and noted, and the traceability of the data to its source should also be recorded.

A risk register may be paper-based or in the form of a spreadsheet or a computer database. The level of risk register sophistication should match the project size and importance and the nature and level of risks. Access to and control of the risk register may be difficult with paper-based or spreadsheet registers.

The plans for treating each risk should be documented, including the actions required, the person responsible and the timing for completion. Risk treatment tasks should be included in the project plan.

In complex projects there can also be risks that arise from complex interactions where symptoms are recognisable but no one clear event, cause or potential consequence can be defined. It is often difficult for these risks to be entered into a simple risk register. Nevertheless such risks still need to be recognized, analysed and treated, and records concerning them should be maintained.

In a large project there can be multiple risk registers prepared by different stakeholders at different project phases. Information from these registers needs to be collated and passed on across phases as the project progresses. However, these risk registers reflect the needs of the organizations at specific project phases and the perceptions of the individual parties who created them, and they can use different criteria. The criteria need to be reconciled and aligned if the risk registers are to be used at a project level or if risks are to be transferred from one register to another, for example if a decision is made to allocate responsibility for a risk to another party who is better placed to treat it.

When information about risks is transferred there should be agreement between the parties involved about who is responsible for the risk (the risk owner) and who will bear the positive or negative consequences associated with the risk.

At the end of each project phase, there are often residual risks that relate to subsequent phases. Information about these risks shall be transferred to relevant stakeholders and included in the associated risk registers for the next phases.

Annex A
(informative)

Examples

A.1 General

The material in this annex shows examples of the kinds of information that can be used or generated in each step of the project risk management process. These are examples based on material from a range of different kinds of projects in simplified form; they are provided for guidance only, and they are not intended to be definitive.

A.2 Project risk management process

A.2.1 Stakeholder analysis (see 7.2)

Identification and analysis of external and internal stakeholders is an important step, as the perceptions and objectives of stakeholders should be taken into account in setting project objectives. Table A.1 lists stakeholders for a government project, showing how specific stakeholders can be grouped into larger categories. Table A.2 extends the analysis to list stakeholders, their key issues and their objectives for a project. Table A.3 shows a small part of a table that could be used to develop a stakeholder communications plan for a civil engineering construction project; such a table can also form part of a more formal stakeholder engagement plan for a larger project, or for a project that requires wider stakeholder involvement, e.g. in an environmental impact analysis.

Table A.1 – Stakeholders for a government project

General	Specific stakeholders
Department	Executive management; business units involved in the project; departmental users
Staff	Departmental staff; support staff; unions
Government and Ministers	Central Government; Cabinet; Portfolio Minister; local government bodies
Other departments	Central funding agencies
Finance providers	Financial institutions and their stakeholders
Industry	Suppliers of capability and resources
Public and community	Public customers and users; local businesses; local communities and neighbours of a project site; special interest groups; media

Table A.2 – Stakeholders and objectives for a ship upgrade

Stakeholder	Key issues and objectives
Ship operator	Functions, delivery schedule, cost, quality
Ship owner	Good availability, cost, delivery schedule, support
Refurbishment prime contractor	Image, profit, continuing business, credibility with this kind of vessel, capability
Sub-contractors, suppliers	Low risk, profit
Politicians	Image, public support, work near home port
Maintenance contractor	Low cost ship when returned to service
Employees	Security, satisfaction
Unions	Membership, power, agreements
Councils, neighbourhood	Support, environment, employment

Table A.3 – Stakeholders and communication needs for a civil engineering project

Stakeholder	Issues, constraints	Communication needs
Directly affected land owners	Acquisition process, compensation and timings Loss of income as a result of loss of productive land Construction and operation impacts (air, noise and vibration) Water quality Visual amenity Severance of property	–
Neighbours	Construction and operation impacts (air, noise and vibration) Water quality Visual amenity	–
Traditional owners	Potential damage to sites of cultural significance Cumulative impacts	–
Local communities	–	
NOTE This is not intended to be a complete list.		

A.2.2 External and internal context (see 7.3.4)

The external and internal context provide a summary of the main factors that influence the project and its environment, and so they provide a good starting point for thinking about sources of uncertainty.

Table A.4 and Table A.5 show examples of how context information can be summarized: the 'factors' columns contain statements or topic headings, and the 'implications' columns list some of the ways each factor could influence the project or give rise to uncertainty. These examples show that in some cases it is not clear whether a factor is better classified as external or internal; however, that is generally less important than recording the factor so it can stimulate thinking when risks are identified in the risk assessment step. They also indicate that considerable detail can be involved, although the detail has been simplified in these examples.

Table A.4 – External context for an energy project

External factors	Implications
Government regulation is becoming more stringent	Many approvals are needed, under many Acts (see list …): there are particular environmental and cultural heritage constraints Auditing Compliance monitoring associated with licence to operate Taxes and royalties could change
Carbon price and carbon trading	Government intentions and rules on carbon pricing and carbon trading are variable and uncertain Changes in rules could affect us directly, and indirectly through their impacts on our customers International rules changes could also affect us in the longer term, but there is huge uncertainty
There are many competing activities in progress	Increased competition for skilled and experienced staff; increased competition for contractors Cumulative impacts could be significant and this could impact on our operations Impact areas include: …
Competitor activities could impact us	Poor practices by competitors could have an adverse effect on our reputation We could be able to gain access to competitor infrastructure There could be scope for cooperative infrastructure developments We will need to take account of other competing activities …
We have several joint venture partners	We have agreements in various operated and non-operated joint ventures The number of JVs and commercial arrangements could increase as we expand our operations We depend on JV partners meeting their contractual obligations …
Contractors	Our safety standards and permit to work conditions must be enforced Contractors could have trouble getting qualified personnel Increased demand for a limited pool of qualified contractors could drive rates up We depend on contractors for critical asset creation, so we need to be assured of the quality of their work
Customers	Possible variable demand from domestic customers Long-term contracts will be necessary to support downstream investments
Technology change	–
–	
NOTE This is not intended to be a complete list.	

Table A.5 – Internal context for a private sector infrastructure project

Internal factors	Implications
Our business is expanding rapidly: demand	Key contracts are in place We will need to contribute substantial capital to exploit these opportunities We need to design and build key infrastructure quickly
Our business is expanding rapidly: people	This requires accelerated growth of our teams, in head office and on site, during both construction (7,000 new direct jobs) and operations (1,000 new direct jobs) There will be competition for experienced staff and retention of competent people could be difficult Training and up-skilling of a growing workforce will be a challenge We will need to expand our administrative and support capability
Our business is expanding rapidly: systems	Management systems could become unsuitable for current operations or not interface effectively Our processes have not been adapted as the business has grown New staff might not be aware of the importance of our business processes, and important processes might not always be followed Communications across multiple remote sites can become more difficult
The project team hands over assets to operations	Interfaces between the project team and the operations and maintenance teams are important Project delivery is critical for operations and planned production increases, and for reaching production and delivery targets
Health and safety is a major focus of the business	Safety management will become more difficult across multiple sites, functions and contractors There are limitations in implementation of health safety and environment directives There can be emergency response challenges in remote locations There are health implications associated with camp living Increased travel requirements
–	
NOTE This is not intended to be a complete list.	

A.2.3 Risk management context (see 7.3.4)

The risk management context describes the scope and objectives for the particular risk assessment activity to be conducted. In some cases it can be a simple statement like the one in A.2.4. In other cases it can be more elaborate, like the diagram in Figure A.1 that shows the physical works, the supporting activities, the relevant project phases and some explicit exclusions from the scope of a project to develop and commission an open pit mine.

A.2.4 Risk management context for a power enhancement project

The risk assessment will consider all activity from now through to the proposed plant upgrades and power stations entering routine operation. All associated activities from which risks could arise that would affect the company or any of its stakeholders, such as the provision of fuel supplies to the power stations or alterations to logistic facilities at the plants, shall also be considered.

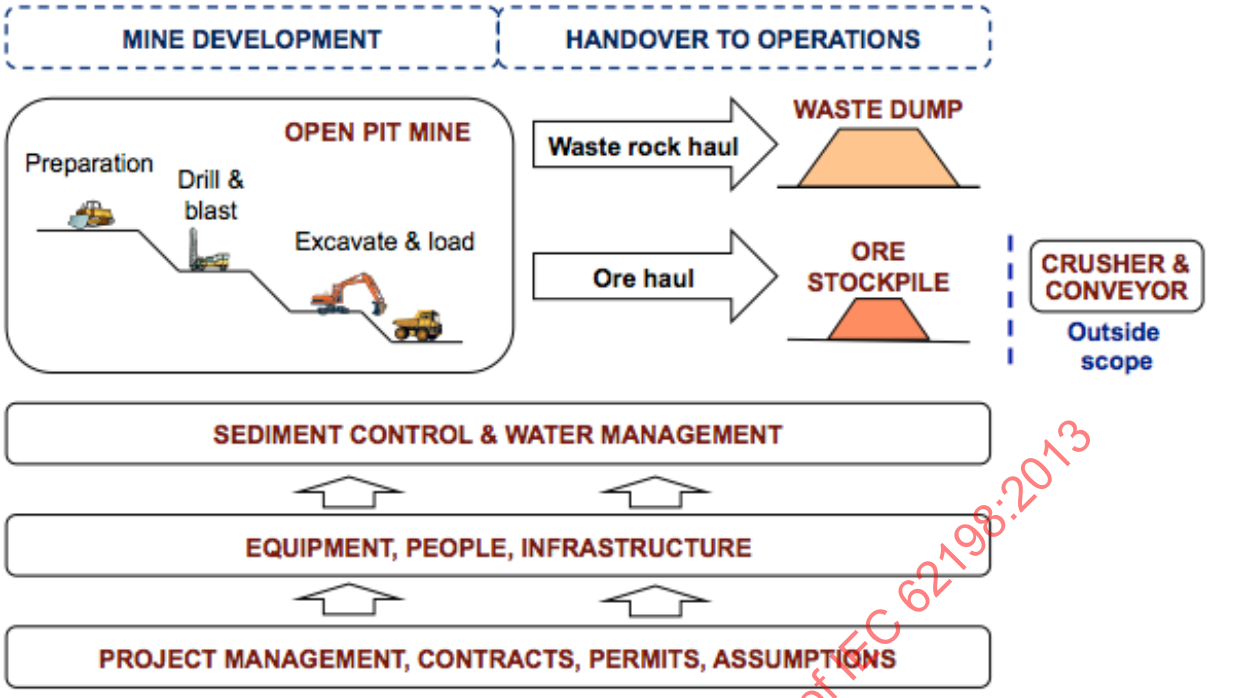


Figure A.1 – Risk management scope for an open pit mine project

A.2.5 Risk criteria (see 7.3.5)

Risk criteria provide a summary of all the detailed objectives for the project that have to be taken into account if 'success' is to be achieved. Table A.6 provides an example; other criteria are listed in Table A.10 below. These examples show that project success criteria are, in practice, usually far more extensive than simply cost, time and quality.

Table A.6 – Criteria for a high-technology project

Project criterion	Notes
Capability	Includes performance, user acceptance, quality, interoperability with existing systems, 'future proof', preparation for use, good man-machine interfaces
Dependability	Includes durability, reliability, availability and maintainability (RAM), integrated logistics support (ILS), support processes, and dependability in relation to safety, occupational health and safety (OH&S) and environmental aspects
Training	User acceptance, appropriateness, completeness
Acquisition cost	Purchase costs, including project office costs
Life cycle cost	Whole-of-life costs for the asset created by the project
Delivery schedule	Project milestones, capability delivery
Linkages	Integration and coordination with other projects
Good management	Includes probity, processes, systems, acquisition to in-service and transition, interfaces with other Government agencies
Industry involvement	Level of local industry involvement in acquisition and support, domestic support capability

A.2.6 Key elements (see 7.3.6)

Key elements are used for structuring the risk assessment activity and providing an agenda for the assessment workshop. In the examples below, the description or notes columns are used to provide additional detail about what is included in each element and what is excluded; if the structure is based on a formal project work breakdown structure (WBS), the description

can be an extract from the WBS dictionary. While the WBS is often a good basis for structuring a risk assessment for a project, other structures can also be useful; for example, the main topics listed in Figure A.1 can also form a good basis for thinking about what could happen in that particular project.

Table A.7 shows key elements for a communications system project based on the project WBS. Table A.8 also uses the project WBS for structuring but extends the table to indicate the main teams involved in each part of the risk assessment. Table A.9 uses a more general structure for a project to establish a health-care service organization.

Table A.7 – Key elements for a communications system project

No	Element	Description, notes
1	**Communications system**	
1.1	Principal equipment	HF and VHF radios, vehicle-mounted and handheld
1.2	Ancillaries and accessories	Interfaces, antennas, audio accessories, speakers, headsets, containers, data terminals, remote control, re-transmission, GPS
1.3	Vehicle sub-systems	Vehicle intercom, vehicle integration
1.4	Spectrum management	Spectrum management
1.5	Power management system	Batteries, chargers, storage, battery management, industry involvement, transition to rechargeable batteries
1.6	Other items	Systems integration; interoperability, linkages with other projects
2	**Integrated logistic support (ILS)**	
2.1	Training	Initial training, continuing training
2.2	Documentation	RAM data, manuals
2.3	ILS philosophy	Maintenance and repair philosophy, support arrangements, software support, spares holdings, special tools and test equipment, spares, maintenance plan, supply support, quality plan, certification, warranty, configuration management
3	**Acquisition management**	
3.1	Project management	Budget, schedule, requirements and solution verification, expectations management, completeness
3.2	Approval processes	External approval, scope changes, internal approvals
3.3	Introduction into service	Installation, test and acceptance, user acceptance, transition planning, initial training, codification
3.4	Procurement strategy	Contracting strategy, contract management
3.5	External issues	Synchronization, external influences, operational timeframes

Table A.8 – Key elements and workshop planning guide for a defence project

Element		Notes	Workshop
1.1	Capability definition	Defence policy issues, requirement, inter-operability	Policy group
1.2	Force structure		
1.3	Sustainability	Concept of operations, support, cost	
1.4	Delivery	Capability, timing, cost	
2.1	Processes	Documented, auditable	Project team
2.2	Structure	People, systems	
2.3	Communication	Consultation	
2.4	Contractors		
2.5	Requirements specification		
2.6	Tendering		
3.1	Aircraft		Operators
3.2	Tactical systems		
3.3	Mission support		
3.4	Personnel	Training, management structure, crew structure	
3.5	Operations	Integration, management, inter-operability	
4.1	Stores	Spares, expendables, etc.	Support team
4.2	Support equipment	Includes facilities	
4.3	Data	Design and engineering data, publications, manuals	
4.4	Personnel	Training, structure	
4.5	Policy	Maintenance concept	

Table A.9 – Key elements for establishing a new health service organization

Element		Description
1	Start-up and transition	All activities required to start up the organization and its internal processes
2	Workforce engagement	Identification, engagement and maintenance of professional health service providers
3	Communications and relationships	Formal and informal communications, engagement of other agencies and entities
4	Commercial	Financial management, contracts
5	Service delivery	Cultural and clinical contact and treatment
6	Other	As required

A.2.7 Risk analysis (see 7.4.3)

A.2.7.1 Assigning a qualitative level of risk

Project risks are often analysed and compared by assigning a value for consequences and their likelihood from predefined assessment scales, then combining the values to provide a qualitative level of risk that is recorded in the risk register.

The assessment scales used can be specific to the project, but many organizations that conduct projects regularly use a set of ‘standard’ scales for all projects. In all cases, the scales should be related to and appropriate for the context in which the risk assessment is being undertaken.

Organizations can measure the consequences of risks in terms of any or all of the risk criteria established earlier (e.g. in Table A.6). Table A.10 shows a five-point scale for measuring consequences against four criteria, suitable for a qualitative risk analysis. Some organizations use more than five points (but fewer than five rarely provides appropriate discrimination between outcomes), and most use other criteria in addition to the ones shown here. Note that the scale descriptions in any one line are not intended to be identical, but they should be broadly equivalent in terms of their importance for the organization. Anomalous as it can seem, many organizations that undertake projects regularly do not have a consequence scale related directly to project timing; instead, they consider project acceleration or delay in terms of their financial or earnings impact on the organization.

Impacts can be positive or negative. They can be measured in absolute terms or in relation to expected outcomes.

Table A.10 – Example consequence scale

	1. People	2. Environment	3. Financial	4. Reputation	...
5	Multiple fatalities or Permanent total disabilities from an accident or occupational illness	Massive effect: Persistent severe environmental damage or severe nuisance extending over a large area. Major loss in terms of commercial, recreational or nature conservation	Direct loss or gain > $ 10 million	International impact: international public and media attention (positive or negative)	
4	Single fatality or permanent total disability from an accident or occupational illness	Major effect: Severe environmental damage. Extensive measures to restore polluted or damaged environment to its original state by the company.	Direct loss or gain of $ 500 000 – $ 10 million	National Impact: National public and media attention (positive or negative)	
3	Major injury or health effects (absences, irreversible health damage, chronic condition)	Localized effect: Limited loss or discharges of known toxicity affecting neighbourhood, spontaneous recovery of limited damage within one year.	Direct loss or gain of $ 100 000 – $ 500 000	Considerable impact: Regional public attention (positive or negative), extensive attention in local media	
2	Minor injuries or health effects (restricted work case or lost time injury.) Limited, reversible health effects	Minor contamination. Damage sufficiently large to attack the environment, but without permanent effects	Direct loss or gain of $ 10 000 – $ 100 000	Limited impact: Some local public attention (positive or negative), some local media attention	
1	Slight injury or health effects (First Aid Case, Medical Treatment Case)	Slight effect. Local environmental damage, within the fence	Direct loss or gain below $ 10 000	Slight impact: Public awareness exists, but there is no public concern	

Table A.11 shows a five-point scale for measuring likelihood, suitable for a qualitative risk analysis. The table contains two ways of assessing likelihoods (in words and in terms of recurrence periods) to accommodate different kinds of events and circumstances and different ways of thinking by those providing the assessment. The specific time scales in the table should be adjusted to the context of the project. They can be measured in absolute terms or in relation to expected outcomes.

Table A.11 – Example likelihood scale

Category	Criteria
A	Consequence is highly likely to arise, or Could occur on a monthly basis
B	Balance of probability will occur, or Could occur annually
C	Could occur shortly but there is a distinct probability it won't, or Could occur every 2 to 10 years
D	Could occur but not anticipated, or Could occur every 11 to 50 years
E	Occurrence requires exceptional circumstances Exceptionally unlikely, even in the long term future Occurs less than once every 50 years

Table A.12 shows one way of converting the consequence and likelihood ratings in a qualitative assessment into a level of risk. In this example, the matrix is not symmetric, and more weight is given to high consequences than to high likelihoods.

Note that care has to be exercised in developing tables like Table A.10, Table A.11 and Table A.12, to ensure the levels of risk are meaningful for the project and reflect the organization's attitude to risk.

Table A.12 – Example of a matrix for determining the level of risk

Likelihood rating	**A**	Medium	Medium	High	High	High
	B	Medium	Medium	High	High	High
	C	Low	Medium	Medium	High	High
	D	Low	Low	Medium	Medium	High
	E	Low	Low	Medium	Medium	Medium
		1	**2**	**3**	**4**	**5**
		Consequence rating				

A.2.7.2 Quantitative risk analysis using simulation

Uncertainty affects project objectives when there are uncertainties in the estimates that are made during the concept and development phase (for example uncertainties in quantities, rates and timings), and because events can occur that were not contemplated when the estimates were generated. Simulation (most commonly Monte Carlo simulation) can be used to determine the effects on project outcomes, such as capital cost or schedule duration, when uncertain inputs are represented as probability distributions.

Simulation can provide information concerning

– the most likely cost, taking into account identified risks,
– the probability that costs will exceed the budget, taking into account the identified risks,
– how much cost contingency is needed, and
– which elements of the cost generate the most need for the cost contingency.

There are many techniques to quantify the effects of uncertainties on project cost. Simulation is one such approach. It usually involves the following steps:

a) review and validate the available information including the contract, work breakdown structure (WBS), cost breakdown structure (CBS), risk register, initial cost estimate, etc. to make sure they are accurate and represent the most likely scenario;

b) review and assess the cost impacts (both positive and negative) of identified risks, the associated uncertainties in those impacts and the probability distributions of impacts that best represent those uncertainties;

c) develop a cost risk model that incorporates the uncertainty distributions;

d) perform a simulation for multiple calculations of the cost risk model using software to provide input data sampled from the appropriate probability distributions;

e) review and validate the outcomes, then modify the cost risk model and repeat the earlier steps if necessary;

f) document and communicate the outcomes, then regularly monitor to ensure the assumptions about the inputs and the uncertainties remain valid.

The following example demonstrates how simulation was used to help assess the positive and negative impacts of risks affecting the estimated direct construction costs for a multi-million dollar port refurbishment.

After following the steps outlined above, the results in Figure A.2 helped the project team to validate the probability of achieving the initial cost estimate and the chance of cost overrun due to identified risks:

1) the initial estimate of the most likely direct construction cost was $ 124 million;

2) when the impact of risks was included the analysis suggested a range of direct construction cost from $ 119 million (optimistic) to $ 137 million (pessimistic), with 0,05 and 0,95 probabilities respectively, and a mean of $ 128 million;

3) following review meetings with the project team, a forecast of $ 128 million (with 50 % likelihood) was selected as the most credible estimate for direct construction cost after consideration of the identified risks;

4) the difference between the initial estimate of $ 124 million and the selected final estimate of $ 128 million equalled $ 4 million. This was considered as the required cost contingency for the project, as a 0,50 probability of achieving the cost budget consisting of the base forecast cost plus the contingency (or equivalently a 50 % chance of exceeding the cost budget) was deemed acceptable.

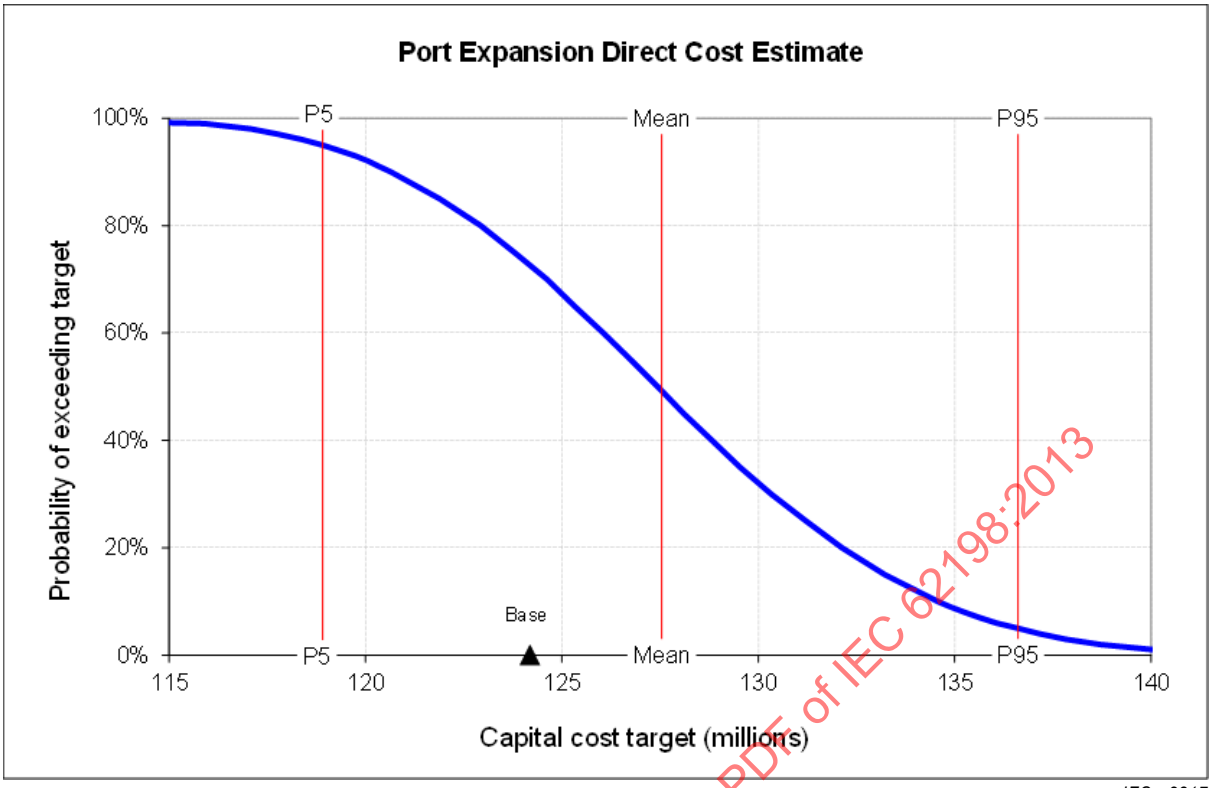


Figure A.2 – Distribution of costs using simulation

A.2.8 Risk evaluation (see 7.4.4)

The priority for attention allocated to a risk depends on several factors, including the nature and level of risk, the effectiveness of the current controls and the maximum potential exposure if the controls were to fail. Table A.13 shows an example based on the level of risk and the effectiveness of the controls; the 'suggested timing' column must be adjusted to suit the timescale and pace of the project, and the delegations of authority in the organizations involved.

Table A.13 – Example of priorities for attention

Level of risk	Suggested action	Suggested timing	Authority for continued toleration of risk
High	Where controls are not as good as reasonably possible, take action to improve controls or reduce the risk to medium or below	Short term: normally within 1 month	Project director (the executive to whom the project manager reports) or the project executive steering group
Medium	Plan to deal with the risk in keeping with the project plan	Medium term: normally within 3 months	Project manager (the manager responsible for project operations)
Low	Plan in keeping with all other priorities; will still require attention	On-going control as part of the project management system	Activity manager (within the project)

A.2.9 Risk treatment (see 7.5)

A simple worksheet like the one in Table A.14 can be used for the evaluation of treatment options. If the right people are involved in the evaluation, it is usually readily apparent whether an option is worth pursuing (Yes), whether it should be discarded or postponed (No) or whether additional information is needed to make a decision (Maybe).

Table A.14 – Example of a treatment options worksheet

Risk: Delay in delivery of critical components, leading to delayed completion of the project phase				
	Option	**Benefits**	**Dis-benefits**	**Conclusion**
1	Start design and procurement processes earlier	Give suppliers advanced warning and more time.	Could require additional design effort, or minor rescheduling of design	Yes
2	Ensure all critical suppliers have business continuity plans in place	Gain more insight and comfort about continuity of supply, quality and standards. Provides transparency. Can do it immediately.	Might not get cooperation from some suppliers. Time involved in doing this properly	Maybe
3	Use multiple suppliers for key items	Can spread the risk of delivery delay.	Loss of consistency of items and spares. Increased costs (reduced economies of scale; additional transport costs)	No
–	–			

A.2.10 Risk register (see 7.4.2 and 7.7.4)

Project risks are often recorded in a database or risk register. Table A.15 shows a simple structure, which is appropriate if the risks are described at a level of detail that includes the causes and the consequences (e.g. in the form 'something happens and leads to an impact on objectives'). If simpler risk descriptions are used, the register should be augmented with new columns, after the risk column, for recording causes and impacts explicitly. In Table A.15, CE records control effectiveness, C records the consequence rating (e.g. from Table A.10), L records the likelihood rating (e.g. from Table A.11), the risk level comes from a combination of C and L (e.g. using a table such as Table A.12) and PE records the potential exposure, which is the maximum consequence if all the controls were to fail.

Table A.15 – Simple risk register structure

Element	**Risk**	**Existing Controls**	**CE**	**C**	**L**	**Risk Level**	**PE**	**Risk Owner**
						–		
						–		

Bibliography

[1] ISO 10006:2003, *Quality management systems – Guidelines for quality management in projects*

[2] ISO Guide 73:2009, *Risk management – Vocabulary*

Additional non-cited references

IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

IEC/ISO 31010, *Risk management – Risk assessment techniques*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DES RISQUES LIÉS À UN PROJET – LIGNES DIRECTRICES POUR L'APPLICATION

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 brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62198 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Cette deuxième édition annule et remplace la première édition, parue en 2001, et constitue une révision technique.

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

a) une restructuration majeure de la première version;

b) maintenant aligné avec l'ISO 31000, *Management du risque – Principes et lignes directrices.*

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1529/FDIS	56/1539/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.

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 stabilité 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

Chaque projet implique un certain niveau d'incertitude et de risque. Ces risques peuvent être liés aux objectifs du projet lui-même ou à ceux des actifs, produits ou services que crée le projet. La présente Norme internationale donne les lignes directrices pour une gestion systématique et cohérente des risques.

Le management du risque inclut les activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du risque. L'ISO 31000, *Management du risque – Principes et lignes directrices*, décrit les principes relatifs à une gestion efficace du risque, offre un cadre établissant 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 dans tout l'organisme, et définit un processus de management du risque applicable à tous les types de risque dans une organisation. La présente norme indique dans quelle mesure ces principes et lignes directrices s'appliquent à la gestion de l'incertitude dans les projets.

La présente norme s'adresse aux individus et organisations impliqués dans tout ou partie des phases du cycle de vie d'un projet. Elle peut également s'appliquer aux sous-projets et ensembles de projets et de programmes étroitement liés.

L’application de la présente norme nécessite d’être adaptée à chaque projet spécifique. Par conséquent, il est considéré comme totalement inapproprié d'imposer une procédure de certification aux acteurs de la gestion de risque.

Les lignes directrices indiquées dans la présente norme n'ont pas pour objet de remplacer les normes spécifiques au secteur industriel existantes, même si elles peuvent s'avérer utiles dans ces cas précis.

GESTION DES RISQUES LIÉS À UN PROJET – LIGNES DIRECTRICES POUR L'APPLICATION

1 Domaine d'application

La présente Norme internationale donne les principes et lignes directrices génériques en matière de management des risques et des incertitudes dans les projets. Elle présente en particulier une démarche systématique de management des risques en s'appuyant sur l'ISO 31000 *Management du risque – Principes et lignes directrices*.

Les lignes directrices s'appuient sur les principes de management des risques liés aux projets, le cadre et les exigences organisationnelles de mise en œuvre du management des risques et le processus d'exécution efficace de management des risques.

La présente norme n'est pas destinée à la certification.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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 – Principes et lignes directrices*

3 Termes et définitions

Pour les besoins de ce document, les termes ou définitions suivants s'appliquent.

3.1
projet
processus unique, qui consiste en un ensemble d'activités coordonnées et maîtrisées, comportant des dates de début et de fin, entrepris dans le but d'atteindre un objectif conforme à des exigences spécifiques, incluant les contraintes de délais, de coûts et de ressources

Note 1 à l'article: Il est possible qu'un projet individuel fasse partie d'une structure de projet plus large.

Note 2 à l'article: Dans certains projets, les objectifs sont mis à jour et les caractéristiques du produit sont déterminées progressivement, à mesure que le projet progresse.

Note 3 à l'article: Le produit du projet est en général défini dans le domaine d'application du projet. Il peut s'agir d'une ou de plusieurs unités de produit, matériel ou non.

Note 4 à l'article: En principe, l'organisation du projet est provisoire et établie pour la durée de vie du projet.

Note 5 à l'article: La complexité des interactions entre les activités d'un projet n'est pas nécessairement liée à la taille du projet.

[SOURCE: ISO 10006:2003, 3.5] [1][1]

1 Les chiffres entre crochets se réfèrent à la Bibliographie.

3.2
gestion de projet
planification, organisation, suivi, maîtrise et compte-rendu de tous les aspects d'un projet et de la motivation des personnes impliquées pour atteindre les objectifs du projet

[SOURCE: ISO 10006:2003, 3.6 modifiée – le mot "gestion" a remplacé le mot "management" dans le terme]

3.3
plan de gestion de projet
document qui spécifie les éléments nécessaires permettant d'atteindre les objectifs du projet

Note 1 à l'article: Il convient que le plan de gestion de projet comprenne le plan qualité du projet ou s'y réfère.

Note 2 à l'article: Le plan de gestion de projet comprend également d'autres plans ou y fait référence, tels que ceux concernant l'organisation, les ressources, le planning, le budget, le management du risque (3.5), le ganagement environnemental, la gestion en matière d'hygiène et de sécurité, ainsi que la gestion de la sûreté, le cas échéant.

[SOURCE: ISO 10006:2003, 3.7, modifiée – le mot "gestion" a remplacé le mot "management" dans le terme]

3.4
risque
effet de l'incertitude sur l'atteinte des objectifs

Note 1 à l'article: Un effet est un écart, positif et/ou négatif, par rapport à une attente.

Note 2 à l'article: Les objectifs peuvent avoir différents aspects (par exemple buts financiers, de santé et de sécurité et environnementaux) et peuvent concerner différents niveaux (niveau stratégique, niveau d'un projet, d'un produit (3.1), d'un processus ou d'un organisme tout entier).

Note 3 à l'article: Un risque est souvent caractérisé en référence à des événements et des conséquences potentiels ou à une combinaison des deux.

Note 4 à l'article: Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa vraisemblance.

Note 5 à l'article: L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

[SOURCE: ISO Guide 73:2009, 1.1] [2]

3.5
management du risque
activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du risque

[SOURCE: ISO Guide 73:2009, 2.1]

3.6
cadre organisationnel de management du risque
ensemble d'éléments établissant 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 dans tout l'organisme

Note 1 à l'article: Les fondements incluent la politique, les objectifs, le mandat et l'engagement envers le management du risque (3.4).

Note 2 à l'article: Les dispositions organisationnelles incluent les plans, les relations, les responsabilités, les ressources les processus et les activités.

Note 3 à l'article: Le cadre organisationnel de management du risque fait partie intégrante des politiques stratégiques et opérationnelles, ainsi que des pratiques de l'ensemble de l'organisme.

[SOURCE: ISO Guide 73:2009, 2.1.1]

3.7
politique de management du risque
déclaration des intentions et des orientations générales d'un organisme en relation avec le management du risque

[SOURCE: ISO Guide 73:2009, 2.1.2]

3.8
plan de management du risque
programme inclus dans le cadre organisationnel de management du risque, spécifiant l'approche, les composantes du management et les ressources auxquelles doit avoir recours le management du risque

Note 1 à l'article: Les composantes du management incluent, par exemple, les procédures, les pratiques, l'attribution des responsabilités et le déroulement chronologique des activités.

Note 2 à l'article: Le plan de management du risque peut être appliqué à un produit, un processus, un projet (3.1) particulier, à une partie de l'organisme ou à l'organisme tout entier.

[SOURCE: ISO Guide 73:2009, 2.1.3]

3.9
processus de management du risque
application systématique de politiques, procédures et pratiques de management aux activités de communication, de concertation, d'établissement du contexte, ainsi qu'aux activités d'identification, d'analyse, d'évaluation, de traitement, de surveillance et de revue des risques

[SOURCE: ISO Guide 73:2009, 3.1]

3.10
traitement du risque
processus destiné à modifier un risque

Note 1 à l'article: Le traitement du risque peut inclure:

– un refus du risque en décidant de ne pas démarrer ou poursuivre l'activité porteuse du risque;
– la prise ou l'augmentation d'un risque afin de saisir une opportunité;
– l'élimination de la source du risque;
– une modification de la vraisemblance;
– une modification des conséquences;
– un partage du risque avec une ou plusieurs autres parties (incluant des contrats et un financement du risque); et
– un maintien du risque fondé sur une décision argumentée.

Note 2 à l'article: Les traitements du risque portant sur les conséquences négatives sont parfois appelés "atténuation du risque", "élimination du risque", "prévention du risque" et "réduction du risque".

Note 3 à l'article: Le traitement du risque peut créer de nouveaux risques ou modifier des risques existants.

[SOURCE: ISO Guide 73:2009, 3.8.1]

4 Management du risque dans les projets

Tous les projets comportent une incertitude pouvant donner lieu à des risques. Ces risques peuvent être liés aux objectifs du projet lui-même (réalisation du projet dans un temps et un budget impartis, par exemple) ou aux exigences des actifs, produits ou services créés dans le cadre du projet (pour un produit sûr, fiable et renouvelable, par exemple).

Les conséquences susceptibles de découler de l'incertitude d'un projet peuvent être tant avantageuses que néfastes. Le management du risque peut donc avoir vocation à éviter ou résoudre des problèmes, mais également à identifier et saisir des opportunités. La prise en compte des risques d'un projet facilite la prise de décision et permet de maîtriser les effets d'un projet et d'augmenter la valeur pour les parties prenantes.

Cette norme s'adresse aux individus et organisations impliqués dans tout ou partie des phases du cycle de vie d'un projet. Pour obtenir le meilleur bénéfice, les activités de management du risque commencent le plus tôt possible et se poursuivent tout au long du projet. Toutefois, le management du risque peut commencer à tout moment dans le cycle de vie, à condition de procéder à un travail préliminaire approprié. Le processus est évolutif. Il peut donc être utilisé dans le cadre de petits projets, de projets importants et de phases individuelles d'un projet. Il peut également s'appliquer à des sous-projets et à des ensembles de projets et de programmes étroitement liés.

Un ensemble de phases d'un projet et leurs caractéristiques sont présentés au Tableau 1.

Tableau 1 – Phases classiques d'un projet

Phase	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6
Nom de la phase	Identification du concept	Sélection de la faisabilité préalable	Conception et développement faisabilité	Livraison Mise en œuvre Installation	Exploitation et entretien	Abandon Mise au rebut
Objet	Évaluation des opportu-nités: déterminer si le projet peut être adapté à la stratégie de l'entreprise	Choix des options: identifier et évaluer les options de développement du projet, et sélectionner l'option privilégiée	Définition du projet: finaliser le domaine d'application et les caractéristiques de l'option choisie	Livraison du projet: produire un actif ou service d'exploitation dans le domaine d'application déterminé	Réalisation des bénéfices: évaluer les effets du projet pour assurer les performances	Fermeture: assurer la sécurité et la fermeture acceptable
Objectif des activités de manage-ment du risque	Menaces et opportunités stratégiques	Choix des options en fonction du risque	Stratégie de conception et de livraison	Livraison, essai et remise du projet	Exploitation et maintenance	Mise au rebut et réhabilitation

En principe, une phase passe par un point de décision (parfois appelé portail) auquel l'approbation des dirigeants est fournie pour progresser et entrer dans la phase suivante.

Les informations sur les risques et le management du risque sont une part importante des informations fournies aux dirigeants pour soutenir leurs décisions à chaque point de décision. Il convient également de transmettre les informations sur les risques et contrôles de chaque phase à l'équipe en charge de la phase suivante du projet.

Les dirigeants et gestionnaires des organismes associés à un projet jouent un rôle dans le management des risques liés à leurs décisions (Figure 1). La présente norme s'adresse:

a) aux directeurs et chefs de projet d'un organisme à l'origine du projet ou qui gèrent les actifs, les produits ou les services que le projet va générer;

b) aux membres des équipes de projet chargés des sous-projets, groupes d'activités ou ensembles de travaux significatifs;

c) aux propriétaires du projet ou sponsors chargés de veiller aux intérêts commerciaux de l'organisme commanditaire et d'atteindre les objectifs et bénéfices prévus;

d) aux dirigeants qui ont à approuver la progression du projet à chaque point de passage et les dépenses liées à la phase suivante;

e) aux réviseurs qui s'efforcent de fournir aux dirigeants décisionnaires l'assurance que les informations sont exhaustives, précises et fiables;

f) aux directeurs et chefs de projet d'un organisme contractant, d'un sous-traitant ou d'un fournisseur, qui proposent ou livrent tout ou partie du projet et de ses actifs, projets ou services associés;

g) aux financiers et assureurs qui proposent un soutien financier ou connexe au projet;

h) aux régulateurs des activités, des actifs, des produits ou des services que peut générer le projet; et

i) aux autres parties prenantes, y compris les sous-traitants, les fournisseurs et les parties ayant un intérêt dans le projet et ses résultats et des utilisateurs ou les bénéficiaires des actifs, des produits ou les services qui peuvent être créés par le projet.

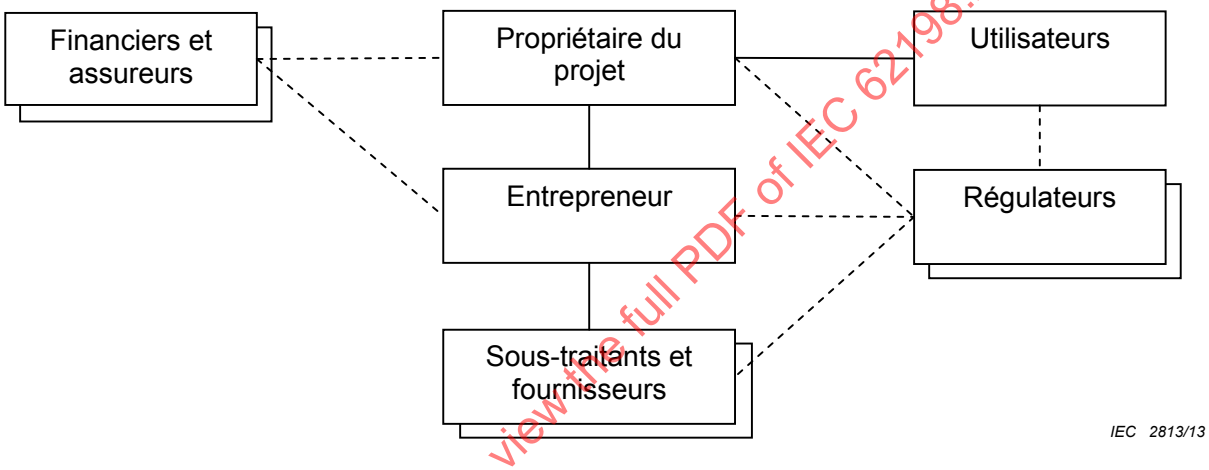


Figure 1 – Principales parties prenantes à un projet

5 Principes

Pour que le management du risque du projet soit efficace, il convient qu'un organisme respecte les principes à tous les niveaux comme indiqués ci-dessous.

a) Le management des risques crée de la valeur et la préserve

Le management des risques contribue de manière tangible à l'atteinte des objectifs et à l'amélioration des performances et de la qualité des projets et des actifs, produits et services qu'il génère. Les objectifs doivent être clairement compris par toutes les parties.

b) Le management des risques fait partie intégrante de tous les processus organisationnels liés à un projet

Le management des risques n'est pas une activité autonome distincte des activités et processus principaux du projet ou de l'organisme. Le management des risques fait partie des responsabilités dévolues aux chefs de projet et au personnel à tous les niveaux. Il s'agit d'une partie intégrante à tous les processus organisationnels liés à un projet, y compris les projets stratégiques et les prévisions d'investissement, la gestion de projet et la gestion des modifications apportées au projet.

c) Le management des risques est intégré aux processus de prise de décision

Le management des risques est une aide à la décision pour faire des choix éclairés concernant le projet, à chaque stade de son cycle de vie, définir des priorités et sélectionner les actions les plus appropriées. Cela implique qu'il convient que les décisions tiennent compte des risques.

d) Le management des risques traite explicitement de l'incertitude

Il convient que tous les gestionnaires tiennent compte de manière explicite de l'incertitude, de sa nature et de la manière de la traiter, notamment dans le cas de processus critiques.

e) Le management des risques est systématique, structuré et opportun

Une approche systématique, opportune et structurée du management des risques contribue à une prise de décision cohérente, comparable et fiable, à l'efficacité des processus de gestion de projet et aux bénéfices du projet. Il convient d'appliquer un cadre solide de management des risques dès le début du projet.

f) Le management des risques s'appuie sur les meilleures informations disponibles

Les entrées du processus de management des risques d'un projet reposent sur des sources d'informations telles que des analyses techniques, des contrôles de site et d'équipement, des résultats d'essai et des rapports d'avancement, complétés par des données historiques, des expériences, des commentaires de parties-prenantes, des prévisions et des jugements d'expert. Toutefois, il convient que les personnes concernées par le management des risques s'informent elles-mêmes et tiennent compte des limites des données ou de la modélisation utilisées, de l'incertitude des informations disponibles ou de la possibilité d'avis divergents entre les experts.

g) Le management des risques est adapté

Les activités de management des risques sont adaptées au type de projet, aux contextes interne et externe du projet et à ceux des organismes concernés, ainsi qu'au niveau d'incertitude et de complexité lié au projet. Le niveau d'effort de management des risques est fonction de la situation.

h) Le management des risques tient compte des facteurs humains et culturels

Le management des risques tient compte des capacités, des perceptions et des intentions des personnes et organismes qui peuvent aider ou empêcher d'atteindre les objectifs du projet.

i) Le management des risques est transparent et participatif

Une implication appropriée et opportune des parties-prenantes et, en particulier, des décisionnaires à tous les niveaux de l'organisation, garantit le caractère pertinent et actualisé du management des risques. Cela permet également aux parties-prenantes d'être correctement représentées et de tenir compte de leurs points de vue lors de la détermination des critères de risque.

j) Le management des risques est dynamique, itératif et réactif au changement

Au fur et à mesure de l'avancement d'un projet et de la survenue d'événements internes et externes connexes, le contexte et les connaissances changent, la surveillance et la revue se produisent, de nouveaux risques apparaissent, d'autres changent et d'autres encore disparaissent. Par conséquent, les activités de management des risques aident les décisionnaires à détecter de manière continue, comprendre et s'adapter aux changements.

k) Le management des risques facilite l'amélioration continue de l'organisation

Il convient que les organismes développent et mettent en œuvre des stratégies d'amélioration de la maturité de leur méthode de management des risques, ainsi que tous les autres aspects de leurs processus organisationnels.

6 Cadre organisationnel du management des risques liés à un projet

6.1 Généralités

Il convient d'intégrer les processus de management des risques liés à un projet à des processus de gestion de projet. Il convient que le cadre organisationnel de gestion de projet (c'est-à-dire la manière dont le processus de gestion de projet est organisé, structuré et contrôlé) établisse les fondements et dispositions qui caractérisent le management des risques tout au long du projet et dans toutes ses phases, à tous les niveaux et dans toutes les organisations concernées. Le succès du management des risques liés à un projet dépend de l'efficacité de cette intégration.

Le cadre organisationnel du management des risques liés à un projet s'inscrit dans un processus cohérent et efficace de management des risques (voir Article 7) à différents niveaux et dans le contexte particulier du projet. Il assure les bonnes transmissions et utilisation des informations relatives aux risques liés au projet déduites de ces processus pour la prise de décision, à tous les niveaux pertinents de l'organisation et du projet.

Cet article décrit les composants nécessaires au management des risques liés au projet et leur mise en corrélation itérative. La Figure 2 présente le cadre organisationnel de management des risques spécifié dans l'ISO 31000 et appliqué au management des risques des projets.

Ce cadre n'a pas pour objet d'imposer un système de gestion, mais plutôt d'aider l'organisation impliquée dans un projet à intégrer le management des risques liés à un projet dans le cadre organisationnel général de gestion de projet. Il convient donc que l'organisation adapte les composants de ce cadre en fonction de ses besoins particuliers et des exigences spécifiques au projet.

Si les pratiques et processus de gestion de projet existants d'une organisation incluent des composants de management des risques ou si l'organisation a déjà adopté un processus formel de management des risques liés à des projets, risques ou situations particuliers, il convient de les examiner et de les évaluer d'un œil critique par rapport à la présente norme afin de déterminer leur adéquation et leur efficacité.

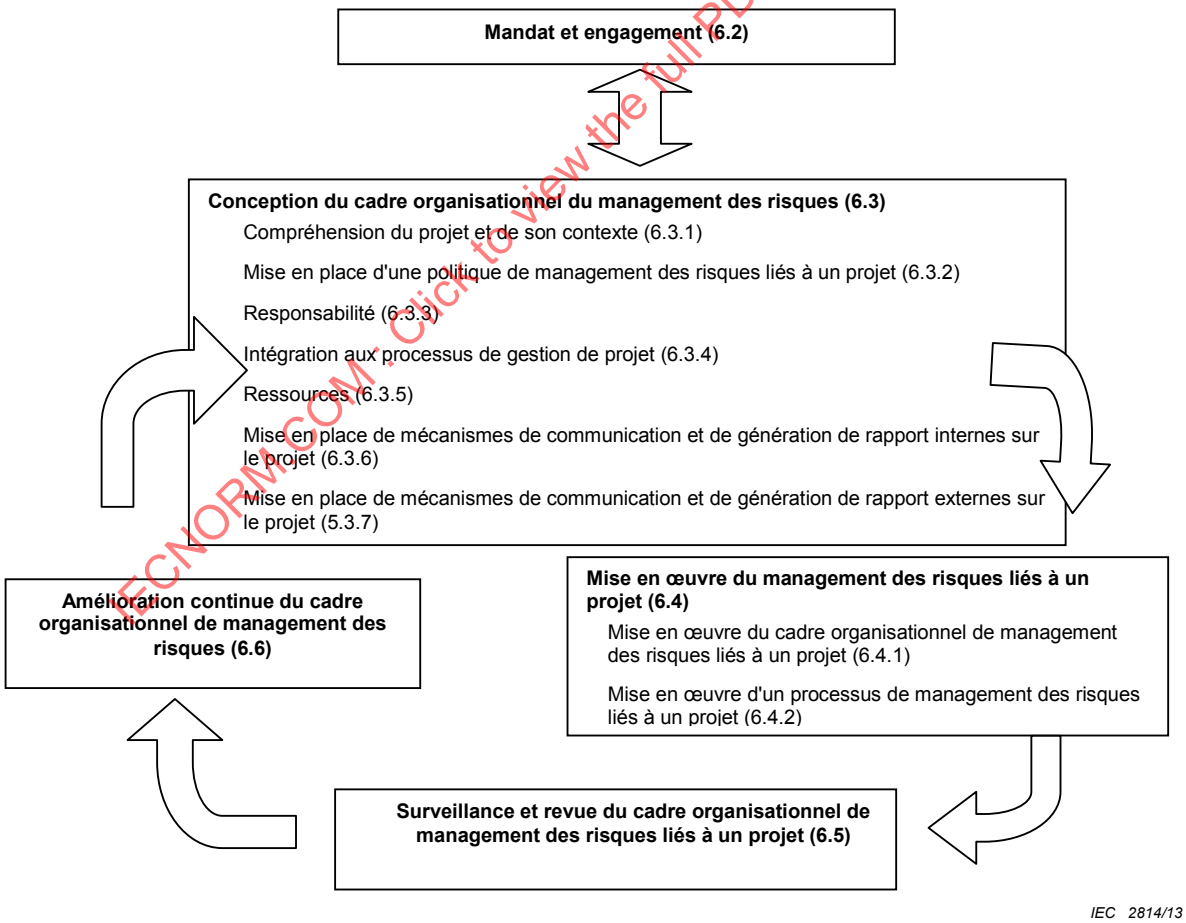


Figure 2 – Relations entre les composants du cadre organisationnel de management des risques, adaptées de l'ISO 31000

6.2 Mandat et engagement

L'introduction du management des risques et la garantie de son efficacité continue impliquent un engagement solide et prolongé du personnel de toute l'organisation impliquée dans le projet, y compris les propriétaires et les entrepreneurs essentiels, ainsi qu'une planification stratégique rigoureuse visant à permettre cet engagement à tous les niveaux. Il convient que la direction du propriétaire, de l'entrepreneur et du principal sous-traitant ou fournisseur

a) définisse et approuve une politique commune de management des risques pour le projet,

b) assure la concordance des cultures des organisations participantes et de la politique de management des risques liés au projet aussi rapidement que possible,

c) aligne les objectifs de management des risques liés au projet aux objectifs et stratégies des organisations concernées, notamment ceux de l'organisation qui en est à l'origine,

d) détermine les indicateurs de performances de management des risques liés au projet, alignés sur ceux du projet lui-même et des organisations concernées,

e) assure la conformité juridique et réglementaire,

f) attribue les responsabilités aux niveaux appropriés au sein des structures organisationnelles et dans le cadre de l'organisation du projet,

g) assure l'attribution des ressources nécessaires au management des risques liés au projet;

h) vérifie la mise en place des systèmes permettant de fournir les ressources nécessaires de manière opportune,

i) communique les avantages que présente le management des risques pour toutes les parties-prenantes au projet, et

j) s'assure que le cadre organisationnel de management des risques reste approprié au fur et à mesure de l'avancement du projet, dans toutes les phases de son cycle de vie.

Dans certains cas, les exigences en matière de management des risques peuvent être précisées dans les contrats.

6.3 Conception du cadre organisationnel de management des risques liés au projet

6.3.1 Compréhension du projet et de son contexte

Avant de concevoir et de mettre en œuvre le cadre organisationnel de management des risques, il est important d'évaluer et de comprendre les contextes externe et interne du projet, puisqu'ils peuvent avoir une influence significative sur la conception du cadre organisationnel.

L'évaluation du contexte externe du projet peut inclure, sans toutefois s'y limiter

a) l'environnement socioculturel, juridique, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local,

b) les principales tendances ayant un impact sur les objectifs ou la réalisation du projet, et

c) les relations, les perceptions et les valeurs des parties-prenantes externes, y compris toutes les organisations associées au projet (Figure 1).

L'évaluation du contexte interne du projet peut inclure, sans toutefois s'y limiter

d) l'objet et les objectifs du projet et la manière de les aligner avec ceux du propriétaire du projet et des utilisateurs de l'actif, des produits ou des services générés par le projet,

e) la gouvernance, les structures organisationnelles, les rôles et les responsabilités liés au projet et à ses performances,

f) les politiques, les objectifs et les stratégies en place pour les atteindre,

g) les capacités des organisations associées au projet, y compris la disponibilité et la capacité de leurs ressources et connaissances (capital, durée, personnes, processus, systèmes et technologies, par exemple),

h) les systèmes d'informations, les flux d'informations et les processus de prise de décision (formels et informels), et notamment les systèmes d'informations à utiliser pour assurer la gestion de projet, le contrôle et la génération de rapport,

i) les relations entre les parties-prenantes internes, ainsi que leurs perceptions et leurs valeurs,

j) les normes, lignes directrices et modèles adoptés par les organisations pour le projet, et

k) la forme et l'étendue des relations contractuelles entre les parties.

6.3.2 Mise en place d'une politique de management des risques liés à un projet

Il convient que la politique de management des risques liés au projet établisse clairement les objectifs et les engagements de management des risques dans toutes les organisations associées au projet. En règle générale, la politique porte sur les points suivants:

a) les raisons qui justifient le management des risques dans le projet;

b) les liens entre les objectifs et politiques des organisations et la politique de management des risques liés au projet;

c) les responsabilités en matière de management des risques liés au projet dans toutes les organisations concernées;

d) la manière de gérer les conflits d'intérêt;

e) l'engagement de mise à disposition des ressources nécessaires pour le management des risques pour encourager la prise de responsabilité au management des risques;

f) la mesure et le rapport des performances du management des risques liés au projet, et la manière de les lier à l'ensemble des performances du projet; et

g) l'engagement à examiner et améliorer régulièrement la politique et le cadre organisationnel du management des risques liés au projet, suite à des événements ou changements au fur et à mesure de l'avancement du projet.

Il convient de communiquer correctement la politique de management des risques aux différentes parties-prenantes.

La politique de management des risques pour un projet particulier peut faire partie d'un ensemble plus large de politiques de l'organisation.

6.3.3 Responsabilité

La responsabilité fait référence à l'obligation d'engagement et de résultats spécifiques. Il convient que les organisations impliquées dans un projet engagent leur responsabilité, leur autorité et leurs compétences en matière de management des risques tout au long du projet, et dans toutes ses phases. Il convient ainsi d'inclure la mise en œuvre et le maintien du processus de management des risques liés au projet, et de garantir l'adéquation, l'efficacité et l'efficience des contrôles. Cela peut être facilité par

a) l'identification des organisations et des propriétaires du risque qui ont la responsabilité du risque et l'autorité pour le gérer,

b) l'identification de la personne responsable du développement, de la mise en œuvre et du maintien du cadre organisationnel de management des risques liés au projet,

c) l'identification des autres responsabilités à tous les niveaux d'une organisation pour le processus de management des risques liés à un projet,

d) la mise en place de mesures de performances et de processus internes et externes de génération de rapport et de transmission à un niveau supérieur.

Dans la plupart des projets, un chef de projet est nommé avec un mandat particulier et des autorités déléguées, comprenant en général la responsabilité du management des risques liés à un projet. Selon l'importance et la complexité du projet, les activités de management des risques peuvent être réalisées par le chef de projet ou être déléguées. Ces responsabilités comprennent les points suivants:

1) définir les responsabilités de management des risques en fonction des différentes activités du projet;
2) mettre en place des mécanismes de communication dans le cadre du projet, et coordonner les informations et activités de management des risques;
3) établir le contexte du processus de management des risques;
4) gérer et signaler des activités d'appréciation du risque;
5) recommander, lancer, attribuer des responsabilités et surveiller la mise en œuvre efficace des activités de traitement du risque;
6) rechercher des décisions de la direction sur les problèmes de risque conflictuels;
7) communiquer de façon appropriée et en temps opportun les informations sur les questions relatives au risque tout au long du projet;
8) assurer que les plans d'urgence sont opérationnels;
9) identifier et noter tout problème concernant le management des risques;
10) surveiller le processus de management des risques et, si nécessaire, la mise en œuvre d'une action corrective;
11) fournir une documentation pour assurer la traçabilité.

Il convient que la responsabilité du management des risques liés à un projet et les interfaces avec d'autres fonctions soient définies et documentées. Il convient de préciser les principales responsabilités organisationnelles dans des documents contractuels.

6.3.4 Intégration aux processus de gestion de projet

Il convient que le management des risques soit intégré dans toutes les pratiques et tous les processus de gestion de projet de façon à être pertinent, opportun, efficace et efficient. Il convient que le processus de management des risques liés au projet fasse partie intégrante et ne soit pas séparé de ces processus de gestion de projet.

Il convient également d'intégrer le management des risques dans des processus organisationnels plus larges, y compris dans le cadre du développement d'une politique, de plans d'activités et de stratégies et leur revue, et dans les processus de gestion des changements.

Il convient de prévoir un plan de management des risques liés au projet afin d'assurer la mise en œuvre de la politique de management des risques et l'intégration du management des risques dans l'ensemble des pratiques et processus en la matière. Le plan de management des risques liés au projet peut être intégré dans d'autres plans (le plan d'exécution du projet, par exemple) d'une phase du projet.

6.3.5 Ressources

Il convient que les organisations impliquées dans un projet allouent les ressources nécessaires au management des risques liés au projet.

Il convient de prendre en compte:

a) les personnes, les aptitudes, l'expérience et les compétences;
b) les ressources nécessaires à chaque étape du processus de management des risques liés au projet;
c) les processus, méthodes, outils et systèmes de prise en charge des risques à utiliser pour le management des risques liés au projet;
d) les processus et procédures documentées en matière de management des risques;
e) les systèmes de gestion des informations et des connaissances;
f) les programmes de formation; et
g) l'allocation contractuelle des risques entre les organisations concernées.

Il convient que le budget du projet tienne compte du coût de la fonction de management des risques ainsi que les coûts des traitement de ces activités.

6.3.6 Mise en place de mécanismes de communication et de génération de rapport internes sur le projet

Il convient que les organisations impliquées dans un projet mettent en place des mécanismes de communication et de rapport internes visant à soutenir et encourager l'appropriation du risque à chaque étape du cycle de vie du projet. Il convient que ces mécanismes garantissent:

a) la communication appropriée des principaux composants du cadre organisationnel de management des risques, et de toutes modifications ultérieures;

b) l'existence de rapports appropriés sur le cadre organisationnel de management des risques, son efficacité et ses effets;

c) la disponibilité des informations pertinentes issues de l'application du management des risques liés au projet aux niveaux et aux moments opportuns dans toutes les organisations concernées, y compris entre les phases successives du projet; et

d) l'existence de processus de concertation entre les parties-prenantes.

Il convient que ces mécanismes comportent des processus permettant de rassembler les informations relatives aux risques liés au projet provenant, le cas échéant, de différentes sources, et tiennent compte de leur sensibilité. Dans certains cas, il convient d'intégrer le rapport de management des risques liés au projet dans des rapports de gestion de projet classiques.

6.3.7 Mise en place de mécanismes de communication et de génération de rapport externes sur le projet

Il convient que les organisations impliquées dans le projet élaborent et mettent en œuvre un plan coordonné sur la manière de communiquer avec les parties-prenantes externes. Il convient que cela implique:

a) la participation des parties-prenantes externes appropriées et l'assurance d'un échange efficace d'informations relatives au projet;

b) l'établissement de rapports externes conformes aux exigences légales et réglementaires, ainsi qu'aux exigences de gouvernance;

c) la mise en place d'un retour d'informations et de rapports sur la communication et la concertation;

d) l'utilisation de la communication pour renforcer la confiance dans les organisations concernées; et

e) la communication avec les parties-prenantes en cas de crise ou d'imprévus.

Il convient que ces mécanismes comportent des processus permettant de rassembler les informations relatives aux risques liés au projet provenant, le cas échéant, de différentes sources, et tiennent compte de leur sensibilité de manière opportune. Dans certains cas, il convient que la communication externe soit coordonnée et contrôlée par le propriétaire du projet, sauf si les entrepreneurs et fournisseurs sont liés par des exigences réglementaires particulières.

6.4 Mise en œuvre du management des risques liés à un projet

6.4.1 Mise en œuvre du cadre organisationnel de management des risques liés au projet

Pour la mise en œuvre du cadre organisationnel de management des risques liés à un projet, il convient que les organisations impliquées dans un projet

a) définissent un calendrier et une stratégie appropriés pour la mise en œuvre du cadre organisationnel dans le projet, en s'appuyant, dans la mesure du possible, sur les synergies des politiques et processus de management des risques de chaque organisation,

b) intègrent la politique et le processus de management des risques liés au projet dans les processus de gestion de projet,

c) se conforment aux exigences légales et réglementaires,

d) s'assurent que les prises de décision liées au projet, y compris l'élaboration et la détermination des objectifs, sont cohérentes avec les conclusions des processus de management des risques,

e) organisent des séances d'informations et de formation, et

f) communiquent et se concertent avec les parties-prenantes afin de s'assurer que le cadre organisationnel de management des risques liés au projet reste approprié.

6.4.2 Mise en œuvre d'un processus de management des risques liés à un projet

Il convient de mettre en œuvre le management des risques liés au projet en s'assurant que le processus de management des risques décrit à l'Article 7 est appliqué dans le cadre d'un plan de management des risques (voir 7.7.2) à tous les niveaux et toutes les fonctions pertinents des organisations concernées, dans le cadre de leurs pratiques et processus de gestion de projet.

Il convient d'élaborer le plan de management des risques très tôt dans le projet, et de l'intégrer dans le plan de gestion de projet. Il convient de définir le domaine d'application des processus de management des risques et les efforts qu'il convient de consentir aux différents stades du projet.

6.5 Surveillance et revue du cadre organisationnel de management des risques liés à un projet

Afin de s'assurer que le management des risques est efficace et contribue à l'atteinte des performances du projet, il convient que les organisations impliquées dans le projet

a) mesurent les performances de management des risques liés au projet en fonction d'indicateurs conformes aux indicateurs de performances du projet, et dont la pertinence est régulièrement revue,

b) mesurent régulièrement les progrès et les écarts par rapport au plan de management des risques,

c) examinent régulièrement si le cadre organisationnel, la politique et le plan de management des risques liés au projet sont toujours appropriés au vu du contexte interne et externe du projet et de l'avancement de sa phase actuelle,

d) établissent des rapports sur les risques liés au projet, sur les avancements du plan de management des risques et sur la manière dont la politique de management des risques est suivie, dans le cadre d'un rapport régulier sur le projet, et

e) vérifient l'efficacité du cadre organisationnel de management des risques liés à un projet.

Les indicateurs de performances pour le management des risques peuvent être

– des indicateurs de la réussite du projet, précisant dans quelle mesure les objectifs ont été atteints,

– des indicateurs de processus précisant dans quelle mesure les processus de management des risques sont respectés, et

– des indicateurs de risque précisant dans quelle mesure les traitements efficaces sont réalisés.

6.6 Amélioration continue du cadre organisationnel de management des risques liés au projet

En fonction des résultats de cette surveillance et de ces revues, il convient de prendre des décisions sur les possibilités d'amélioration du cadre organisationnel, de la politique et du plan de management des risques. Il convient que ces décisions entraînent des améliorations du management des risques liés au projet et de la culture du management des risques de l'organisation. Un processus de "leçons apprises" peut donner des informations à ce sujet.

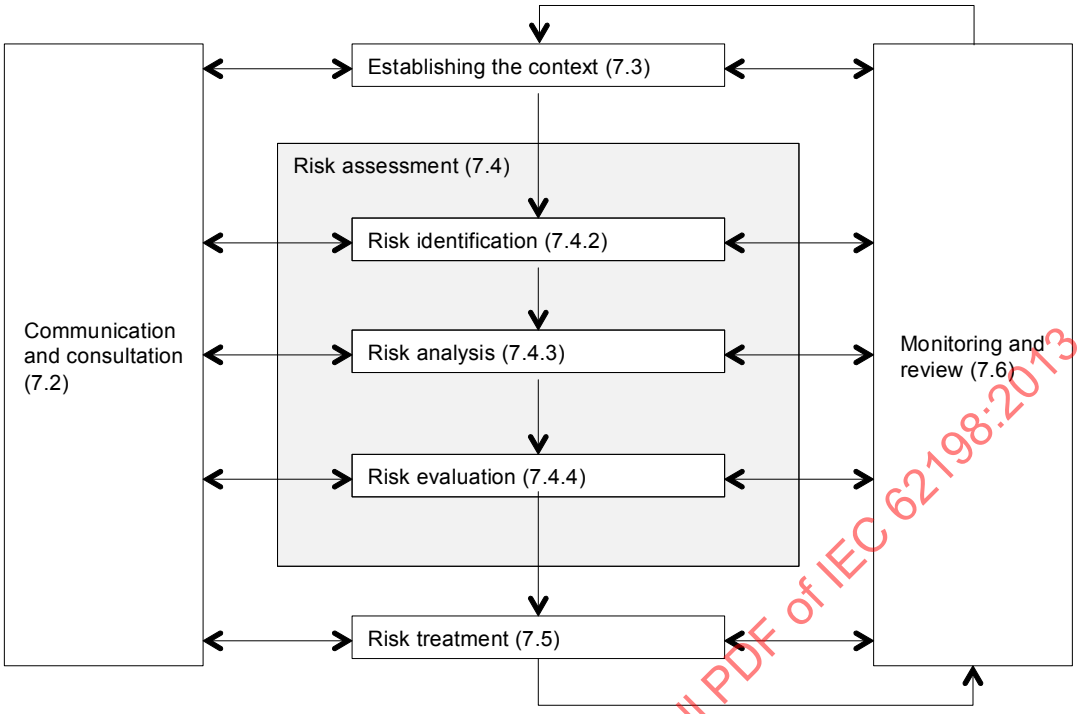
7 Processus de management des risques liés au projet

7.1 Généralités

Il convient que le processus de management des risques

– fasse partie intégrante de la gestion de projet,
– soit intégré dans la culture et les pratiques des organisations impliquées dans le projet, et
– soit adapté et intégré aux processus de gestion d'activité et de projet des organisations impliquées.

Il est composé des activités décrites de 7.2 à 7.7. Le processus de management des risques liés au projet est présenté en Figure 3.



Légende

Anglais	Français
Communication and consultation	Communication et concertation
Risk assessment	Appréciation du risque
Establishing the context	Établissement du contexte
Risk identification	Identification du risque
Risk analysis	Analyse du risque
Risk evaluation	Evaluation du risque
Risk treatment	Traitement du risque
Monitoring and review	Surveillance et revue

Figure 3 – Projet de processus de management des risques, adapté de l'ISO 31000

7.2 Communication et concertation

Il convient que la communication et la concertation avec les parties-prenantes externes et internes aient lieu à tous les stades du processus de management des risques. Il convient que l'efficacité de la communication et de la concertation externes et internes permette de s'assurer que les personnes responsables de la mise en œuvre du processus de management des risques liés au projet et que les parties-prenantes concernées comprennent l'objet et les objectifs du processus de management des risques, la base d'intégration des informations sur les risques liés au projet dans les décisions et les raisons justifiant des actions particulières.

La communication et la concertation avec les parties-prenantes sont importantes, leur jugement sur les risques étant fonction de leur propre perception des risques. Ces perceptions peuvent varier selon les différentes valeurs, leur culture, les besoins, les hypothèses, les concepts et les préoccupations. Leurs opinions pouvant avoir un impact significatif sur les décisions à prendre, il convient que la perception des parties-prenantes soit identifiée, enregistrée et prise en compte dans le processus de prise de décision.

Il convient que la communication et la concertation facilitent les échanges d'informations francs, pertinents, précis et compréhensibles, tenant compte de leur confidentialité et de l'intégrité personnelle.

Les effets de la communication et de la concertation entre les principales organisations impliquées dans un projet (Figure 1) peuvent être établis dans différents documents, y compris les contrats, les protocoles d'accord et les termes principaux d'un accord, ainsi que dans l'allocation convenue des responsabilités des risques spécifiques et contrôles des individus et des organisations participantes.

Il convient d'élaborer des plans de communication et de concertation très tôt dans le projet.

Une approche consultative en équipe peut

a) aider à définir correctement le contexte,
b) s'assurer que les intérêts des parties-prenantes sont compris et pris en considération,
c) s'assurer que les risques sont correctement identifiés,
d) réunir différents domaines d'expertise pour l'analyse des risques,
e) s'assurer que les différents points de vue sont pris en compte de manière appropriée dans la définition des critères de risque et dans l'appréciation des risques,
f) conforter l'adhésion et le soutien à un plan de traitement,
g) favoriser une gestion judicieuse des changements au cours du processus de management des risques, et
h) élaborer un plan de communication et de concertation interne et externe approprié.

Un management efficace des risques repose sur la disponibilité des données de différents domaines du projet sur l'ensemble de la durée de vie du projet. Il convient d'établir formellement et de maintenir les interfaces et les liens de communication entre le management des risques liés au projet et des domaines tels que

1) la conception et le développement,
2) les fonctions commerciales et de gestion de projet,
3) la maîtrise de configuration,
4) la qualité et la sûreté de fonctionnement,
5) un soutien postérieur au projet, y compris des utilisateurs et des gestionnaires.
6) Il convient de définir ces interfaces à un niveau suffisant d'autorité et de détail assurant une réaction rapide.

7.3 Etablissement du contexte

7.3.1 Généralités

En établissant le contexte, les organisations impliquées dans le projet énoncent clairement leurs objectifs et définissent les paramètres internes et externes à prendre en compte dans le management des risques liés au projet. Le contexte nécessite d'être compris afin de définir le domaine d'application, les critères de risque et la structure pour les étapes du processus de management des risques qui suivent.

Bien que la plupart de ces paramètres soient semblables à ceux pris en compte dans la conception du cadre organisationnel de management des risques liés au projet (voir 6.3), pour l'établissement du contexte du processus de management des risques, il convient de les examiner plus en détail. Leurs implications et la manière dont ils se rapportent au domaine d'application du projet et du processus de management des risques sont particulièrement importantes.

7.3.2 Etablissement du contexte externe

Le contexte externe est l'environnement externe dans lequel le projet est traité.

Il est important de comprendre le contexte externe afin de s'assurer que les objectifs et les préoccupations des parties-prenantes externes sont pris en compte lors de l'élaboration des critères de risque liés au projet. Il repose sur le contexte à l'échelle de l'organisation, avec toutefois des détails spécifiques découlant des exigences légales et réglementaires, des perceptions des parties-prenantes et d'autres aspects des risques propres au domaine d'application du projet.

Le contexte externe peut inclure, sans toutefois s'y limiter

– l'environnement socioculturel, politique, juridique, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local,
– les facteurs et tendances ayant un impact déterminant sur les objectifs du projet, et
– les relations avec les parties-prenantes externes, ainsi que leurs perceptions et leurs valeurs.

7.3.3 Etablissement du contexte interne

Le contexte interne est l'environnement interne dans lequel les organisations impliquées dans le projet cherchent à atteindre les objectifs du projet. Il s'agit d'un élément de l'organisation qui peut avoir une influence sur la manière de gérer les risques liés au projet. Il convient de l'établir car

– le management des risques liés au projet a lieu dans le contexte des objectifs des organisations,
– il convient que le processus de management des risques liés au projet soit conforme aux cultures, processus, structures et stratégies des organisations, et
– certaines organisations ne parviennent pas à identifier les opportunités leur permettant d'atteindre leurs objectifs en matière de stratégie, de projet ou d'activité, cela compromettant la continuité de l'engagement, de la crédibilité, de la confiance et des valeurs.

Le contexte interne peut inclure, sans toutefois s'y limiter

a) la gouvernance, les structures organisationnelles et les responsabilités,
b) les politiques, les objectifs et les stratégies en place pour les atteindre,
c) les aptitudes et les ressources (le capital, le temps, le personnel, les processus, les systèmes, les technologies, l'expertise et les connaissances, par exemple),
d) les relations avec les parties-prenantes internes, ainsi que leurs perceptions et leurs valeurs,
e) les systèmes d'information, les flux d'information et les processus de prise de décision (formels et informels),
f) les normes, lignes directrices et modèles adoptés par les organisations, et
g) la forme et l'étendue des relations contractuelles et autres entre les organisations impliquées.

7.3.4 Etablissement du contexte du processus de management des risques liés au projet

Il convient de fixer les objectifs, le domaine d'application et les paramètres des activités du projet ou des parties du projet dans lesquels le processus de management des risques s'applique. Il convient d'assurer le management des risques liés au projet en tenant compte de la nécessité de justifier les ressources servant à sa mise en œuvre. Il convient également de spécifier les ressources nécessaires, les responsabilités et autorités, ainsi que les enregistrements à conserver.

Le contexte du processus de management des risques varie selon les besoins liés au projet. Il peut inclure, sans toutefois s'y limiter

a) la définition du projet en termes d'activités et de processus à réaliser, d'actifs, de produits ou de services à créer, de ressources à engager, et de coût, de temps et de lieu,

b) l'identification et la spécification des décisions à prendre,

c) la définition du domaine d'application, ainsi que le degré et l'étendue des activités de management des risques liés au projet à entreprendre, y compris ce qui est spécifiquement inclus et exclus, et, lorsque cela est approprié les types de risques à adressés,

d) la définition des relations entre le projet spécifique et d'autres projets, processus ou activités des organisations concernées,

e) la définition des buts et objectifs des activités de management des risques liés au projet,

f) la définition des responsabilités dans le cadre du processus de management des risques liés au projet,

g) l'identification du domaine d'application ou du cadre organisationnel des études requises, leur étendue et leurs objectifs, ainsi que les ressources nécessaires à leur réalisation,

h) la définition des méthodologies d'appréciation des risques liés au projet,

i) la définition de la méthode d'évaluation des performances et de l'efficacité du processus de management des risques.

Il convient que la prise en compte de ces facteurs et des autres facteurs pertinents permette de s'assurer que l'approche adoptée du management des risques est adaptée aux circonstances, au projet et aux risques affectant l'atteinte des objectifs.

7.3.5 Définition des critères de risque

Il convient que les organisations impliquées dans un projet soient d'accord sur les critères de risque permettant d'évaluer l'importance du risque. Il convient que les critères reflètent les valeurs des organisations et des objectifs liés au projet. Certains critères peuvent être imposés ou résulter d'exigences légales et réglementaires ou d'autres exigences auxquelles les organisations répondent. Il convient que les critères de risque soient cohérents avec la politique de management des risques liés au projet (voir 6.3.2), soient définis au début du processus de management des risques et soient revus régulièrement.

Lors de la définition des critères de risque, il convient de tenir compte des facteurs suivants:

a) la nature et les types ou sources de causes et la manière dont la probabilité est définie;

b) la nature et les types de conséquences qui peuvent se produire et la manière de mesurer leurs impacts;

c) les délais de survenue des conséquences;

d) la manière de déterminer le niveau de risque;

e) le niveau auquel le risque devient acceptable ou tolérable; et

f) s'il convient de prendre en compte ou non les combinaisons de plusieurs risques et, le cas échéant, la méthode à utiliser et les combinaisons à considérer.

Il convient de tenir compte du point de vue des parties-prenantes lors de la définition des critères.

Il convient que les mesures de l'impact des risques tiennent compte de tous les objectifs du projet, à savoir

1) les objectifs commerciaux et liés à l'activité des organisations impliquées dans le projet,

2) l'atteinte des cibles en matière de coût et de planification liés au projet,

3) la qualité, la sûreté de fonctionnement et les performances des actifs, produits ou services créés par le projet,
4) la santé et la sécurité des parties-prenantes au projet,
5) la protection et l'amélioration de l'environnement, et
6) la conformité statutaire et réglementaire.

Il convient d'établir les critères d'acceptation et de tolérance des risques. Ces critères sont utilisés pour évaluer les conséquences des risques dans les étapes ultérieures du processus.

7.3.6 Eléments essentiels

Pour assurer l'exhaustivité de l'identification des risques et faire en sorte de ne pas oublier des risques importants, il est fréquent de diviser le projet en un ensemble d'éléments essentiels permettant d'organiser l'activité d'identification des risques.

Il existe plusieurs méthodes de génération d'une structure d'éléments essentiels, selon la nature du projet et l'objectif, le domaine d'application et la définition de l'évaluation. Par exemple, les éléments essentiels peuvent reposer sur un ou plusieurs des éléments ci-dessous:

a) le WBS (organigramme des tâches, *en anglais: work breakdown structure*) de projet, une structure générale de répartition des risques, de répartition fonctionnelle, de répartition des paramètres ou de répartition des coûts relatifs au projet;
b) les autres phases du cycle de vie du projet;
c) les principales rubriques des informations relatives au projet à fournir aux décisionnaires au stade suivant;
d) les composants d'un actif, d'un produit ou d'un service créé par un projet;
e) les zones du site d'un projet;
f) les contrats et contrats de sous-traitance ou les termes d'un contrat;
g) les composants d'une structure organisationnelle.

La structure d'éléments essentiels permet aux personnes chargées de l'identification des risques de se concentrer sur chaque élément essentiel, et d'approfondir leur réflexion dans une plus large mesure que si elles avaient abordé le projet de manière plus globale. Un ensemble d'éléments essentiels bien défini stimule la créativité.

Le développement des éléments essentiels permet également d'identifier si certains domaines d'expertise particuliers nécessitent d'appréhender certains éléments spécifiques, permettant d'intégrer cette expertise dans l'équipe chargée de l'identification des risques lorsqu'elle traite l'élément considéré.

7.4 Appréciation du risque

7.4.1 Généralités

L'appréciation du risque est le processus global d'identification, d'analyse et d'évaluation des risques. Elle a pour objet d'identifier les risques susceptibles d'avoir un impact, positifs ou négatifs, sur les objectifs du projet, de comprendre comment ils peuvent se produire et de définir les priorités pour les résoudre.

7.4.2 Identification du risque

Le but de l'identification des risques est de détecter, répertorier et caractériser les risques qui peuvent porter atteinte, de manière positive ou négative, à la réalisation des objectifs liés au projet retenus d'un commun accord.

Il convient que l'identification des risques tienne compte des sources de risque, des domaines d'impact, des événements (y compris les changements de circonstance) et de leurs causes et conséquences potentielles. Cette étape a pour objectif de dresser une liste exhaustive des risques en fonction des événements, circonstances ou changements susceptibles de créer, d'améliorer, d'empêcher, de gêner, d'accélérer ou de retarder l'atteinte des objectifs liés au projet. Il est également important d'identifier les risques liés à une opportunité qui n'a pas été saisie. Il est essentiel de procéder à une identification exhaustive, car un risque non identifié à ce stade ne peut pas être inclus dans une analyse, avant que l'itération suivante ne soit entreprise.

Il convient que l'identification des risques considère l'impact des risques sur tous les objectifs du projet.

Une gestion efficace des risques liés à un projet dépend fondamentalement de l'identification exhaustive des risques. Cela implique un processus systématique.

Différentes méthodes permettent d'identifier des risques. Il convient de sélectionner les outils et techniques les mieux adaptés aux objectifs du projet, aux capacités organisationnelles et aux types de risques prévus. Il peut s'agir

a) de brainstorming dans la structure des éléments essentiels,
b) d'avis d'expert,
c) d'entretiens et de questionnaires,
d) de listes de contrôle,
e) de données historiques,
f) d'expérience précédente des participants et suite à d'autres projets,
g) d'essai et de modélisation,
h) de techniques formelles telles que l'AMDE (analyse des modes de défaillance et de leurs effets) ou l'HAZOP (*en anglais: hazard and operability studies*).

Il convient que l'identification inclue les risques, que leur source soit ou non sous le contrôle des organisations impliquées dans le projet, même si la source ou la cause peut ne pas être immédiatement évidente. Il convient que l'identification des risques comporte l'examen des réactions en chaîne et des effets cumulés des conséquences particulières. Il convient de tenir compte de toutes les causes et conséquences significatives.

Il est important d'utiliser des informations pertinentes et à jour pour identifier les risques. Dans la mesure du possible, il convient d'inclure des données historiques appropriées. Il convient que les personnes ayant les connaissances appropriées participent à l'identification des risques. Il convient que l'identification des risques fasse appel à toutes les sources d'information disponibles.

L'objectif de l'identification des risques varie selon les phases du projet. Dans les premières phases, l'identification porte souvent sur les risques élevés, généraux et stratégiques, ainsi que sur les "défauts graves" pouvant compromettre le succès du projet. Dans les phases ultérieures, l'identification porte sur des risques beaucoup plus spécifiques.

Il convient que l'identification des risques tienne compte des phases restantes du cycle de vie du projet, et de celui de l'actif, du produit ou du service créé par le projet. Il convient d'impliquer dans le processus d'identification des risques les parties-prenantes et les experts techniques aux connaissances adaptées en la matière.

Au fur et à mesure de l'avancement du projet, certains risques étant résolus et d'autres apparaissant, il convient que l'identification des risques soit un processus continu. Certains risques identifiés dans les premières phases du projet restent d'actualité dans les phases ultérieures. Il est donc important de conserver ces risques au fur et à mesure de l'avancement du projet.

Il convient que les risques soient enregistrés. C'est en général consigné dans un registre des risques liés au projet (voir 7.7.4).

7.4.3 Analyse de risque

L'analyse de risque implique de bien comprendre chaque risque, ses causes et conséquences, ainsi que la manière dont ils peuvent se produire. L'analyse de risque fournit des données pour évaluer les risques et prendre la décision de les traiter ou non, et permet de choisir les stratégies et méthodes de traitement les plus appropriées. L'analyse de risque peut également contribuer à la prise de décision quant aux choix qui doivent être faits et aux options impliquant les différents types et niveaux de risque.

L'analyse de risque implique la prise en compte des causes et sources de risque, de leurs conséquences positives ou négatives sur les objectifs du projet, et de la probabilité de survenue de ces conséquences. Il convient d'identifier les facteurs affectant les conséquences et leur probabilité. Il convient de tenir compte des contrôles du projet et de leur efficacité.

Un risque peut avoir des conséquences multiples liées à plusieurs objectifs du projet.

Il convient que la manière dont les conséquences et leur probabilité sont exprimées, ainsi que la manière dont elles sont combinées afin de déterminer un niveau de risque, correspondent au type de risque, aux informations disponibles et à l'objectif de l'appréciation du risque. Il convient de veiller à la cohérence avec les critères de risque. Il est également important de tenir compte de l'interdépendance des différents risques et de leurs sources.

Il convient que le degré de confiance dans la détermination du niveau de risque et de sa sensibilité à des conditions préalables et à des hypothèses soit pris en compte dans l'analyse, et communiqué effectivement aux décideurs et, le cas échéant, aux autres parties-prenantes. Il convient d'établir, voire de mettre en évidence, des facteurs tels que les divergences d'opinion entre experts, l'incertitude, la disponibilité, la qualité, la quantité et la pertinence continue des informations ou les limites de modélisation.

Les risques peuvent être analysés à différents niveaux de détail, en fonction du risque, de l'objectif de l'analyse et des informations, données et ressources disponibles. Il peut être nécessaire de reprendre le processus d'identification de risque lors de l'analyse afin de poursuivre la clarification des risques liés au projet.

L'analyse peut être qualitative et/ou quantitative, selon les circonstances. Des approches d'analyse qualitatives et quantitatives peuvent être utilisées dans toutes les phases du projet, mais ils font des contributions différentes dans des phases différentes. Par exemple, l'analyse qualitative des risques peut être réalisée très tôt dans le cycle de vie du projet afin de prendre en charge les décisions stratégiques, l'analyse quantitative pouvant avoir lieu plus tard pour prendre en charge le développement des coûts et du budget. D'autres analyses de l'incertitude (l'évaluation du coût de la sûreté de fonctionnement et du cycle de vie, par exemple) peuvent être réalisées dans le cadre de la sélection des options du projet et de la conception détaillée aux phases pertinentes du projet.

7.4.4 Evaluation du risque

L'évaluation du risque a pour objet de faciliter la prise de décision, en fonction des résultats de l'analyse de risque, quant aux risques devant être traités et à la priorité de mise en œuvre du traitement.

L'évaluation du risque consiste à comparer les résultats de l'analyse aux critères de risque établis lors de l'établissement du contexte. Sur la base de cette comparaison, il est possible d'étudier la nécessité d'un traitement.

L'évaluation peut impliquer d'équilibrer un large éventail de risques différents présentant des résultats positifs et négatifs, afin de prendre une décision quant à la poursuite d'un projet ou à la démarche à adopter dans le cadre d'un projet.

Dans certains cas, l'évaluation du risque peut donner lieu à la décision de procéder à une analyse plus approfondie. Par exemple, dans les premières phases d'un projet, l'analyse de risque peut aider à développer des plans de travail pour les études à réaliser dans les phases suivantes du projet.

7.5 Traitement du risque

7.5.1 Généralités

Le traitement du risque implique le choix d'une ou de plusieurs options de modification des risques, et la mise en œuvre de ces options. Une fois mis en œuvre, les traitements engendrent ou modifient les moyens de maîtrise du risque.

Certains risques peuvent être acceptés sans autre traitement que le maintien des moyens de maîtrise du risque existants. Il convient que ces risques soient inclus dans le registre des risques de telle sorte que la surveillance qui les concerne puisse être accomplie. Les risques qui ne sont pas acceptés sont traités.

Il convient que les décisions tiennent compte du contexte élargi du risque, et considèrent la tolérance au risque des parties autres que l'organisation à laquelle profite le risque. Il convient que les décisions respectent les obligations légales, réglementaires et autres exigences.

Le traitement du risque implique un processus cyclique: suite aux actions de traitement initial, les risques sont de nouveau évalués pour voir s'ils sont acceptables avec les nouveaux traitements et, si ce n'est pas le cas, un traitement supplémentaire est réalisé.

7.5.2 Sélection des options de traitement du risque

Les options de traitement du risque peuvent être les suivantes:

a) éviter un risque aux conséquences négatives en supprimant la source du risque ou en décidant de ne pas commencer ou poursuivre l'activité qui a engendré le risque (voire en interrompant le projet);

b) engager une activité qui peut donner lieu à des risques aux conséquences positives afin de saisir une opportunité (y compris en modifiant le domaine d'application ou les objectifs du projet);

c) entreprendre une action qui modifie la probabilité du risque, afin d'augmenter les probabilités de conséquences positives et de réduire celles de conséquences négatives;

d) entreprendre une action qui modifie les conséquences du risque, afin d'augmenter les chances de conséquences positives et de réduire celles de conséquences négatives;

e) partager le risque avec une ou plusieurs autres parties (y compris par des contrats, une assurance ou un financement du risque); et

f) maintenir le risque fondé sur une décision argumentée.

Les décisions relatives au traitement du risque suivent une séquence simple:

1) si les conséquences d'un risque vont à l'encontre des exigences légales ou réglementaires, une action est requise;

2) si les conséquences d'un risque vont à l'encontre d'une politique organisationnelle ou dépassent les critères de risque élaborés lors de l'établissement du contexte, une action est en général requise;

3) si les conséquences d'un risque présentent des implications dangereuses pour la santé et la sécurité des personnes, le risque doit être traité, le critère correspondant de sélection

des tâches de traitement étant au niveau le "plus faible qu'il est raisonnablement possible d'atteindre";

4) dans tous les autres cas, il convient d'entreprendre des actions uniquement si les avantages et inconvénients globaux pour le projet dépassent les coûts et inconvénients globaux, compte tenu de tous les avantages et inconvénients sur l'ensemble du projet.

Les options de traitement du risque ne s'excluent mutuellement ni ne s'appliquent à un seul risque. Un certain nombre d'options de traitement peuvent être prises en compte et appliquées individuellement ou en combinaison. Il peut souvent être avantageux pour le projet d'adopter une combinaison d'options de traitement.

Lors de la sélection des options de traitement, les valeurs et perceptions des parties-prenantes, ainsi que la plupart des moyens de communication avec elles, peuvent être des considérations pratiques importantes. A efficacité égale pour le projet, certains traitements du risque peuvent être plus acceptables que d'autres pour certaines parties-prenantes.

La mise en œuvre des actions de traitement du risque peut introduire de nouveaux risques qu'il convient également de prendre en compte. Il convient d'évaluer, de traiter, de surveiller et de revoir ces risques secondaires.

7.5.3 Plans de traitement du risque

Les plans de traitement du risque ont pour objet de documenter les options de traitement sélectionnées et la manière dont elles sont mises en œuvre. Il convient que les informations fournies dans les plans de traitement comportent:

a) les raisons ayant motivé la sélection des options de traitement, y compris les avantages attendus;

b) les personnes responsables de l'approbation du plan et celles responsables de la mise en œuvre du plan;

c) les actions proposées et leur priorité;

d) les exigences en matière de ressource, y compris les impondérables;

e) la mesure des performances et les contraintes;

f) les exigences en matière de rapports et de surveillance; et

g) le calendrier et la planification.

Pour chaque traitement du risque, il convient de désigner une personne chargée de ce traitement (propriétaire de la tâche). La personne la plus indiquée peut être:

1) celle qui est responsable de l'activité qui est à l'origine du risque;

2) celle qui peut maîtriser au mieux la probabilité d'occurrence du risque;

3) celle la mieux placée pour réagir à l'occurrence du risque ou modifier ses conséquences;

4) celle qui a le niveau approprié de responsabilité pour traiter le risque.

Il convient d'intégrer les plans de traitement au plan de gestion du projet.

7.6 Surveillance et revue

Il convient de planifier la surveillance et la revue dans le cadre du processus de management des risques liés au projet, et de les intégrer aux autres aspects liés à la surveillance et la maîtrise normales du projet.

Il convient de clairement définir les responsabilités en matière de surveillance et de revue.

Il convient d'appliquer les processus de surveillance et de revue à tous les aspects du processus de management des risques afin de pouvoir

a) détecter les changements de contexte externe et interne, y compris les changements du domaine d'application, des objectifs ou des critères de risque du projet qui peuvent nécessiter une révision des risques, des traitements du risque et des priorités,

b) obtenir des informations supplémentaires pour améliorer l'appréciation du risque,

c) s'assurer de l'efficacité et de l'efficience des moyens de maîtrise, tant sur le plan de leur conception que de leur fonctionnement,

d) analyser et tirer les leçons des succès et des échecs (y compris les incidents et quasi-accidents), des changements et des tendances, et

e) identifier les risques émergents.

Il convient d'intégrer les activités de traitement du risque au plan du projet et de les surveiller dans le cadre d'activités de contrôle régulier du projet. Il convient d'intégrer l'avancement de la mise en œuvre des tâches de traitement des risques à la gestion globale des performances du projet, à leur mesure et aux activités de génération de rapports externes et internes.

A la fin du projet, il est utile, s'il y un contrôle de l'efficacité du contrôle, de tirer les leçons et le retour d'expérience dans les projets à venir pouvant faire l'objet d'un examen postérieur au projet. Il est important que cette activité commence pendant le projet, de sorte qu'elle ne soit pas laissée en suspens jusqu'à la fin du projet et que la personne compétente en la matière ne soit pas déjà en charge d'un autre projet.

Il convient que les résultats de la surveillance et de la revue soient enregistrés et fassent l'objet d'un rapport, selon le cas. Il convient qu'ils servent de données à la revue du cadre organisationnel de management des risques (voir 6.5).

7.7 Enregistrement et rapport d'un processus de management des risques liés à un projet

7.7.1 Rapport

Il est nécessaire d'établir des rapports sur les problèmes liés au risque afin de servir de base à la prise de décision relative à la gestion, et pour vérifier que les objectifs du projet sont réalisables. Toutes les réunions traitant du projet sont une opportunité de discuter et de résoudre les questions sur le risque. Les réunions consacrées au projet peuvent être formelles ou informelles, mais il convient que toutes les discussions et toutes les décisions relatives aux risques soient enregistrées et fassent l'objet d'un rapport.

Les discussions relatives aux questions sur le risque peuvent inclure les aspects suivants ci-joint:

a) identification et appréciation des risques nouveaux ou émergents;

b) revue du registre des risques liés au projet;

c) revue du statut des risques, de l'efficacité des contrôles associés et de la mise en œuvre des activités de traitement du risque;

d) identification et reconnaissance des modifications apportées aux informations concernant le risque, ainsi qu'une nouvelle analyse des modifications et de la mise à jour du registre des risques;

e) estimation de l'efficacité du processus de management du risque;

f) discussion des relations entre les parties liées par contrat, incluant les allocation des risques.

Des indicateurs de performances spécifiques peuvent être élaborés pour la plupart des points ci-dessus.

Il convient que le plan de management du risque spécifie les exigences en matière de rapport. Dans la mesure du possible, il convient d'intégrer le rapport de management du risque à d'autres formes de rapport de gestion de projet.

7.7.2 Plan de management des risques liés à un projet

Le plan de management des risques liés au projet décrit le processus structuré de management du risque à appliquer au projet.

Le management des risques liés au projet peut faire partie intégrante du plan de management du projet ou peut être un document séparé. Il peut inclure ou faire référence

a) au contexte et aux limites du management des risques liés au projet, y compris ses objectifs,

b) au cadre organisationnel, aux processus et aux interfaces de management des risques liés au projet,

c) aux responsabilités en matière d'activités de management des risques, aux autorités et aux lignes de compte rendu,

d) à des interfaces internes et externes,

e) au planning des réunions de management des risques liés au projet (souvent conforme, en totalité ou en partie, aux réunions de gestion de projet normales),

f) aux processus de revue des risques liés au projet,

g) aux liens avec tout autre document ou avec d'autres plans du projet,

h) aux procédures d'organisation appropriées,

i) aux interfaces avec les plans de management des risques ayant d'autres origines, selon le cas (pour les fournisseurs et sous-traitants, par exemple),

j) au format du registre des risques liés au projet.

Il convient que le plan soit révisé régulièrement et mis à jour si nécessaire.

7.7.3 Documentation

Une documentation est nécessaire pour faciliter la mise en œuvre et la maîtrise du processus de management des risques, notamment sur l'ensemble des phases du cycle de vie du produit.

La documentation vient en aide à la planification, à l'évaluation de l'avancement et à la traçabilité. Il convient de documenter le processus de management des risques, ainsi que les risques et leur traitement. Dans le processus de management des risques liés au projet, les enregistrements sont la pierre angulaire de l'amélioration des méthodes et des outils, ainsi que de l'ensemble du processus.

Il convient que les décisions concernant la création des enregistrements tiennent compte

a) des besoins de l'organisation en matière d'apprentissage continu,

b) des avantages que présente la réutilisation des informations pour les besoins de la gestion de projet,

c) des coûts et des efforts nécessaires à la création et au maintien des enregistrements,

d) des exigences légales, réglementaires et opérationnelles liées aux enregistrements,

e) de la méthode d'accès, de la facilité de consultation et du support de stockage,

f) de la période de conservation, et

g) de la sensibilité des informations.

7.7.4 Registre des risques liés au projet

Le registre des risques liés au projet est un document particulièrement important. Il s'agit d'un support qui sert à consigner les modifications apportées à l'état des risques. Son contenu est la base des rapports réguliers au niveau de la gestion de projet et pour la discussion des risques et leur traitement lors des réunions consacrées au projet.