BRITISH STANDARD

BS IEC
62198:2001

Project risk management — Application guidelines

ICS 03.100.01

National foreword

This British Standard reproduces verbatim IEC 62198:2001 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability and terotechnology, which has the responsibility to:

— aid enquirers to understand the text;

— present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;

— monitor related international and European developments and promulgate them in the UK.

The business aspects of project risk are dealt with by BS 6079-3:2000, Project management - Part 3: Guide to the management of business related project risk. BS 6079-3 includes guidance on defining business relationships; modelling techniques for business related risks; and the application of stakeholder analysis; and complements this standard.

A list of organizations represented on this committee can be obtained on request to its secretary.

From 1 January 1997, all IEC publications have the number 60000 added to the old number. For instance, IEC 27-1 has been renumbered as IEC 60027-1. For a period of time during the change over from one numbering system to the other, publications may contain identifiers from both systems.

Cross-references

The British Standards which implement international publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled "International Standards Correspondence Index", or by using the "Find" facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

This British Standard, having been prepared under the direction of the Management Systems Sector Policy and Strategy Committee, was published under the authority of the Standards Policy and Strategy Committee and comes into effect on 14 February 2002

Summary of pages

This document comprises a front cover, an inside front cover, the IEC title page, pages 2 to 19, and a back cover.

The BSI copyright date displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

ISBN 0 580 39019 5

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
62198

Première édition
First edition
2001-04

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

Project risk management – Application guidelines

Numéro de référence
Reference number
CEI/IEC 62198:2001

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

PROJECT RISK MANAGEMENT – APPLICATION GUIDELINES

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The 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.

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

FDIS	Report on voting
56/727/FDIS	56/732/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 3.

Annex A is for information only.

The committee has decided that the contents of this publication will remain unchanged until 2007. At this date, the publication will be

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

INTRODUCTION

Risk management is the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, assessing, treating, monitoring and communicating risks in a way that will enable organizations to minimize loss and maximize opportunity in a cost-effective way. This International Standard is concerned with the application of risk management to a project.

Project management and its related processes are described in ISO 10006. Every project involves risk. Project risks are related to the project itself and to its product. Examples of risk factors affecting a project are shown in figure 1.

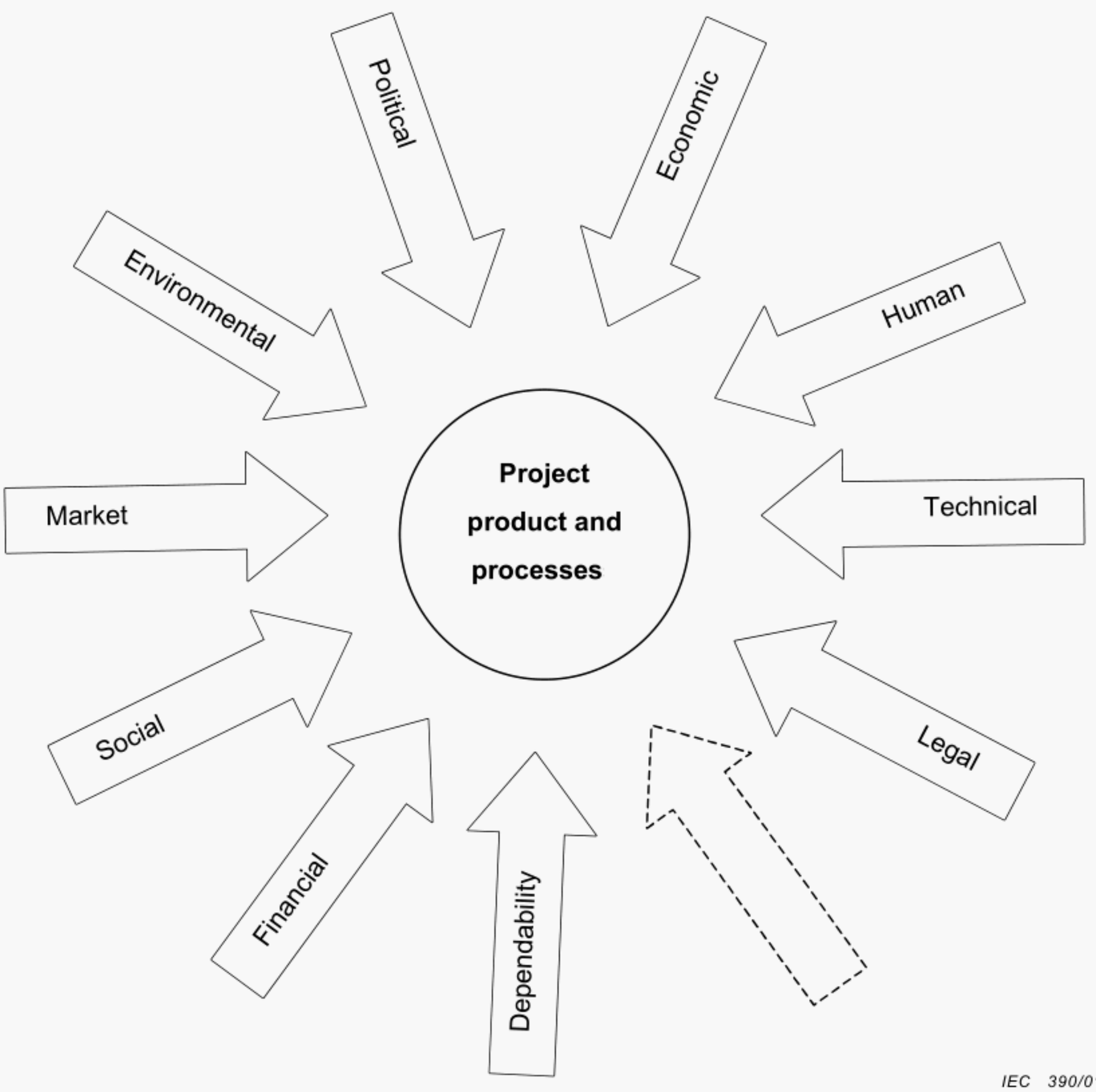


Figure 1 – Examples of risk issues affecting a project

This standard provides a process for managing risks in a systematic and consistent way. To obtain maximum benefit, risk management activities are initiated at the earliest possible phase of a project and continued through subsequent phases.

The intended users of this standard are decision-makers, including project managers, risk managers and business managers.

The application of this standard needs to be tailored to each specific project. Therefore, it is considered wholly inappropriate to impose a certification system for risk management practitioners.

This standard does not deal specifically with safety-related issues. While application of this standard may raise safety-related issues, management of these risks is dealt with in safety group standards or product standards and not in this standard.

PROJECT RISK MANAGEMENT – APPLICATION GUIDELINES

1 Scope

This International Standard is applicable to any project with a technological content. It may also apply to other projects.

It provides a general introduction to project risk management, its subprocesses and influencing factors. These subprocesses are:

- establishing the context, including confirmation of project objectives;
- risk identification;
- risk assessment, including risk analysis and evaluation;
- risk treatment;
- review and monitoring;
- communication (including consultation);
- learning from the project.

Guidelines are provided on the organizational requirements for implementing the process of risk management appropriate to the various phases of a project.

It is recognized that, in certain circumstances, it may be inappropriate to include all the clauses of this standard within a contract. Accordingly, this standard should only be considered as forming part of a contract – however that contract may be formed – if the parties to that contract explicitly call upon and refer to this standard (or parts thereof) and require it to be included within the contract.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 60050(191):1990, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 60300-3-3:1996, *Dependability management – Part 3-3: Application guide – Life cycle costing*

IEC 60812:1985, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61025:1990, *Fault tree analysis (FTA)*

ISO 10006:1997, *Quality management – Guidelines to quality in project management*

3 Definitions

For the purposes of this International Standard, the terms and definitions of IEC 60050(191) apply, together with the following.

3.1
product
results of an activity or process which may include service, hardware, processed materials, software or a combination thereof

3.2
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 An individual project may form part of a larger project structure.

NOTE 2 In some projects, the objective(s) is (are) refined and the product characteristics defined progressively as the project proceeds.

[ISO 10006]

3.3
process
set of inter-related resources and activities which transform inputs into outputs

[ISO 10006]

3.4
project risk
combination of the probability of an event occurring and its consequences for project objectives

3.5
risk management
systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk

3.6
risk treatment
process of selection and implementation of measures to modify risk

NOTE 1 The term "risk treatment" is sometimes used for measures themselves.

NOTE 2 Risk treatment measures may include avoiding, optimizing, transferring or retaining risk.

4 Project risk management overview

4.1 Role of risk management in a project

Risk is associated with every project and with each process and each decision throughout the life of a project. Risk should therefore be managed at each stage of the project and the risk management process should be integrated with both the project management processes and the product-related processes. Everyone is involved in risk management. A structured process of risk management is required in order to facilitate open communication and cost-effective management of risks.

A prerequisite of effective project risk management is frank and open communication both inside and outside the project.

4.2 Outline of the process

The project risk management process starts by establishing the context in which the project is undertaken. This includes identifying the interested parties, understanding the objectives and outputs of the project and defining the scope and boundaries of the risk management activity for a particular project. The interface to, and overlap with, any other projects and the organizational and strategic constraints within which the project operates, should be defined.

The next step in the risk management process is risk identification. This task is fundamental to the risk management process.

Each identified risk should be subjected to subsequent project risk management activities of risk assessment, risk treatment and review and monitoring.

The process may be applied first at a broad level to identify general risk issues, then at a more detailed level to look at particular risks and how they might arise. Risks should be managed at each phase of the project and risks to the project itself and to its product should be reviewed.

The concept of the project risk management process is illustrated in figure 2.

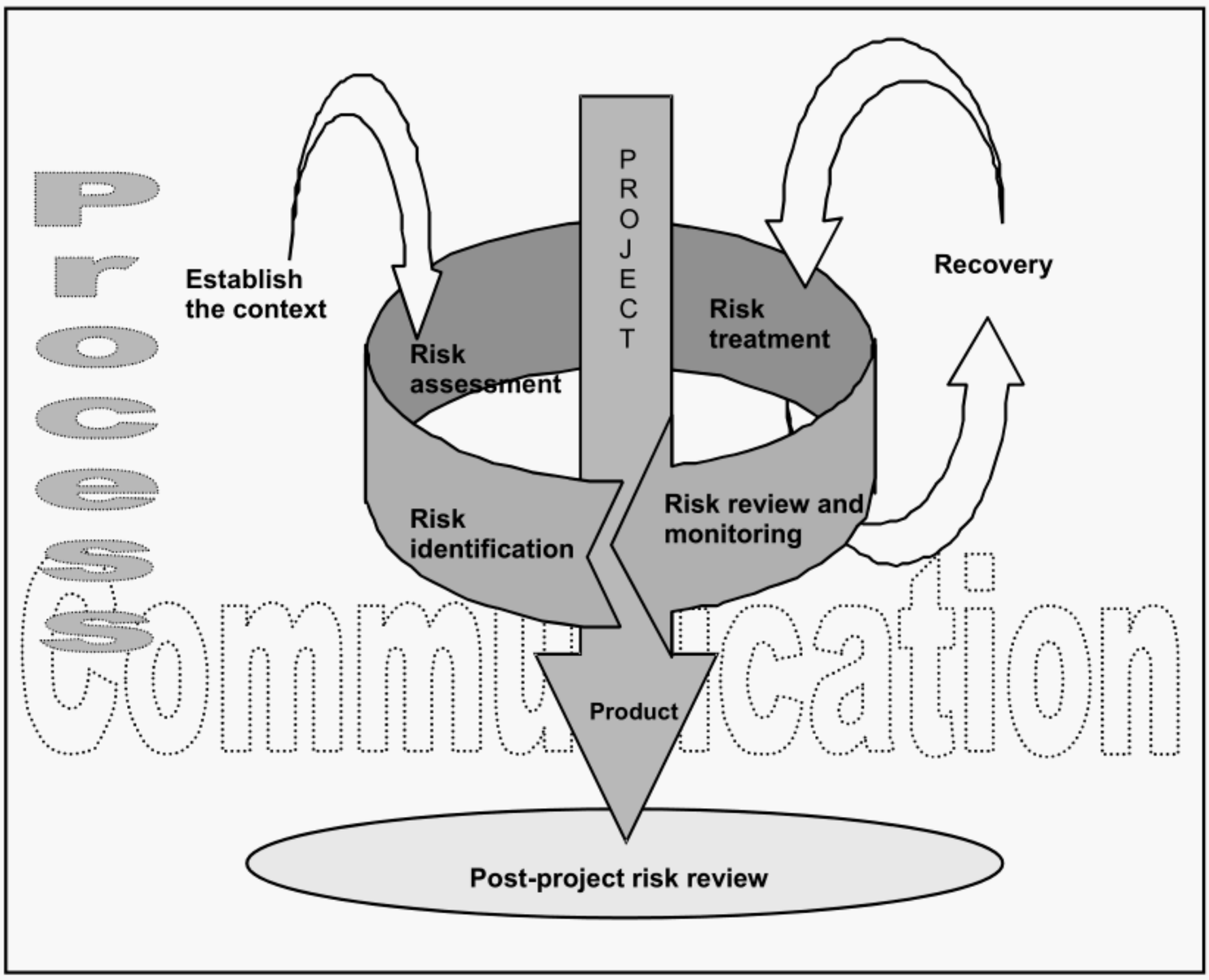


Figure 2 – Project risk management concept

5 Organizational issues

5.1 Management responsibilities

The project manager is responsible for the project risk management tasks as a part of the overall project management function. Depending upon the size and complexity of the project, risk management tasks may be performed by the project manager or may be delegated. The tasks include:

– establishing the context for project risk management process;
– managing risk identification activities;
– managing risk analysis and evaluation activities;
– recommending, initiating and implementing risk treatment activities until the level of risk is tolerable;
– applying for an executive decision on conflicting risk issues;
– verifying the implementation of decisions and their effectiveness;
– communicating information about risk issues in an appropriate and timely fashion throughout the project;
– ensuring contingency plans are in place;
– identifying and recording any problems relating to the management of risk;
– monitoring the risk management process and implementing corrective action where necessary;
– providing documentation to ensure traceability.

The authority for project risk management and interfaces with other functions should be defined and documented.

5.2 Resources

The project manager should ensure the availability of resources for project risk management, including adequately experienced personnel. The project should take into account the cost of managing risks.

5.3 Communication

5.3.1 General

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

– quality and dependability;
– configuration control;
– commercial functions;
– design and development;
– post-project support, including product support.

These interfaces should be defined at a sufficient level of authority and detail for a rapid reaction to be possible. This minimizes the exposure of the project to the consequences of the risk occurring.

Effective internal and external communication is important in order to ensure that those responsible for implementing risk management and interested parties understand the basis on which decisions are made, the relevant roles and responsibilities, and why particular actions are required.

5.3.2 Risk reporting and meetings

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

Discussions of risk matters may include:

– identifying and assessing risks;
– reviewing the project risk register;
– reviewing the status of the risk and associated risk treatment activities;
– identifying and agreeing any changes to the risk data, and re-analysing the changes;
– assessing the effectiveness of the risk management process;
– discussing the relationship between contracted parties.

Reporting requirements should be specified in the project risk management plan.

5.4 Documentation

5.4.1 Purpose

Documentation facilitates the implementation and control of the risk management process particularly at the handover of different project stages.

Documentation aids planning, progress evaluation and traceability. The risk management process and the risks and their treatment should all be documented.

5.4.2 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, as part of the project plan, may include or refer to:

- the context and boundaries of the project including the objectives of project risk management;
- proposed risk management methodology, processes and interfaces;
- personnel responsible for risk management activities;
- responsibilities, authority and lines of reporting;
- internal and external interfaces;
- programme of risk management meetings;
- project risk register format;
- review processes;
- relationship with other project documentation and plans;
- relevant organizational procedures;
- risk management plans from other sources as appropriate (for example, subcontractors).

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

5.4.3 The project risk register

The project risk register 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.

It should be initiated at the risk identification stage. It may consist of a database that includes all the information relating to identified risks. It should contain at least a list of the identified risks, their rankings and the names of the people responsible for treating them. A unique identification number should be allocated and noted, and the traceability of the data to its source should also be recorded.

The plans for treating each risk should be documented, including the actions required, the person responsible and the schedule.

6 Project risk management processes

NOTE A project risk management process flow diagram is given in annex A.

6.1 Establishing the context

The risk context, including the technical, corporate, commercial, political, financial, legal, contractual and market objectives which may constrain or redirect the project, should be defined. Project objectives which should be achieved in order to satisfy project, corporate and customer requirements at all stages of the project should be identified and should be used to assist in identifying and ranking risks.

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

6.2 Risk identification

The purpose of risk identification is to find, list and characterize risks which may affect the achievement of the agreed project or project phase objectives. This process may also reveal opportunities.

Effective risk management is fundamentally dependent upon the identification of risks. Hence, it should be a systematic process. For the majority of cases, risk identification relies upon prediction and interpretation of anticipated problem areas.

There are a number of methods of risk identification. These may include:

– brainstorming;
– expert opinion;
– structured interviews;
– questionnaires;
– checklists;
– historical data;
– previous experience;
– testing and modelling;
– evaluation of other projects.

All practicable sources should be used when identifying risks. The requirements specification, work breakdown structure and statement of work are some of the starting points.

Risk identification should consider the impact of risks upon all project objectives. These objectives usually include cost, time and quality. They may also include other objectives that relate to statutory and regulatory compliance, security, dependability, liability, safety, health and environment.

Assumptions made at project start-up may be a source of risk and their validity should be tested periodically.

Risk identification may take place at all or some of the product phases defined in IEC 60300-3-3. Table 1 shows an example of some risk areas that may be significant at different phases of the life cycle of a typical project or product.

Table 1 – Example of phase-related risk areas

Concept and definition	Design and development	Manufacturing	Installation and commissioning	Operation and maintenance	Decom-missioning and disposal
Bid/no bid Budgets Safety Warranties Technology Contracts Regulatory requirements Project management	Trade-offs Make/buy Performance Producibility Technology Dependability Information sources Contracts Penalties Safety Inherited risks	Subcontractors Materials Resources Integration Configuration changes Dependability Penalties Safety Inherited risks	Drawings Integration Performance Dependability Safety Testing Procedures Penalties Guarantees Inherited risks	Dependability Safety Interoperability Modifications Penalties Legislation Guarantees Inherited risks	Safety Replacement Salvage Scrap Penalties Inherited risks

Risks may be inherited from previous project phases. In the transitional stages of projects, it is sensible to determine those risks that are carried into the next phase of the project.

It may be useful for an organization to generate a checklist (or lists) to cover risk areas appropriate to its application or project.

6.3 Risk assessment

6.3.1 General

The purpose of risk assessment is to analyse and evaluate identified risks to determine whether treatment is required.

6.3.2 Risk analysis

Risk analysis identifies the limits and effective boundaries of the risk, identifies any dependencies and determines the probability of occurrence and the associated impact on the agreed objectives.

It may be necessary to revisit the risk identification process during risk analysis to further clarify project risks.

Risk analysis may be performed qualitatively or quantitatively. A preliminary qualitative analysis may be carried out early in the project life-cycle, when there is little or no firm data, and quantitative analysis may be applied if and when there is more data available.

Diagrams such as the example shown in figure 3 may be used to display the risks. Such diagrams can also be displayed as a matrix (see figure 4).

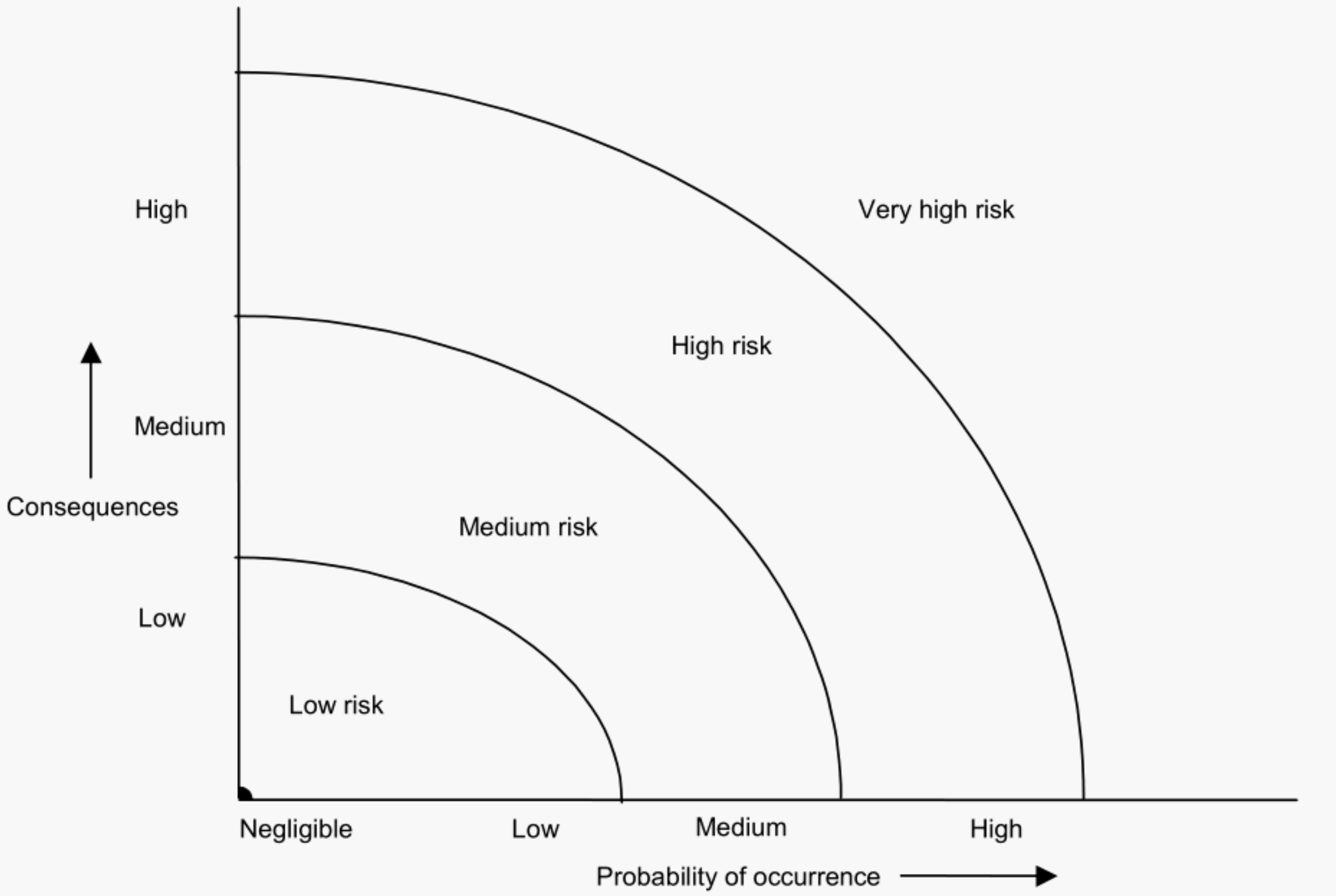


Figure 3 – Risk diagram

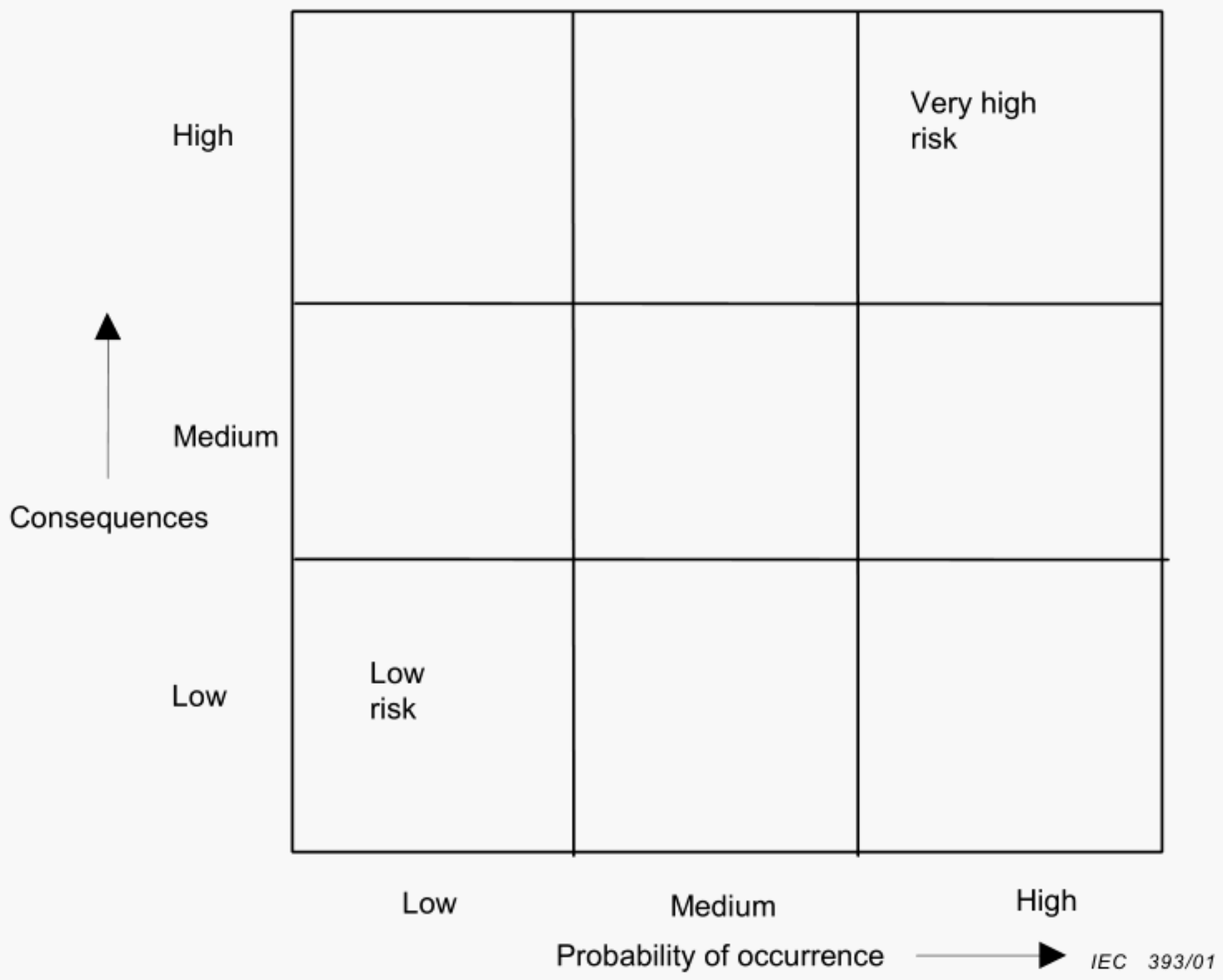


Figure 4 – Risk matrix

When analysing risk, techniques such as fault tree analysis (see IEC 61025), failure modes and effects analysis (see IEC 60812), event tree analysis, sensitivity analysis, statistical techniques and network analysis may be applied.

6.3.3 Risk evaluation

Risk evaluation involves comparing the level of risk with tolerability criteria and setting initial priorities for treating the risks.

6.3.4 Risk acceptance

Some risks may be accepted without treatment (or further treatment). These risks should be included in the project risk register so that effective monitoring can be carried out. Risks which are not accepted are treated.

6.4 Risk treatment

6.4.1 Purpose

The purpose of risk treatment is to identify and implement cost-effective actions that will make risks tolerable. It is the process of deciding on and implementing options for dealing with identified risks. It may include actions to

– avoid the risk altogether;
– reduce the probability of occurrence of the risk;
– reduce the resulting consequences should the event occur;
– transfer or share the risk;
– retain the risk and make plans to recover from the outcome.

Risk treatment may itself generate new risks that should also be considered.

Figure 5 illustrates the risk treatment process.

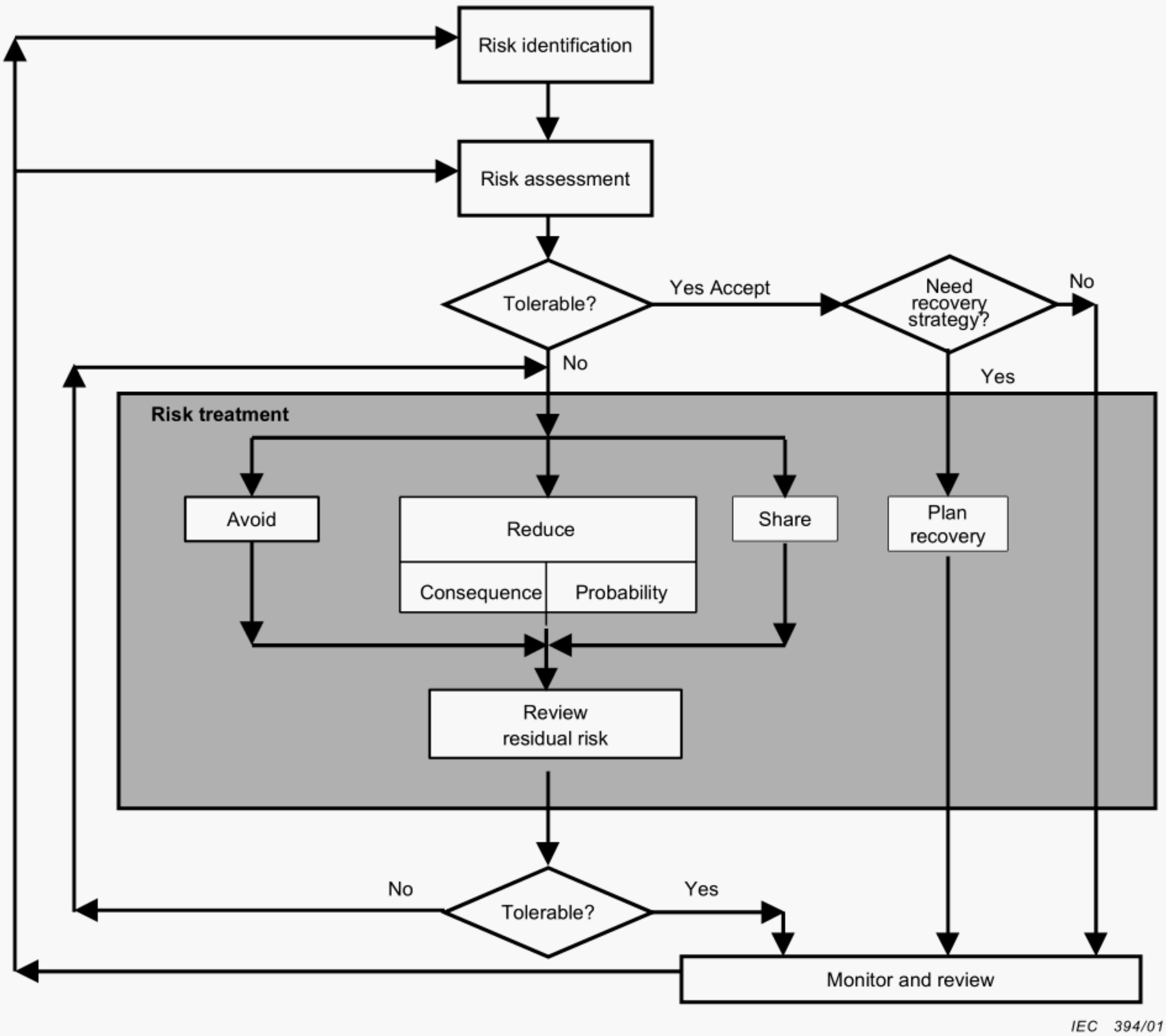


Figure 5 – Risk treatment process

6.4.2 Responsibility for risk treatment

For each risk treatment, a person should be nominated to have responsibility for that treatment. The most appropriate person may be

– the person who is responsible for the activity from which the risk arises;

– the person who can best control the probability of the risk occurring;

– the person best positioned to react to and recover from the occurrence of the risk or reduce its consequences;

– the person with the appropriate level of authority to deal with the risk.

6.4.3 Assessment of treatment options

A risk treatment option, or combination of options, should be selected by considering the costs of treating or recovering from the risk, in conjunction with the potential benefits arising from the implementation of those treatment options. Risks are interlinked and have dependencies both to and from other risks, so there may be trade-offs between different treatment options that should be considered.

The residual risk retained after options have been implemented should be considered to see if it is tolerable. If the sum of the risks is not tolerable, cancellation of the project should be considered, or possible further treatment carried out.

If the risk is considered tolerable and is accepted, then the need for a recovery strategy to deal with unwanted consequences should be considered. If a recovery strategy is required, a risk recovery plan should be prepared detailing that strategy.

6.4.4 Risk avoidance

Risks may be designed out of the project if the cost of doing so can be justified, or cancellation of the project may be considered.

6.4.5 Probability reduction

Probability reduction aims at reducing or eliminating the causes of a risk.

It is sometimes possible to reduce a risk by combining it with one or more other risks, the resultant risk being of a different nature than that of the contributing risks. The resultant risk may be more amenable to treatment. However, reducing risks of one sort may introduce risks of a different nature.

6.4.6 Consequence limitation

Risk consequences may be limited, for example by design and planning to reduce adverse impacts if a risk is realized, and by planning for recovery.

The timing of the project and the order in which different aspects of the project are undertaken can affect the risks and the ability to manage them. The project schedule may be able to be changed to improve management of risk while still allowing project objectives to be achieved. It is important to ensure that any new risks which may appear due to changes in the order of the project activities are identified.

6.4.7 Risk sharing

Risks which remain after risk reduction may be transferred or shared outside the project to someone who is paid to deal with them, for example by subcontracting or taking out insurance.

It is seldom possible to transfer risks completely, and when risk is transferred or shared, new risks may be introduced.

The feasibility of sharing risk is determined by addressing questions such as:

– which party can best control the causes of the risk occurring ?
– which party can best manage and sustain the consequences of the risk if it is realized ?
– is the premium charged by the transferee acceptable ?
– if the risk is transferred, are new risks created ?

6.4.8 Recovery strategy

The recovery plan assumes that a risk has been realized. It may or may not have been anticipated. If the risk has been anticipated, it is usually easier to recover from it if a strategy for recovery has been previously defined and set-up.

Justification for funding a recovery strategy depends on:

– the level of the risk that remains after risk treatment options have been implemented;
– the magnitude of the potential consequences;
– the inability to treat the risk adequately in advance of its occurrence;
– the cost effectiveness of the recovery strategy.

An acceptance of the need for a recovery strategy could form the justification for the creation of a contingency fund to be used in the event that the risk materializes. The recovery strategy will be initiated when predefined conditions occur. This point may be based on cost, schedule, performance or other criteria.

6.5 Risk review and monitoring

6.5.1 Continuous

The primary purpose of risk review and monitoring is to identify any new risks which arise, and ensure that risk treatment remains effective. The effectiveness of the risk management process should also be reviewed.

Risk reviews during the life cycle of a project ensure that relevant documents, standards, procedures and registers are updated and maintained.

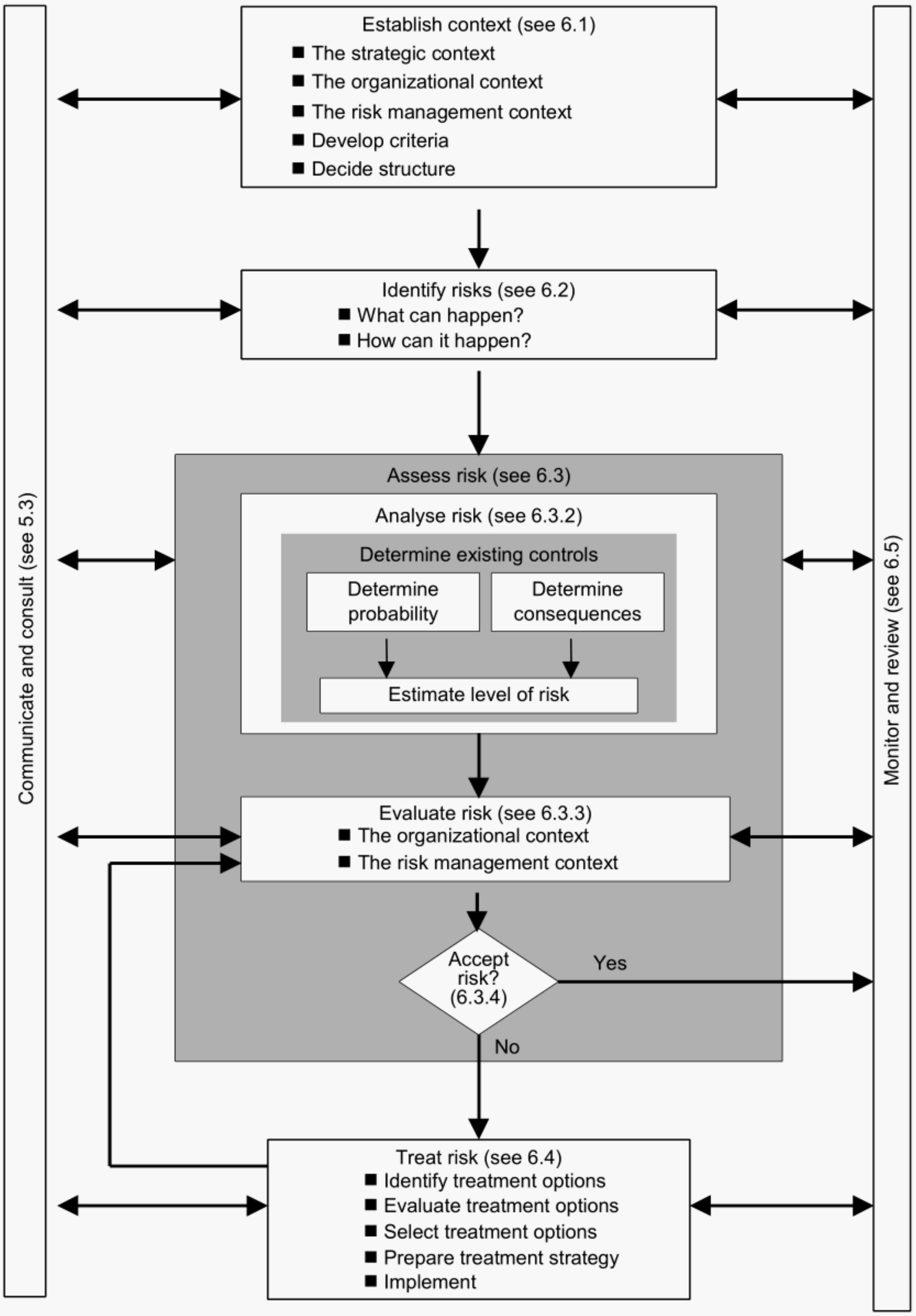
Risk monitoring should be continuous throughout the life of the project. It should involve examination of project budgets, the project network and other input from the project. Major monitoring activities may be conducted at key project milestones or when the project environment has changed significantly.

6.5.2 Post-project

After project completion, a risk management review should be carried out to ensure that the risk management process has been effective and to determine how the process may be improved on future projects. In many cases lessons will be learned, the essence of which should be refined and incorporated into procedures and processes.

Annex A
(informative)

Project risk management – Summary



IEC 395/01

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001. Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111. Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002. Fax: +44 (0)20 8996 7001. Email: membership@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsi-global.com.

BSI
389 Chiswick High Road
London
W4 4AL