INTERNATIONAL STANDARD

ISO 31000

First edition
2009-11-15

Risk management — Principles and guidelines

Management du risque — Principes et lignes directrices

Reference number
ISO 31000:2009(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Terms and definitions 1

3 Principles 7

4 Framework 8
4.1 General 8
4.2 Mandate and commitment 9
4.3 Design of framework for managing risk 10
4.3.1 Understanding of the organization and its context 10
4.3.2 Establishing risk management policy 10
4.3.3 Accountability 11
4.3.4 Integration into organizational processes 11
4.3.5 Resources 11
4.3.6 Establishing internal communication and reporting mechanisms 12
4.3.7 Establishing external communication and reporting mechanisms 12
4.4 Implementing risk management 12
4.4.1 Implementing the framework for managing risk 12
4.4.2 Implementing the risk management process 13
4.5 Monitoring and review of the framework 13
4.6 Continual improvement of the framework 13

5 Process 13
5.1 General 13
5.2 Communication and consultation 14
5.3 Establishing the context 15
5.3.1 General 15
5.3.2 Establishing the external context 15
5.3.3 Establishing the internal context 15
5.3.4 Establishing the context of the risk management process 16
5.3.5 Defining risk criteria 17
5.4 Risk assessment 17
5.4.1 General 17
5.4.2 Risk identification 17
5.4.3 Risk analysis 18
5.4.4 Risk evaluation 18
5.5 Risk treatment 18
5.5.1 General 18
5.5.2 Selection of risk treatment options 19
5.5.3 Preparing and implementing risk treatment plans 20
5.6 Monitoring and review 20
5.7 Recording the risk management process 21

Annex A (informative) **Attributes of enhanced risk management** 22

Bibliography 24

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 31000 was prepared by the ISO Technical Management Board Working Group on risk management.

Introduction

Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is “risk”.

All activities of an organization involve risk. Organizations manage risk by identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Throughout this process, they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required. This International Standard describes this systematic and logical process in detail.

While all organizations manage risk to some degree, this International Standard establishes a number of principles that need to be satisfied to make risk management effective. This International Standard recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities.

Although the practice of risk management has been developed over time and within many sectors in order to meet diverse needs, the adoption of consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently and coherently across an organization. The generic approach described in this International Standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.

Each specific sector or application of risk management brings with it individual needs, audiences, perceptions and criteria. Therefore, a key feature of this International Standard is the inclusion of “establishing the context” as an activity at the start of this generic risk management process. Establishing the context will capture the objectives of the organization, the environment in which it pursues those objectives, its stakeholders and the diversity of risk criteria – all of which will help reveal and assess the nature and complexity of its risks.

The relationship between the principles for managing risk, the framework in which it occurs and the risk management process described in this International Standard are shown in Figure 1.

When implemented and maintained in accordance with this International Standard, the management of risk enables an organization to, for example:

— increase the likelihood of achieving objectives;

— encourage proactive management;

— be aware of the need to identify and treat risk throughout the organization;

— improve the identification of opportunities and threats;

— comply with relevant legal and regulatory requirements and international norms;

— improve mandatory and voluntary reporting;

— improve governance;

— improve stakeholder confidence and trust;

— establish a reliable basis for decision making and planning;

— improve controls;

— effectively allocate and use resources for risk treatment;

— improve operational effectiveness and efficiency;

— enhance health and safety performance, as well as environmental protection;

— improve loss prevention and incident management;

— minimize losses;

— improve organizational learning; and

— improve organizational resilience.

This International Standard is intended to meet the needs of a wide range of stakeholders, including:

a) those responsible for developing risk management policy within their organization;

b) those accountable for ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity;

c) those who need to evaluate an organization's effectiveness in managing risk; and

d) developers of standards, guides, procedures and codes of practice that, in whole or in part, set out how risk is to be managed within the specific context of these documents.

The current management practices and processes of many organizations include components of risk management, and many organizations have already adopted a formal risk management process for particular types of risk or circumstances. In such cases, an organization can decide to carry out a critical review of its existing practices and processes in the light of this International Standard.

In this International Standard, the expressions “risk management” and “managing risk” are both used. In general terms, “risk management” refers to the architecture (principles, framework and process) for managing risks effectively, while “managing risk” refers to applying that architecture to particular risks.

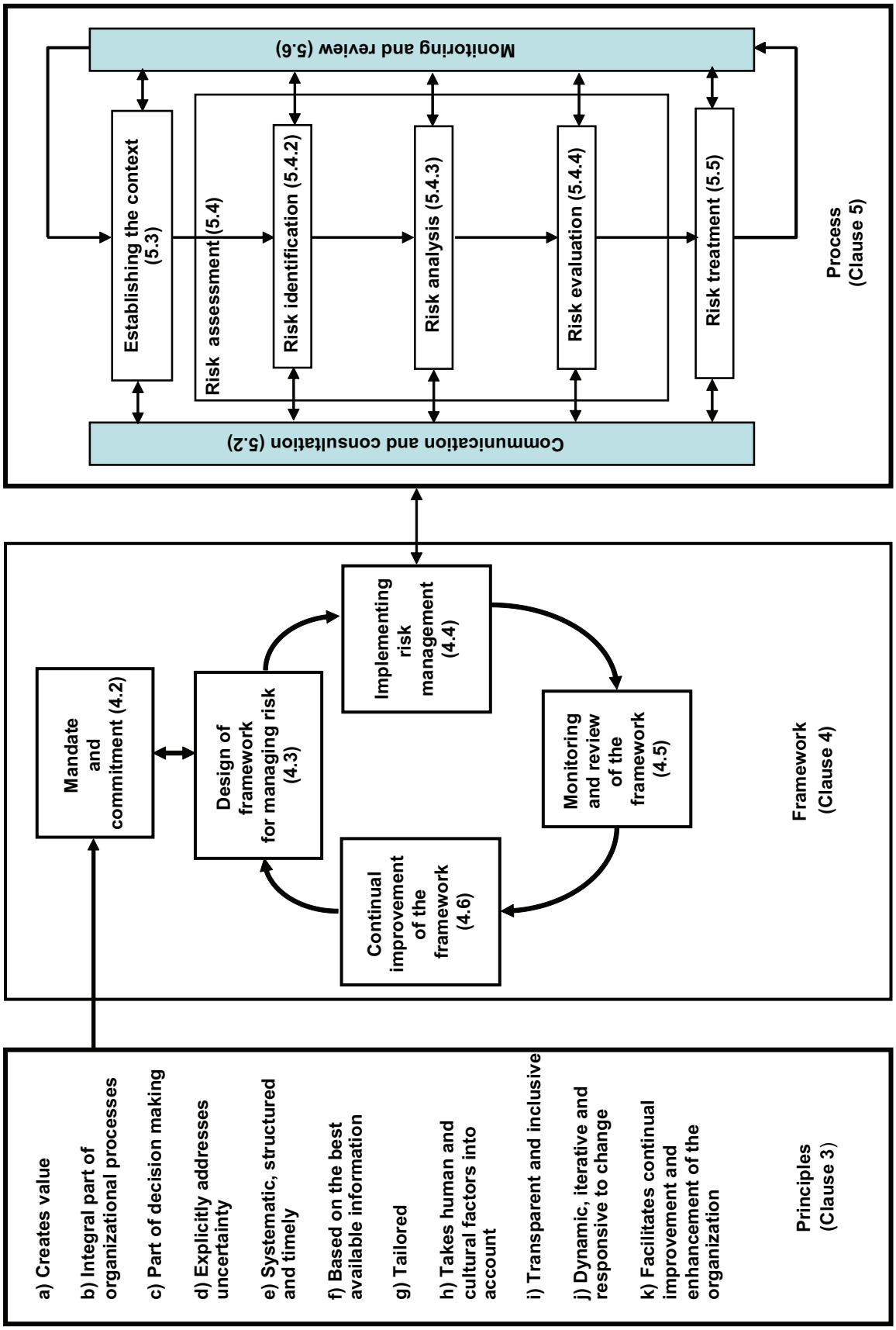

Figure 1 — Relationships between the risk management principles, framework and process

Risk management — Principles and guidelines

1 Scope

This International Standard provides principles and generic guidelines on risk management.

This International Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.

NOTE For convenience, all the different users of this International Standard are referred to by the general term "organization".

This International Standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

This International Standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Although this International Standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

It is intended that this International Standard be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.

This International Standard is not intended for the purpose of certification.

2 Terms and definitions

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

2.1
risk
effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 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, product and process).

NOTE 3 Risk is often characterized by reference to potential **events** (2.17) and **consequences** (2.18), or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** (2.19) of occurrence.

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

[ISO Guide 73:2009, definition 1.1]

2.2
risk management
coordinated activities to direct and control an organization with regard to **risk** (2.1)

[ISO Guide 73:2009, definition 2.1]

2.3
risk management framework
set of components that provide the foundations and organizational arrangements for designing, implementing, **monitoring** (2.28), reviewing and continually improving **risk management** (2.2) throughout the organization

NOTE 1 The foundations include the policy, objectives, mandate and commitment to manage **risk** (2.1).

NOTE 2 The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.

NOTE 3 The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

[ISO Guide 73:2009, definition 2.1.1]

2.4
risk management policy
statement of the overall intentions and direction of an organization related to **risk management** (2.2)

[ISO Guide 73:2009, definition 2.1.2]

2.5
risk attitude
organization's approach to assess and eventually pursue, retain, take or turn away from **risk** (2.1)

[ISO Guide 73:2009, definition 3.7.1.1]

2.6
risk management plan
scheme within the **risk management framework** (2.3) specifying the approach, the management components and resources to be applied to the management of **risk** (2.1)

NOTE 1 Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.

NOTE 2 The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.

[ISO Guide 73:2009, definition 2.1.3]

2.7
risk owner
person or entity with the accountability and authority to manage a **risk** (2.1)

[ISO Guide 73:2009, definition 3.5.1.5]

2.8
risk management process
systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, **monitoring** (2.28) and reviewing **risk** (2.1)

[ISO Guide 73:2009, definition 3.1]

2.9
establishing the context
defining the external and internal parameters to be taken into account when managing risk, and setting the scope and **risk criteria** (2.22) for the **risk management policy** (2.4)

[ISO Guide 73:2009, definition 3.3.1]

2.10
external context
external environment in which the organization seeks to achieve its objectives

NOTE External context can include:

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

— key drivers and trends having impact on the objectives of the organization; and

— relationships with, and perceptions and values of external **stakeholders** (2.13).

[ISO Guide 73:2009, definition 3.3.1.1]

2.11
internal context
internal environment in which the organization seeks to achieve its objectives

NOTE Internal context can include:

— governance, organizational structure, roles and accountabilities;

— policies, objectives, and the strategies that are in place to achieve them;

— the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

— information systems, information flows and decision-making processes (both formal and informal);

— relationships with, and perceptions and values of, internal stakeholders;

— the organization's culture;

— standards, guidelines and models adopted by the organization; and

— form and extent of contractual relationships.

[ISO Guide 73:2009, definition 3.3.1.2]

2.12
communication and consultation
continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with **stakeholders** (2.13) regarding the management of **risk** (2.1)

NOTE 1 The information can relate to the existence, nature, form, **likelihood** (2.19), significance, evaluation, acceptability and treatment of the management of risk.

NOTE 2 Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:

— a process which impacts on a decision through influence rather than power; and

— an input to decision making, not joint decision making.

[ISO Guide 73:2009, definition 3.2.1]

2.13
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

NOTE A decision maker can be a stakeholder.

[ISO Guide 73:2009, definition 3.2.1.1]

2.14
risk assessment
overall process of **risk identification** (2.15), **risk analysis** (2.21) and **risk evaluation** (2.24)

[ISO Guide 73:2009, definition 3.4.1]

2.15
risk identification
process of finding, recognizing and describing **risks** (2.1)

NOTE 1 Risk identification involves the identification of **risk sources** (2.16), **events** (2.17), their causes and their potential **consequences** (2.18).

NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and **stakeholder**'s (2.13) needs.

[ISO Guide 73:2009, definition 3.5.1]

2.16
risk source
element which alone or in combination has the intrinsic potential to give rise to **risk** (2.1)

NOTE A risk source can be tangible or intangible.

[ISO Guide 73:2009, definition 3.5.1.2]

2.17
event
occurrence or change of a particular set of circumstances

NOTE 1 An event can be one or more occurrences, and can have several causes.

NOTE 2 An event can consist of something not happening.

NOTE 3 An event can sometimes be referred to as an “incident” or “accident”.

NOTE 4 An event without **consequences** (2.18) can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.

[ISO Guide 73:2009, definition 3.5.1.3]

2.18
consequence
outcome of an **event** (2.17) affecting objectives

NOTE 1 An event can lead to a range of consequences.

NOTE 2 A consequence can be certain or uncertain and can have positive or negative effects on objectives.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

NOTE 4 Initial consequences can escalate through knock-on effects.

[ISO Guide 73:2009, definition 3.6.1.3]

2.19
likelihood
chance of something happening

NOTE 1 In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

NOTE 2 The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

[ISO Guide 73:2009, definition 3.6.1.1]

2.20
risk profile
description of any set of **risks** (2.1)

NOTE The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

[ISO Guide 73:2009, definition 3.8.2.5]

2.21
risk analysis
process to comprehend the nature of **risk** (2.1) and to determine the **level of risk** (2.23)

NOTE 1 Risk analysis provides the basis for **risk evaluation** (2.24) and decisions about **risk treatment** (2.25).

NOTE 2 Risk analysis includes risk estimation.

[ISO Guide 73:2009, definition 3.6.1]

2.22
risk criteria
terms of reference against which the significance of a **risk** (2.1) is evaluated

NOTE 1 Risk criteria are based on organizational objectives, and **external** (2.10) and **internal context** (2.11).

NOTE 2 Risk criteria can be derived from standards, laws, policies and other requirements.

[ISO Guide 73:2009, definition 3.3.1.3]

2.23
level of risk
magnitude of a **risk** (2.1) or combination of risks, expressed in terms of the combination of **consequences** (2.18) and their **likelihood** (2.19)

[ISO Guide 73:2009, definition 3.6.1.8]

2.24
risk evaluation
process of comparing the results of **risk analysis** (2.21) with **risk criteria** (2.22) to determine whether the **risk** (2.1) and/or its magnitude is acceptable or tolerable

NOTE Risk evaluation assists in the decision about **risk treatment** (2.25).

[ISO Guide 73:2009, definition 3.7.1]

2.25
risk treatment
process to modify **risk** (2.1)

NOTE 1 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** (2.16);

— changing the **likelihood** (2.19);

— changing the **consequences** (2.18);

— sharing the risk with another party or parties (including contracts and risk financing); and

— retaining the risk by informed decision.

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

NOTE 3 Risk treatment can create new risks or modify existing risks.

[ISO Guide 73:2009, definition 3.8.1]

2.26
control
measure that is modifying **risk** (2.1)

NOTE 1 Controls include any process, policy, device, practice, or other actions which modify risk.

NOTE 2 Controls may not always exert the intended or assumed modifying effect.

[ISO Guide 73:2009, definition 3.8.1.1]

2.27
residual risk
risk (2.1) remaining after **risk treatment** (2.25)

NOTE 1 Residual risk can contain unidentified risk.

NOTE 2 Residual risk can also be known as “retained risk”.

[ISO Guide 73:2009, definition 3.8.1.6]

2.28
monitoring
continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

NOTE Monitoring can be applied to a **risk management framework** (2.3), **risk management process** (2.8), **risk** (2.1) or **control** (2.26).

[ISO Guide 73:2009, definition 3.8.2.1]

2.29
review
activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

NOTE Review can be applied to a **risk management framework** (2.3), **risk management process** (2.8), **risk** (2.1) or **control** (2.26).

[ISO Guide 73:2009, definition 3.8.2.2]

3 Principles

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

a) **Risk management creates and protects value**.

Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

b) **Risk management is an integral part of all organizational processes**.

Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.

c) **Risk management is part of decision making**.

Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.

d) **Risk management explicitly addresses uncertainty**.

Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

e) **Risk management is systematic, structured and timely**.

A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

f) **Risk management is based on the best available information**.

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

g) **Risk management is tailored**.

Risk management is aligned with the organization's external and internal context and risk profile.

h) **Risk management takes human and cultural factors into account**.

Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.

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**.

Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

k) **Risk management facilitates continual improvement of the organization**.

Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.

Annex A provides further advice for organizations wishing to manage risk more effectively.

4 Framework

4.1 General

The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organization at all levels. The framework assists in managing risks effectively through the application of the risk management process (see Clause 5) at varying levels and within specific contexts of the organization. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels.

This clause describes the necessary components of the framework for managing risk and the way in which they interrelate in an iterative manner, as shown in Figure 2.

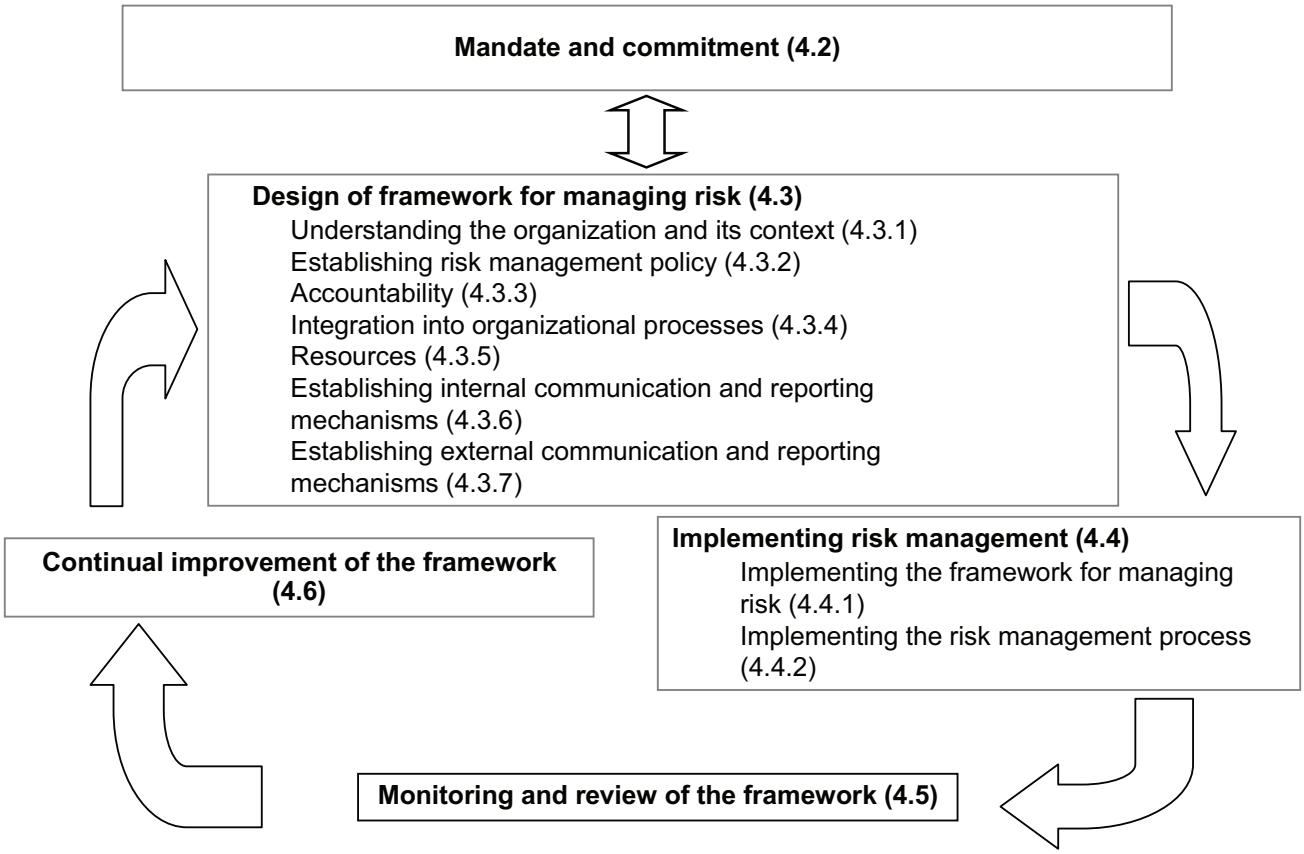

Figure 2 — Relationship between the components of the framework for managing risk

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

If an organization's existing management practices and processes include components of risk management or if the organization has already adopted a formal risk management process for particular types of risk or situations, then these should be critically reviewed and assessed against this International Standard, including the attributes contained in Annex A, in order to determine their adequacy and effectiveness.

4.2 Mandate and commitment

The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organization, as well as strategic and rigorous planning to achieve commitment at all levels. Management should:

— define and endorse the risk management policy;

— ensure that the organization's culture and risk management policy are aligned;

— determine risk management performance indicators that align with performance indicators of the organization;

— align risk management objectives with the objectives and strategies of the organization;

— ensure legal and regulatory compliance;

— assign accountabilities and responsibilities at appropriate levels within the organization;

— ensure that the necessary resources are allocated to risk management;

— communicate the benefits of risk management to all stakeholders; and

— ensure that the framework for managing risk continues to remain appropriate.

4.3 Design of framework for managing risk

4.3.1 Understanding of the organization 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 organization, since these can significantly influence the design of the framework.

Evaluating the organization's external context may include, but is not limited to:

a) the social and cultural, political, 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 of the organization; and

c) relationships with, and perceptions and values of, external stakeholders.

Evaluating the organization's internal context may include, but is not limited to:

— governance, organizational structure, roles and accountabilities;

— policies, objectives, and the strategies that are in place to achieve them;

— capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

— information systems, information flows and decision making processes (both formal and informal);

— relationships with, and perceptions and values of, internal stakeholders;

— the organization's culture;

— standards, guidelines and models adopted by the organization; and

— the form and extent of contractual relationships.

4.3.2 Establishing risk management policy

The risk management policy should clearly state the organization's objectives for, and commitment to, risk management and typically addresses the following:

— the organization's rationale for managing risk;

— links between the organization's objectives and policies and the risk management policy;

— accountabilities and responsibilities for managing risk;

— the way in which conflicting interests are dealt with;

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

— the way in which risk management performance will be measured and reported; and

— commitment to review and improve the risk management policy and framework periodically and in response to an event or change in circumstances.

The risk management policy should be communicated appropriately.

4.3.3 Accountability

The organization should ensure that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness and efficiency of any controls. This can be facilitated by:

— identifying risk owners that have the accountability and authority to manage risks;

— identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;

— identifying other responsibilities of people at all levels in the organization for the risk management process;

— establishing performance measurement and external and/or internal reporting and escalation processes; and

— ensuring appropriate levels of recognition.

4.3.4 Integration into organizational processes

Risk management should be embedded in all the organization's practices and processes in a way that it is relevant, effective and efficient. The risk management process should become part of, and not separate from, those organizational processes. In particular, risk management should be embedded into the policy development, business and strategic planning and review, and change management processes.

There should be an organization-wide risk management plan to ensure that the risk management policy is implemented and that risk management is embedded in all of the organization's practices and processes. The risk management plan can be integrated into other organizational plans, such as a strategic plan.

4.3.5 Resources

The organization should allocate appropriate resources for risk management.

Consideration should be given to the following:

— people, skills, experience and competence;

— resources needed for each step of the risk management process;

— the organization's processes, methods and tools to be used for managing risk;

— documented processes and procedures;

— information and knowledge management systems; and

— training programmes.

4.3.6 Establishing internal communication and reporting mechanisms

The organization should establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk. These mechanisms should ensure that:

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

— there is adequate internal reporting on the framework, its effectiveness and the outcomes;

— relevant information derived from the application of risk management is available at appropriate levels and times; and

— there are processes for consultation with internal stakeholders.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

4.3.7 Establishing external communication and reporting mechanisms

The organization should develop and implement a plan as to how it will communicate with external stakeholders. This should involve:

— engaging appropriate external stakeholders and ensuring an effective exchange of information;

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

— providing feedback and reporting on communication and consultation;

— using communication to build confidence in the organization; and

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

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

4.4 Implementing risk management

4.4.1 Implementing the framework for managing risk

In implementing the organization's framework for managing risk, the organization should:

— define the appropriate timing and strategy for implementing the framework;

— apply the risk management policy and process to the organizational processes;

— comply with legal and regulatory requirements;

— ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;

— hold information and training sessions; and

— communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.

4.4.2 Implementing the risk management process

Risk management should be implemented by ensuring that the risk management process outlined in Clause 5 is applied through a risk management plan at all relevant levels and functions of the organization as part of its practices and processes.

4.5 Monitoring and review of the framework

In order to ensure that risk management is effective and continues to support organizational performance, the organization should:

— measure risk management performance against indicators, which are periodically reviewed for appropriateness;

— periodically measure progress against, and deviation from, the risk management plan;

— periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;

— report on risk, progress with the risk management plan and how well the risk management policy is being followed; and

— review the effectiveness of the risk management framework.

4.6 Continual improvement of the framework

Based on results of monitoring and reviews, decisions should be made on how the risk management framework, policy and plan can be improved. These decisions should lead to improvements in the organization's management of risk and its risk management culture.

5 Process

5.1 General

The risk management process should be

— an integral part of management,

— embedded in the culture and practices, and

— tailored to the business processes of the organization.

It comprises the activities described in 5.2 to 5.6. The risk management process is shown in Figure 3.

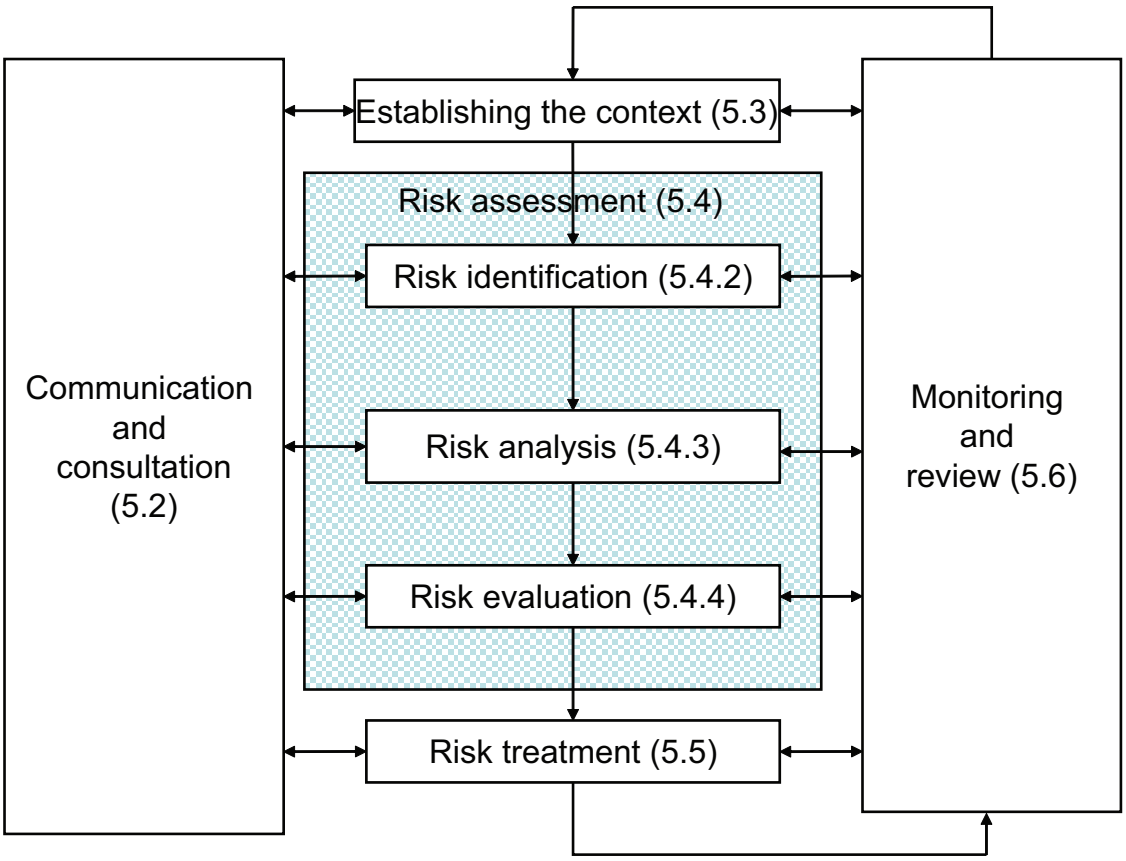

Figure 3 — Risk management process

5.2 Communication and consultation

Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.

Therefore, plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

A consultative team approach may:

— help establish the context appropriately;

— ensure that the interests of stakeholders are understood and considered;

— help ensure that risks are adequately identified;

— bring different areas of expertise together for analyzing risks;

— ensure that different views are appropriately considered when defining risk criteria and in evaluating risks;

— secure endorsement and support for a treatment plan;

— enhance appropriate change management during the risk management process; and

— develop an appropriate external and internal communication and consultation plan.

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 values, needs, assumptions, concepts and concerns of stakeholders. As their views can have a significant impact on the decisions 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.

5.3 Establishing the context

5.3.1 General

By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process. While many of these parameters are similar to those considered in the design of the risk management framework (see 4.3.1), when establishing the context for the risk management process, they need to be considered in greater detail and particularly how they relate to the scope of the particular risk management process.

5.3.2 Establishing the external context

The external context is the external environment in which the organization seeks to achieve its objectives.

Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing 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 risk management process.

The external context can include, but is not limited to:

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

— key drivers and trends having impact on the objectives of the organization; and

— relationships with, perceptions and values of external stakeholders.

5.3.3 Establishing the internal context

The internal context is the internal environment in which the organization seeks to achieve its objectives.

The risk management process should be aligned with the organization's culture, processes, structure and strategy. Internal context is anything within the organization that can influence the way in which an organization will manage risk. It should be established because:

a) risk management takes place in the context of the objectives of the organization;

b) objectives and criteria of a particular project, process or activity should be considered in the light of objectives of the organization as a whole; and

c) some organizations fail to recognize opportunities to achieve their strategic, project or business objectives, and this affects ongoing organizational commitment, credibility, trust and value.

It is necessary to understand the internal context. This can include, but is not limited to:

— governance, organizational structure, roles and accountabilities;

— policies, objectives, and the strategies that are in place to achieve them;

— capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

— the relationships with and perceptions and values of internal stakeholders;

— the organization's culture;

— information systems, information flows and decision making processes (both formal and informal);

— standards, guidelines and models adopted by the organization; and

— form and extent of contractual relationships.

5.3.4 Establishing the context of the risk management process

The objectives, strategies, scope and parameters of the activities of the organization, or those parts of the organization where the risk management process is being applied, should be established. The management of 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 an organization. It can involve, but is not limited to:

— defining the goals and objectives of the risk management activities;

— defining responsibilities for and within the risk management process;

— defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;

— defining the activity, process, function, project, product, service or asset in terms of time and location;

— defining the relationships between a particular project, process or activity and other projects, processes or activities of the organization;

— defining the risk assessment methodologies;

— defining the way performance and effectiveness is evaluated in the management of risk;

— identifying and specifying the decisions that have to be made; and

— identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.

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

5.3.5 Defining risk criteria

The organization should define criteria to be used to evaluate the significance of risk. The criteria should reflect the organization's values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the organization subscribes. Risk criteria should be consistent with the organization's risk management policy (see 4.3.2), be defined at the beginning of any risk management process and be continually reviewed.

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

— the nature and types of causes and consequences that can occur and how they will be measured;

— how likelihood will be defined;

— the timeframe(s) of the likelihood and/or consequence(s);

— how the level of risk is to be determined;

— the views of stakeholders;

— the level at which risk becomes acceptable or tolerable; and

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

5.4 Risk assessment

5.4.1 General

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

NOTE ISO/IEC 31010 provides guidance on risk assessment techniques.

5.4.2 Risk identification

The organization should identify 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 that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is 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 will not be included in further analysis.

Identification should include risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered.

The organization should apply risk identification tools and techniques that are suited to its objectives and capabilities, and to the risks faced. 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.

5.4.3 Risk analysis

Risk analysis involves developing an understanding of the risk. 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 into making decisions where choices must 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, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

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 ongoing relevance of information, or limitations on modelling should be stated and can be highlighted.

Risk analysis can be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data and resources available. Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances.

Consequences and their likelihood can be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or from available data. Consequences can be expressed in terms of tangible and intangible impacts. In some cases, more than one numerical value or descriptor is required to specify consequences and their likelihood for different times, places, groups or situations.

5.4.4 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 level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

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.

In some circumstances, the risk evaluation can lead to a decision to undertake further analysis. The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls. This decision will be influenced by the organization's risk attitude and the risk criteria that have been established.

5.5 Risk treatment

5.5.1 General

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

Risk treatment involves a cyclical process of:

— assessing a risk treatment;

— deciding whether residual risk levels are tolerable;

— if not tolerable, generating a new risk treatment; and

— assessing the effectiveness of that treatment.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:

a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

b) taking or increasing the risk in order to pursue an opportunity;

c) removing the risk source;

d) changing the likelihood;

e) changing the consequences;

f) sharing the risk with another party or parties (including contracts and risk financing); and

g) retaining the risk by informed decision.

5.5.2 Selection of risk treatment options

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment. Decisions should also take into account risks which can warrant risk treatment that is not justifiable on economic grounds, e.g. severe (high negative consequence) but rare (low likelihood) risks.

A number of treatment options can be considered and applied either individually or in combination. The organization can normally benefit from the adoption of a combination of treatment options.

When selecting risk treatment options, the organization should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them. Where risk treatment options can impact on risk elsewhere in the organization or with stakeholders, these should be involved in the decision. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

The treatment plan should clearly identify the priority order in which individual risk treatments should be implemented.

Risk treatment itself can introduce risks. A significant risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an integral part of the risk treatment plan to give assurance that the measures remain effective.

Risk treatment can also introduce secondary risks that need to be assessed, treated, monitored and reviewed. These secondary risks should be incorporated into the same treatment plan as the original risk and not treated as a new risk. The link between the two risks should be identified and maintained.

5.5.3 Preparing and implementing risk treatment plans

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

— the reasons for selection of treatment options, including expected benefits to be gained;

— those who are accountable for approving the plan and those responsible for implementing the plan;

— proposed actions;

— resource requirements including contingencies;

— performance measures and constraints;

— reporting and monitoring requirements; and

— timing and schedule.

Treatment plans should be integrated with the management processes of the organization and discussed with appropriate stakeholders.

Decision makers and other stakeholders should be aware of the nature and extent of the residual risk after risk treatment. The residual risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

5.6 Monitoring and review

Both monitoring and review should be a planned part of the risk management process and involve regular checking or surveillance. It can be periodic or *ad hoc*.

Responsibilities for monitoring and review should be clearly defined.

The organization's monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

— ensuring that controls are effective and efficient in both design and operation;

— obtaining further information to improve risk assessment;

— analyzing and learning lessons from events (including near-misses), changes, trends, successes and failures;

— detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and

— identifying emerging risks.

Progress in implementing risk treatment plans provides a performance measure. The results can be incorporated into the organization's overall performance management, measurement and external and internal reporting activities.

The results of monitoring and review should be recorded and externally and internally reported as appropriate, and should also be used as an input to the review of the risk management framework (see 4.5).

5.7 Recording the risk management process

Risk management activities should be traceable. In the 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:

— the organization's needs for continuous learning;

— benefits of re-using information for management purposes;

— costs and efforts involved in creating and maintaining records;

— legal, regulatory and operational needs for records;

— method of access, ease of retrievability and storage media;

— retention period; and

— sensitivity of information.

Annex A
(informative)

Attributes of enhanced risk management

A.1 General

All organizations should aim at the appropriate level of performance of their risk management framework in line with the criticality of the decisions that are to be made. The list of attributes below represents a high level of performance in managing risk. To assist organizations in measuring their own performance against these criteria, some tangible indicators are given for each attribute.

A.2 Key outcomes

A.2.1 The organization has a current, correct and comprehensive understanding of its risks.

A.2.2 The organization's risks are within its risk criteria.

A.3 Attributes

A.3.1 Continual improvement

An emphasis is placed on continual improvement in risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.

This can be indicated by the existence of explicit performance goals against which the organization's and individual manager's performance is measured. The organization's performance can be published and communicated. Normally, there will be at least an annual review of performance and then a revision of processes, and the setting of revised performance objectives for the following period.

This risk management performance assessment is an integral part of the overall organization's performance assessment and measurement system for departments and individuals.

A.3.2 Full accountability for risks

Enhanced risk management includes comprehensive, fully defined and fully accepted accountability for risks, controls and risk treatment tasks. Designated individuals fully accept accountability, are appropriately skilled and have adequate resources to check controls, monitor risks, improve controls and communicate effectively about risks and their management to external and internal stakeholders.

This can be indicated by all members of an organization being fully aware of the risks, controls and tasks for which they are accountable. Normally, this will be recorded in job/position descriptions, databases or information systems. The definition of risk management roles, accountabilities and responsibilities should be part of all the organization's induction programmes.

The organization ensures that those who are accountable are equipped to fulfil that role by providing them with the authority, time, training, resources and skills sufficient to assume their accountabilities.

A.3.3 Application of risk management in all decision making

All decision making within the organization, whatever the level of importance and significance, involves the explicit consideration of risks and the application of risk management to some appropriate degree.

This can be indicated by records of meetings and decisions to show that explicit discussions on risks took place. In addition, it should be possible to see that all components of risk management are represented within key processes for decision making in the organization, e.g. for decisions on the allocation of capital, on major projects and on re-structuring and organizational changes. For these reasons, soundly based risk management is seen within the organization as providing the basis for effective governance.

A.3.4 Continual communications

Enhanced risk management includes continual communications with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance, as part of good governance.

This can be indicated by communication with stakeholders as an integral and essential component of risk management. Communication is rightly seen as a two-way process, such that properly informed decisions can be made about the level of risks and the need for risk treatment against properly established and comprehensive risk criteria.

Comprehensive and frequent external and internal reporting on both significant risks and on risk management performance contributes substantially to effective governance within an organization.

A.3.5 Full integration in the organization's governance structure

Risk management is viewed as central to the organization's management processes, such that risks are considered in terms of effect of uncertainty on objectives. The governance structure and process are based on the management of risk. Effective risk management is regarded by managers as essential for the achievement of the organization's objectives.

This is indicated by managers' language and important written materials in the organization using the term “uncertainty” in connection with risks. This attribute is also normally reflected in the organization's statements of policy, particularly those relating to risk management. Normally, this attribute would be verified through interviews with managers and through the evidence of their actions and statements.

Bibliography

[1] ISO Guide 73:2009, *Risk management — Vocabulary*

[2] ISO/IEC 31010, *Risk management — Risk assessment techniques*

ICS 03.100.01

Price based on 24 pages