DRAFT INTERNATIONAL STANDARD

ISO/DIS 31000

ISO/TC **262**

Secretariat: **BSI**

Voting begins on:
2017-02-17

Voting terminates on:
2017-05-11

Risk management — Guidelines

Management du risque — Lignes directrices

ICS: 03.100.01

Reference number
ISO/DIS 31000:2017(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/TC 262

This second edition cancels and replaces the first edition which been technically revised.

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.

Managing risk is dynamic and assists organizations in making informed decisions about setting strategy and achieving objectives.

Managing risk is part of governance and leadership and how the organization is managed.

Managing risk includes interaction with stakeholders as an integral part of all activities of the organization.

Managing risk considers the internal and external context of the organization including human behaviour and cultural factors.

Managing risk is based on the principles, framework and process outlined in this document. These components might already exist in full or in part within the organization, however they might need to be adapted or improved so that managing risk is consistent, efficient and effective. See Figure 1.

This document is for use by people who create and protect value in organizations by managing risks, making decisions, setting and achieving objectives and improving performance.

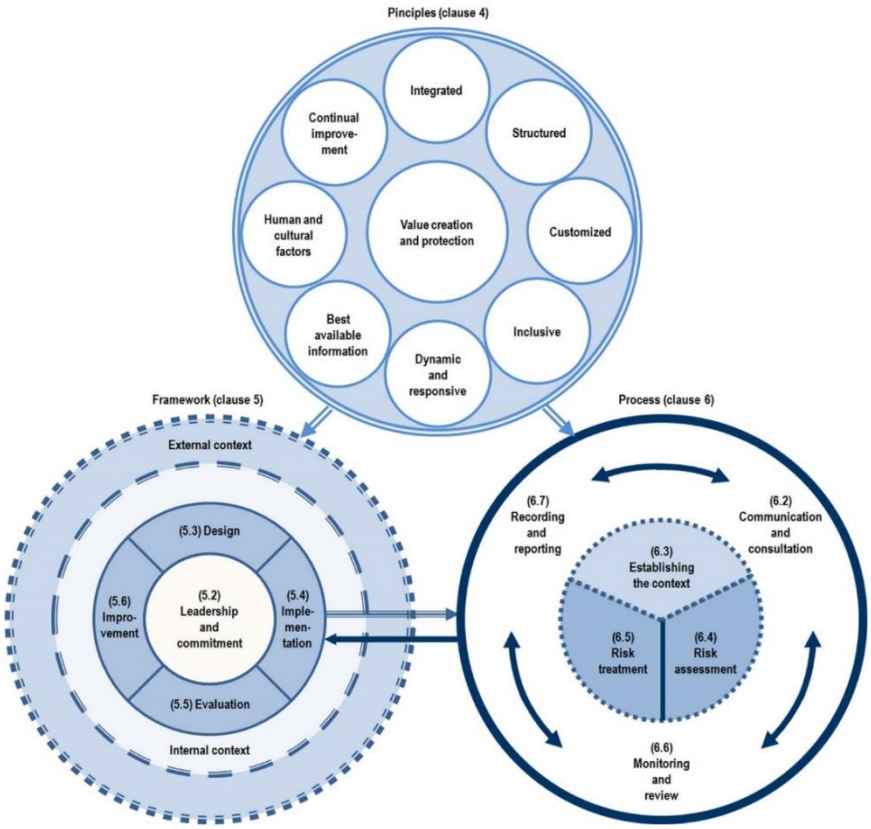

Figure 1 — Relationship between the principles, framework and process

Risk Management — Guidelines

1 Scope

This document provides adaptable guidelines on managing risk faced by organizations.

It can be used by any organization, provides a common approach to managing any type of risk and is not specific to any industry or sector.

This document can be used throughout the life of the organization and applied to any activity, including decision making at all levels.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO Guide 73 and the following apply.

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

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

3.1
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive (sometimes expressed as opportunities), negative (sometimes expressed as threats) or both.

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

Note 3 to entry: Risk is often characterized by reference to potential events, their consequences and their likelihood."

[SOURCE: ISO Guide 73:2009, 1.1, modified — The original Notes 1, 2 and 3 to entry have been modified; the original Notes 4 and 5 to entry have been deleted.]

3.2
risk management
coordinated activities to direct and control an organization with regard to risk (3.1)

[SOURCE: ISO Guide 73:2009, 3.1]

3.3
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Note 1 to entry: A decision maker can be a stakeholder.

[SOURCE: ISO Guide 73:2009, 3.2.1.1]

3.4
risk source
element which alone or in combination has the intrinsic potential to give rise to risk (3.1)

[SOURCE: ISO Guide 73:2009, 3.5.1.2, modified — The original Note to entry has been deleted.]

3.5
event
occurrence or change of a particular set of circumstances

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

Note 2 to entry: An event can also be something that is expected, not happening.

[SOURCE: ISO Guide 73:2009, 3.5.1.3, modified — The original Note 2 entry has been modified; the original Notes 3 and 4 to entry have been deleted.]

3.6
consequence
outcome of an event (3.10) affecting objectives

Note 1 to entry: A consequence can be certain or uncertain and can have positive or negative effects on objectives.

Note 2 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 3 to entry: Initial consequences can escalate through cascading and cumulative effects.

[SOURCE: ISO Guide 73:2009, 3.6.1.3, modified — The original Note 1 to entry has been deleted.]

3.6
likelihood
chance of something happening

Note 1 to entry: 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 to entry: 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.

[SOURCE: ISO Guide 73:2009, 3.6.1.1]

3.7
control
measure that maintains or modifies risk

Note 1 to entry: Controls include any process, policy, device, practice, or other conditions and/or actions which maintain and modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO Guide 73:2009, 3.8.1.1, modified — The original definition and Note 1 to entry have been modified; Note 3 to entry has been added.]

4 Principles

These principles provide guidelines on the attributes of effective and efficient risk management, communicating its value and explaining its intention and purpose. These principles should enable an organization to manage the effects of uncertainty on its objectives. See Figure 2.

a) Value creation and protection

Risk management creates and protects value. It contributes to the achievement of objectives, encourages innovation and improves performance.

b) Integrated

Risk management is an integral part of all organizational activities, including decision making. It is not a stand-alone activity that is separate from the activities and processes of the organization. Everyone in an organization has responsibility for managing risk. Risk management improves decision making at all levels.

c) Structured

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

d) Customized

The risk management framework and processes should be customized to the organization's external and internal context and related to its objectives.

e) Inclusive

Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management and decision making.

f) Dynamic and responsive

Risks may emerge, change or disappear as a result of changes and events in an organization’s internal and external context. Risk management anticipates, detects, acknowledges and responds to those changes and events in a timely manner.

g) Best available information

The inputs to risk management are based on historical and current information as well as future expectations, taking into account any limitations and uncertainties associated with the information.

h) Human and cultural factors

Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

i) Continual improvement

Risk management improves organizational performance through increasing awareness and developing capabilities based on continuous learning and experience. These activities support organizational learning and resilience.

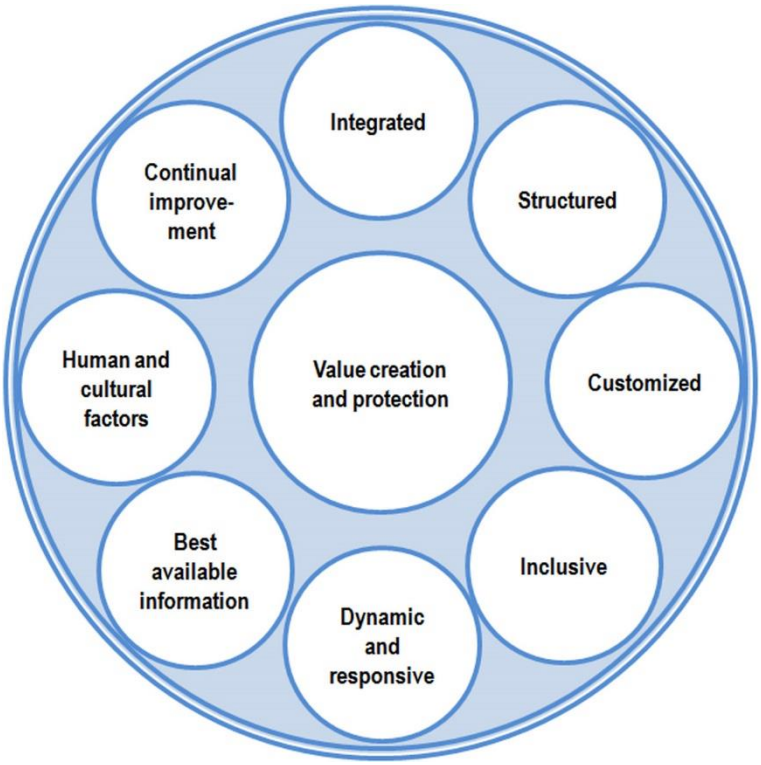

Figure 2— Principles

5 Framework

5.1. General

The success of risk management will depend on the integration of risk management into the governance and all activities of the organization; this requires support from stakeholders, particularly top management.

The framework encompasses the organizational arrangements for designing, implementing, evaluating and improving the use of risk management. Figure 3 illustrates the relationship between the components of the framework.

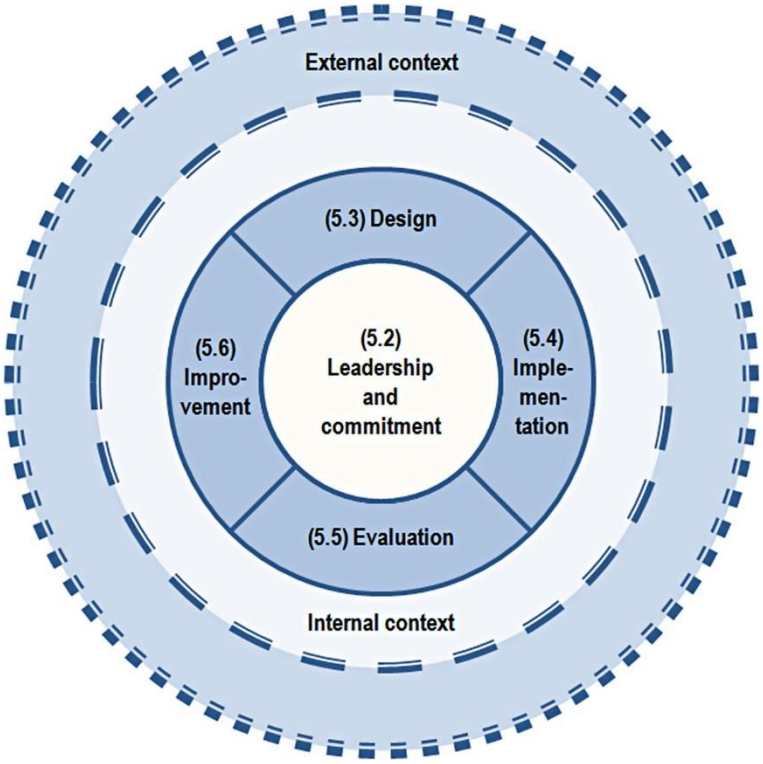

Figure 3 — Framework

This framework is intended to assist the organization to integrate risk management into all its activities by offering a structure for implementing the risk management process as a basis for decision making and accountability at all levels of the organization.

The following clauses describe the components of the framework and the way in which they work together. The components should be customized to the specific needs of the organization.

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 document.

5.2.Leadership and commitment

5.2.1. General

Top management and oversight bodies should establish the intent of the organization to manage risk and demonstrate leadership and commitment by:

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

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

— defining and endorsing the risk management policy;

— ensuring that the necessary resources are allocated to the management of risk;

— assigning accountabilities, responsibilities and authority at appropriate levels within the organization;

— recognising and addressing contractual obligations as well as voluntary commitments;

— establishing risk criteria, risk appetite and risk tolerance, ensuring that they are understood, articulated and communicated to stakeholders;

— ensuring that the risk management performance indicators are part of the performance indicators of the organization including communicating these indicators;

— communicating the value of risk management to the organization and its stakeholders;

— promoting systematic monitoring of risks;

— ensuring that the framework and process for managing risk continue to remain appropriate;

Top management can demonstrate leadership by tracking continual improvement of risk management within the organization by emphasising the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.

Assessing the progress of risk management within an organization is an integral part of the organization’s governance.

NOTE Top management is accountable for managing risk while risk oversight bodies such as boards of directors are accountable for overseeing risk management.

5.2.2. Integrating risk management

Top management should ensure that risk management is integrated into all organizational activities. Integrating risk management into an organization is a dynamic and iterative process, and should be customized to the organization’s needs and culture.

The design of the risk management framework should facilitate the integration of the risk management process into decision-making and the overall management of the organization. The organization should evaluate any gaps in its existing approaches for managing risk, then address those gaps within the framework. The risk management process should become part of, and not separate from, organizational processes.

5.3.Design

5.3.1. Understanding the organization and its context

When designing the framework for managing risk, the organization should examine and understand its external and internal context.

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

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

— key drivers and trends affecting the objectives of the organization;

— external stakeholders' relationships, perceptions, values and expectations;

— contractual relationships and commitments; and

— the complexity of networks and dependencies.

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

— vision, mission and values;

— governance, organizational structure, roles and accountabilities;

— strategies, objectives and policies;

— standards, guidelines and models adopted by the organization;

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

— information systems, information flows ;

— relationships with internal stakeholders taking into account their perceptions and values;

— the organization's culture;

— contractual relationships and commitments; and

— interdependencies.

5.3.2. Articulate risk management commitment(s)

Top management should articulate their commitment to risk management which can be through a policy, a statement or other forms, that clearly convey an organization's objectives and commitment to risk management. The commitment should include:

— the organization's purpose for managing risk and links to the organization's objectives and other policies;

— accountabilities and responsibilities;

— making the necessary resources available;

— the way in which conflicting objectives are dealt with;

— measurement and reporting within the organization's performance indicators; and

— review and improvement.

The risk management commitment should be communicated as appropriate within an organization and stakeholders.

5.3.3. Assigning organizational roles, accountabilities, responsibilities and authorities

Top management should ensure that the accountabilities, responsibilities and authorities for relevant roles with respect to risk management are assigned and communicated at all levels of the organization:

— emphasizing that risk management is a core responsibility; and

— identifying individuals that have the accountability and authority to manage risk (sometimes referenced as risk owners).

5.3.4. Allocating resources

Top management should ensure allocation of appropriate resources for risk management that can include:

— 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

— professional development and training needs.

The organization should consider the capabilities of, and constraints on, existing resources.

5.3.5. Establishing communication and consultation

The organization should establish communication and consultation to facilitate the exchange of information and effective application of risk management. Communication requires imparting or exchanging information. Consultation is undertaken specifically to share views or knowledge. Communication and consultation should reflect the expectations of identified internal and external stakeholders.

Communication and consultation should be in a timely manner and ensure that relevant information is captured, consolidated and shared as appropriate and, feedback is provided and improvements are made.

5.4. Implementation

The organization should implement the risk management framework by:

— developing an appropriate plan including timing;

— identifying where, when, and how different types of decisions are made across the organization, and by whom;

— modifying the applicable decision-making processes where necessary; and

— ensuring that the organization's arrangements for managing risk are clearly understood and practiced.

Successful implementation of the framework requires the engagement and awareness of stakeholders. This enables organizations to explicitly address uncertainty as part of decision making, while also ensuring that any new or subsequent uncertainty can be taken into account as it arises.

Properly designed and implemented, the risk management framework will ensure that the risk management process is a part of all activities including decision-making throughout the organization.

5.5. Evaluation

In order to assess the effectiveness of the risk management framework the organization should:

— periodically measure risk management framework performance against its purpose, implementation plans and expected behaviours;

— determine whether it remains suitable to achieve the objectives of the organization.

5.6. Improvement

5.6.1. Adapting

The organization should continually monitor and adapt the risk management framework to address internal and external changes to the organization. In doing so the organization can improve its resilience.

5.6.2. Continually improving

The organization should continually improve suitability, adequacy and effectiveness of the risk management framework and the way the risk management process is integrated.

As relevant gaps or improvement opportunities are identified, the organization should develop plans and tasks and assign them to those accountable for implementation. Once implemented, these improvements should contribute to advances in risk management maturity.

6 Process

6.1.General

The risk management process provides a consistent and structured approach for establishing context, risk assessment and risk treatment along with ongoing monitoring, review, communication and consultation. See Figure 4.

The risk management process should be an integral part of management and decision making and integrated into the structure, operations and business processes. It can be applied at strategic, operational, program or project levels.

There can be many applications of the risk management process within an organization, customized to achieve objectives and suit the external and internal context in which they are applied.

The dynamic and variable nature of human behaviour and culture should be considered throughout the risk management process.

Although the risk management process is often presented as sequential, in practice it is iterative.

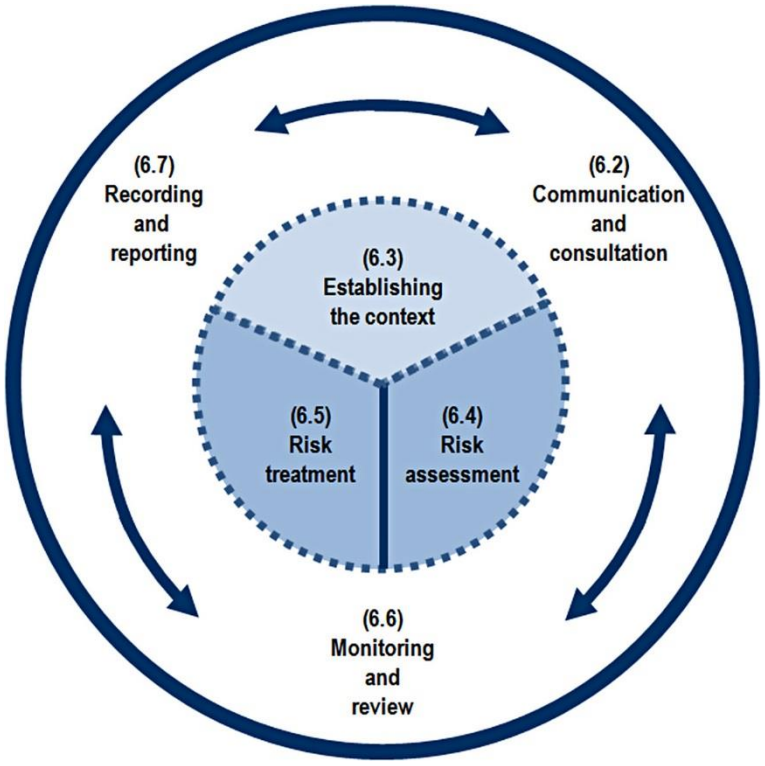

Figure 4 — Process

6.2.Communication and consultation

Communication and consultation with appropriate external and internal stakeholders should take place within all steps of the risk management process.

The purpose of communication and consultation is to assist relevant stakeholders in understanding the basis on which decisions are made, and the reasons why particular actions are required. This should

facilitate factual, timely, relevant, accurate and understandable exchanges of information, taking into account the confidentiality and integrity of information as well as the privacy rights of individuals.

Communication and consultation aims to:

— bring different areas of expertise together for each step of the risk management process;

— provide sufficient information to facilitate risk oversight; and

— build a sense of inclusiveness and ownership among those affected by risk.

6.3. Establishing the context

6.3.1. General

It is essential for an organization to determine the internal and external factors that can influence the way in which it will manage risk. Conducting this analysis provides an understanding of the internal and external influences and their effect on objectives and outcomes. By establishing the context, an organization can define the scope of its risk management processes and design a fit-for-purpose approach to managing risk.

Successful establishment of the context will enhance the risk assessment and treatment processes.

6.3.2. Defining the purpose and scope of the process

The organization should define the purpose and scope of its risk management activities. To determine completeness and appropriateness, the purpose and scope should be revisited and re-evaluated based on information identified in establishing the context and assessing the risks. It can involve, but is not limited to:

— considering the decisions that have to be made and associated objectives;

— outcomes expected from the various process steps;

— scope in terms of time, location, specific inclusions and exclusions;

— selecting appropriate risk assessment techniques; and

— resources required, responsibilities and records to be kept.

6.3.3. Internal and external context

The internal and external context is the environment in which the organization seeks to define and achieve its objectives. Common factors between the internal and external environment are:

— risk management takes place in the context of the objectives and activities of the organization;

— organizational factors can be a source of risk; and

— purpose and scope of where the risk management process is being applied may be interrelated to the objectives of the organization as a whole.

For external and environmental factors refer to 5.3.1.

6.3.4. Defining risk criteria

The organization should identify and define its risk criteria in order to evaluate the significance and level of acceptability of risk to support decision making processes. Risk criteria should be aligned to the risk management framework and customised to the specific purpose and scope of the activity under consideration.

Risk criteria should reflect the organization's values, objectives and resources. The criteria should be defined taking into consideration the organization’s legal, regulatory and contractual obligations, voluntary commitments (e.g. human rights and social responsibility) and stakeholder views.

While risk criteria should be established at the beginning of the risk assessment process, they are dynamic and should be continually reviewed and amended if required.

Criteria should be consistent with the organization’s policies and statements about risk management.

Risk criteria should consider:

— the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible);

— how likelihood and consequences (both positive and negative) will be defined and measured;

— timeframes;

— consistency in the use of measurements;

— how the level of risk is to be determined;

— how combinations and sequences of multiple risks will be taken into account.

Risk criteria should specify the types and level of risk or group of risks that an organization is prepared to pursue, retain or take relative to their objectives (risk appetite).

6.4. Risk assessment

6.4.1. General

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

Risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use best available information supplemented by further enquiry as necessary.

6.4.2. Risk identification

The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization achieving their objectives. Relevant, appropriate and up-to-date information is important in identifying risks.

The organization can use a range of techniques for identifying uncertainties which may affect one or more objectives. The following factors and the interplay between these factors should be considered:

— tangible and intangible sources of risk;

441 — causes and events,

442 — threats and opportunities;

443 — vulnerabilities and capabilities;

444 — changes to the internal and external context;

445 — nature and value of assets and organizational resources;

446 — criticality and consequences;

447 — limitations of knowledge and reliability of information;

448 — timeframes and time influences; and

449 — bias, assumptions and beliefs of those involved.

450 The organization should identify risks whether or not their source is under their control. Consideration
451 should be given that there may be more than one type of outcome which may result in a variety of
452 tangible or intangible consequences.

453 **6.4.3. Risk analysis**

454 The purpose of risk analysis is to comprehend the nature of risk and to determine the level of risk

455 Risk analysis provides an input to risk evaluation, to decisions on whether and how risks need to be
456 treated and on the most appropriate risk treatment strategies and methods. It can also provide an input
457 into making decisions where choices are being made and the options involve different types and levels
458 of risk.

459 Risk analysis involves a detailed consideration of uncertainties, risk sources, events and scenarios,
460 likelihoods and consequences. An event can have multiple consequences and can affect multiple
461 objectives.

462 Risk analysis can be undertaken with varying degrees of detail, and formality depending on the purpose
463 of the analysis, the availability and reliability of information, and the resources available. Analysis
464 techniques can be qualitative, semi-quantitative or quantitative or a combination of these depending on
465 the circumstances and intended use.

466 Risk analysis should consider factors such as :

467 — likelihood of events and consequences;

468 — nature and magnitude of consequences;

469 — timeframes and volatility;

470 — effectiveness of existing controls;

471 — sensitivity and confidence levels.

The risk analysis may be influenced by any divergence of opinions; biases, perceptions of risk and judgements. Additional influences are the quality of the information used; the assumptions and exclusions made; any limitations of the techniques and how they are executed. These influences should be considered, documented and communicated to decision makers.

Highly uncertain events may be difficult to quantify. This can be an issue when analysing events with severe consequences.

6.4.4. Risk evaluation

The purpose of risk evaluation is to assist in making decisions on prioritization and treatment of risk. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria.

Decisions should take account of the wider context of the risk and the actual and perceived consequences for internal and external stakeholders. Decisions should be made in accordance with legal, regulatory and other requirements.

The risk evaluation should lead to a decision to consider risk treatment options; to undertake further analysis, to maintain existing controls, or to reconsider objectives.

The outcome of risk evaluation should be recorded, communicated and confirmed by top management.

6.5. Risk treatment

6.5.1. General

Risk treatment involves selecting and implementing options for addressing risk.

Risk treatment involves an iterative process of:

— formulating and selecting risk treatment;

— implementing risk treatment;

— deciding whether residual risk levels are acceptable;

— if not acceptable, generating further risk treatment; and

— assessing the effectiveness of that treatment.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Options for treating risk may involve one or more of the following:

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

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

— removing the risk source;

— changing the likelihood;

— changing the consequences;

— sharing the risk (e.g. through contracts, buying insurance);

— retaining the risk by informed decision.

6.5.2. Selection of risk treatment options

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against any costs, effort, or disadvantages of implementation. Justification for risk treatment may be broader than economic considerations and take into account the organization's contractual obligations, voluntary commitments (e.g. human rights and social responsibility) and stakeholder views. The selection of risk treatment options should be made in accordance with the organization's objectives, risk criteria and available resources.

When selecting risk treatment options, the organization should consider the values, perceptions and potential involvement of stakeholders and the most appropriate ways to communicate and consult with them. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

Even if carefully designed and implemented, risk treatments might not produce the expected outcomes. It can also create unintended consequences inside or outside the organization. Monitoring needs to be an integral part of the risk treatment implementation to give assurance that the treatments remain effective.

Risk treatment can also introduce new risks that need to be managed.

If there are no treatment options available or if treatment options do not sufficiently modify the level of risk, the risk should be recorded and kept under ongoing review by top management.

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.

6.5.3. Preparing and implementing risk treatment plans

The purpose of risk treatment plans is to specify how the chosen treatment options will be implemented so that arrangements are understood by those involved and progress against the plan can be monitored. The treatment plan should clearly identify the order in which risk treatments should be implemented.

The information provided in the treatment plan should include:

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

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

— the proposed actions;

— the resource requirements including contingencies;

— the performance measures and constraints;

— the reporting and monitoring requirements; and

— timing and schedule.

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

6.6. Monitoring and review

Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined.

Monitoring and review should take place at all steps of the process to assure the quality and effectiveness of process design, implementation and outcomes. Monitoring and review includes planning, gathering and analyzing information, recording results and providing feedback.

The results of monitoring and review should be incorporated into the organization's overall performance management, measurement and reporting activities.

6.7. Recording and reporting

The risk management process and its implementation should be documented and reported. Recording and reporting facilitates:

— communication of risk management activities and outcomes across the organization;

— provision of information for decision making;

— improvement of risk management activities;

— interaction with stakeholders, including those with responsibility and accountability for risk management activities.

Decisions concerning the creation, retention and handling of documented information should take into account, but not be limited to, their use, information sensitivity, and internal and external context.

Reporting is an integral part of organization's governance and should enhance the quality of dialogue with stakeholders. Factors to consider for reporting include, but are not limited to:

— differing stakeholders and their specific information needs;

— frequency and timeliness of reporting;

— method of reporting;

— relevance of information to organizational objectives and decision making.

Bibliography

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

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