DRAFT INTERNATIONAL STANDARD ISO/DIS 31000

ISO/PC **992** Secretariat: **TMB**

Voting begins on: **2008-04-01** Voting terminates on: **2008-09-01**

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Risk management — Principles and guidelines on implementation

Management du risque — Principes et lignes directrices de mise en application

ICS 03.100.01

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

Contents

Page

Foreword iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Principles for managing risk 1
5 Framework for managing risk 3
5.1 General 3
5.2 Mandate and commitment 4
5.3 Design of framework for managing risk 4
5.3.1 Understanding the organization and its context 4
5.3.2 Risk management policy 5
5.3.3 Integration into organizational processes 5
5.3.4 Accountability 5
5.3.5 Resources 5
5.3.6 Establishing internal communication and reporting mechanisms 6
5.3.7 Establishing external communication and reporting mechanisms 6
5.4 Implementing risk management 6
5.4.1 Implementing the framework for managing risk 6
5.4.2 Implementing the risk management process 7
5.5 Monitoring and review of the framework 7
5.6 Continual improvement of the framework 7
6 Process for managing risk 7
6.1 General 7
6.2 Communication and consultation 8
6.3 Establishing the context 9
6.3.1 General 9
6.3.2 Establishing the external context 9
6.3.3 Establishing the internal context 9
6.3.4 Establishing the context of the risk management process 10
6.3.5 Developing risk criteria 10
6.4 Risk assessment 11
6.4.1 General 11
6.4.2 Risk identification 11
6.4.3 Risk analysis 11
6.4.4 Risk evaluation 12
6.5 Risk treatment 12
6.5.1 General 12
6.5.2 Selection of risk treatment options 13
6.5.3 Preparing and implementing risk treatment plans 13
6.6 Monitoring and review 13
6.7 Recording the risk management process 14
Annex A (Informative) Attributes of enhanced risk management 15
A.1 General 15
A.2 Attributes 15
Bibliography 17

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.

This standard may be revised after 5 years on the basis of practical experience. Committees writing standards are invited to inform the ISO Central Secretariat of any difficulties encountered with the implementation of its provisions.

Introduction

Organizations of all types and sizes face a range of risks that can affect the achievement of their objectives.

These objectives can relate to a range of the organization's activities, from strategic initiatives to its operations, processes and projects, and be reflected in terms of strategic, operational, financial and reputational outcomes and impacts.

All activities of an organization involve risks. Risk management aids decision making by taking account of uncertainty and its effect on achieving objectives and assessing the need for any actions.

Risk management process involves applying logical and systematic methods for:

— communication and consultation throughout the process;

— establishing the context;

— identifying, analyzing, evaluating and treating risk associated with any activity, process, function, project, product, service or asset;

— monitoring and reviewing risk; and

— recording and reporting the results appropriately.

This International Standard recognizes the variety of the nature, level and complexity of risks and provides generic guidelines on principles and implementation of risk management. To apply these generic guidelines in a specific situation, this International Standard sets out how an organization should understand the specific context in which it implements risk management.

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

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

— encourage proactive rather than reactive management;

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

— improve identification of opportunities and threats;

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

— improve financial reporting;

— improve corporate 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;
- improve incident management and prevention;
- minimize loss;
- Improve organizational learning; and
- Improve organizational resilience.

Risk management should ensure that organizations have an appropriate response to the risks affecting them. Risk management should thus help avoid ineffective and inefficient responses to risk that can unnecessarily prevent legitimate activities and/or distort resource allocation.

To be effective within an organization, risk management should be an integrated part of the organization's overall governance, management, reporting processes, policies, philosophy and culture.

The same risk management approach can be adopted for all activities of an organization including projects, defined functions, assets, and products or activities and will in turn strengthen the linkages between these activities and the organization’s overall objectives.

This International Standard is intended to be used by a wide range of stakeholders including:

- those responsible for implementing risk management within their organization;
- those who need to ensure that an organization manages risk;
- those who need to manage risk for the organization as a whole or within a specific area or activity;
- those needing to evaluate an organization’s practices in managing risk; and
- 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.

Many organizations' existing management practices and processes include components of risk management and many organizations have already adopted a formal risk management process for particular types of risk or circumstances. Management can decide to critically review their existing practices and processes in light of this standard.

Although the practice of risk management has been developed over time and within many sectors to meet diverse needs, a generic approach consisting of a framework of essential components can help to ensure that risk is managed effectively and coherently across an organization. The generic approach described in this International Standard provides guidelines on implementing essential components for managing risk in a transparent and credible manner 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 process of risk management. This feature will capture the diversity of criteria as well as the nature and complexity of risk and other factors that need to be considered and managed in each case.

Some areas of risk management within, for example, the areas of safety, human health and environment, impose criteria that reflect an aversion to negative consequences. Such criteria can be contained in legal and regulatory requirements and international norms. The application of the risk management approach described in this International Standard helps to ensure that those criteria are identified and applied. Therefore, this

International Standard can also help an organization to comply with legal and regulatory requirements and international norms as well as to improve an organization's performance.

The relationship between the principles for managing risk, the risk management framework and the risk management process described in this standard is shown in Figure 1.

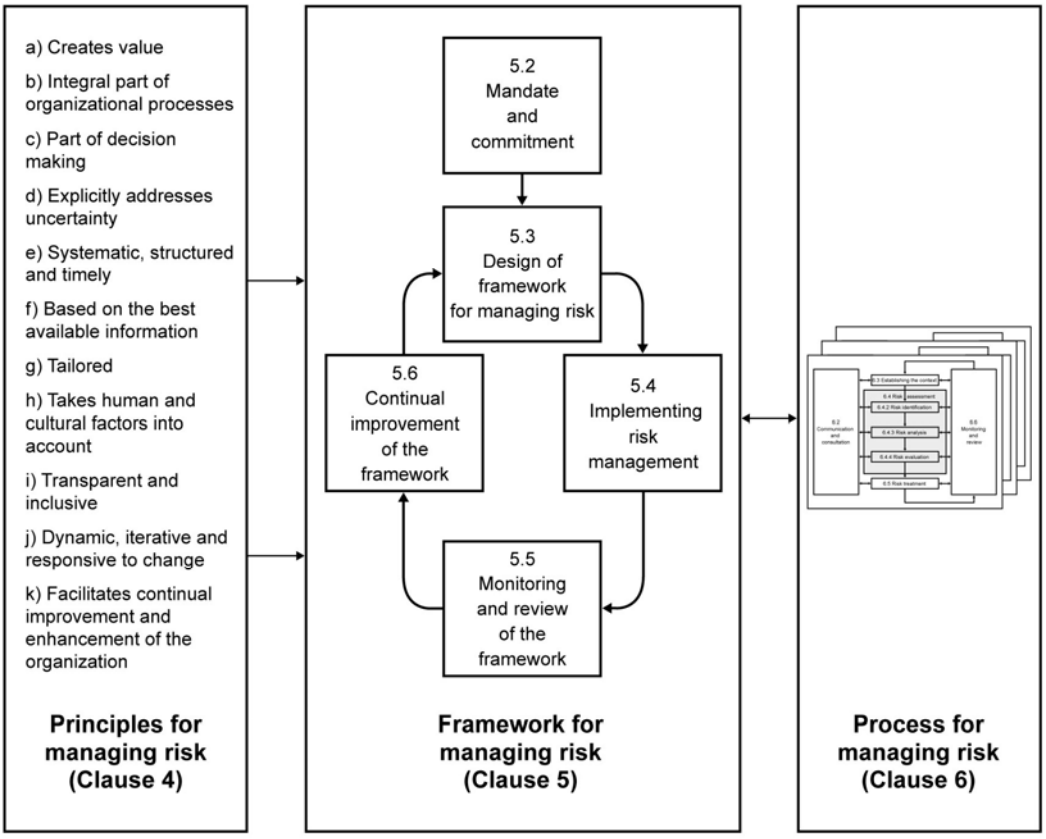

Figure 1 — Relationship between the risk management principles, framework and process

Risk management — Principles and guidelines on implementation

1 Scope

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

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

NOTE For convenience, all the different addressees 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, processes, functions, projects, products, services, assets, operations and decisions.

Although this International Standard provides generic guidelines, it is not intended to impose uniformity of risk management across organizations. The design and implementation of risk management will depend on the varying needs of a specific organization, its particular objectives, context, structure, products, services, projects, the operational processes and specific practices employed.

This International Standard intends 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 to be used for the purpose of certification.

2 Normative references

The following referenced document is indispensable for the application of this document. For dated reference, only the edition cited applies.

ISO/IEC Guide 73, *Risk management — Vocabulary*[1].

3 Terms and definitions

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

4 Principles for managing risk

To be most effective, an organization's risk management should adhere to the following principles.

a) Risk management creates value.

[1] To be published.

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

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

Risk management is part of the responsibilities of management and an integral part of the normal organizational processes as well as of all project and change management processes. Risk management is not a stand-alone activity which is separate from the main activities and processes of the organization.

c) Risk management is part of decision making.

Risk management helps decision makers make informed choices. Risk management can help prioritize actions and distinguish among alternative courses of action. Ultimately, risk management can help with decisions on whether a risk is unacceptable and whether risk treatment will be adequate and effective.

d) Risk management explicitly addresses uncertainty.

Risk management deals with those aspects of decision making that are uncertain, 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 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 experience, feedback, observation, forecasts and expert judgement. However, decision makers should be informed 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.

The organization’s 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.

As internal and external events occur, context and knowledge change, monitoring and review take place, new risks emerge, some change, and others disappear. Therefore an organization should ensure that risk management continually senses and responds to change.

k) Risk management facilitates continual improvement and enhancement of the organization.

Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization. Annex A "Attributes of enhanced risk management" provides further information.

5 Framework for managing risk

5.1 General

To be successful, risk management should function within a risk management framework which provides the foundations and organizational arrangements that will embed it throughout the organization at all levels. The framework assists an organization in managing its risks effectively through the application of the risk management process (see Clause 6) at varying levels and within specific contexts of the organization. The framework should ensure that risk information derived from these processes is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels.

This clause describes the components of the framework for managing risk that are necessary and the way in which they interrelate as shown in Figure 2.

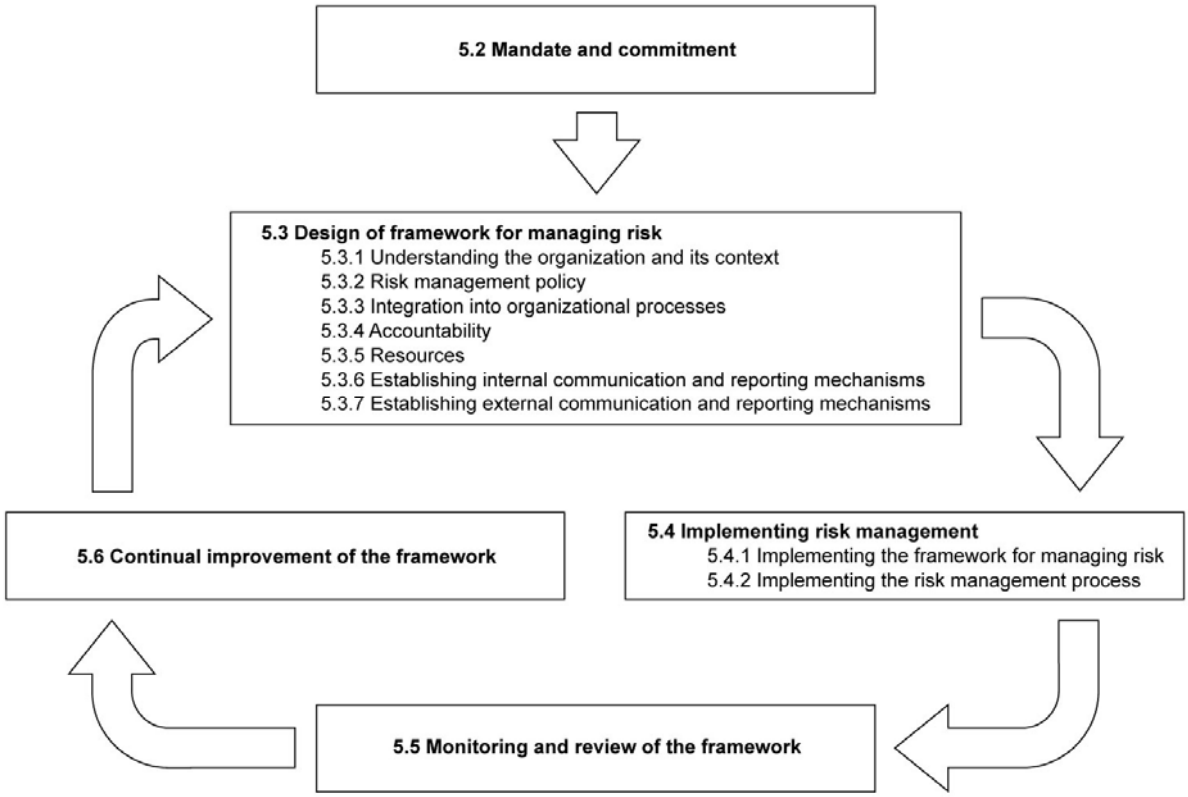

Figure 2 — Components of the framework for managing risk

This framework is not intended to describe a management system; but rather, it is to assist the organization to integrate risk management within 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 as the basis for determining their adequacy.

5.2 Mandate and commitment

The introduction of risk management and ensuring its on-going effectiveness requires strong and sustained commitment by management of the organization as well as strategic and rigorous planning. Management should:

— articulate and endorse the risk management policy;

— determine risk management performance indicators that align with organizational performance indicators;

— ensure alignment of risk management objectives with the objectives and strategies of the organization;

— ensure legal and regulatory compliance;

— assign management 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.

5.3 Design of framework for managing risk

5.3.1 Understanding the organization and its context

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

Aspects of the organization's external context include, but not limited to:

— the 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

— perceptions and values of external stakeholders.

Aspects of the organization's internal context include, but not limited to:

— 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);

— internal stakeholders;

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

— perceptions, values and culture;

— standards and reference models adopted by the organization; and

— structures (e.g. governance, roles and accountabilities).

5.3.2 Risk management policy

The risk management policy should clarify the organization's objectives for and commitment to risk management and should specify the following:

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

— the organization's rationale for managing risk;

— accountabilities and responsibilities for managing risk;

— the way in which conflicting interests are dealt with;

— the organization’s risk appetite or risk aversion;

— processes, methods and tools to be used for managing risk;

— resources available to assist those accountable or responsible for managing risk;

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

— commitment to the periodic review and verification of the risk management policy and framework and its continual improvement; and

The risk management policy should be communicated appropriately.

5.3.3 Integration into organizational processes

Risk management should be embedded in all the organization’s practices and business processes so 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 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 the organization’s practices and business processes.

5.3.4 Accountability

The organization should ensure that there is accountability and authority for managing risks, including the implementation and maintenance of the risk management process and ensure the adequacy and effectiveness of any risk controls. This can be facilitated by:

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

— specifying risk owners for implementing risk treatment, maintaining risk controls and reporting of relevant risk information;

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

— ensuring appropriate levels of recognition, reward, approval and sanction.

5.3.5 Resources

The organization should develop the practical means to allocate appropriate resources for risk management.

Consideration should be given to the following:

— people, skills, experience and competences;

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

— documented processes and procedures; and

— information and knowledge management systems.

5.3.6 Establishing internal communication and reporting mechanisms

The organization should establish internal communication and reporting mechanisms. These 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 include processes to consolidate risk information where appropriate from a variety of sources within the organization taking into account its sensitivity.

5.3.7 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 corporate governance requirements;

— making legally required disclosures;

— 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.

5.4 Implementing risk management

5.4.1 Implementing the framework for managing risk

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

— define an 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;

— document justified decision making, including the development and setting of objectives which are aligned with the outcomes of the risk management process;

— hold information and training sessions; and

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

5.4.2 Implementing the risk management process

Risk management is implemented by ensuring that the risk management process outlined in Clause 6 is applied at all relevant levels and functions of an organization as part of the organization's practices and business processes.

5.5 Monitoring and review of the framework

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

— establish performance measures;

— 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' internal and external context;

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

— review the effectiveness of the risk management framework.

5.6 Continual improvement of the framework

Based on the review, 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 risk management, and risk management culture.

6 Process for managing risk

6.1 General

The risk management process should be an integral part of management, be embedded in culture and practices and tailored to the business processes of the organization. It comprises the activities described from 6.2 to 6.7. The risk management process includes five activities: communication and consultation, establishing the context, risk assessment, risk treatment, monitoring and review as shown in Figure 3. These activities, as well as recording the risk management process, are described in this clause.

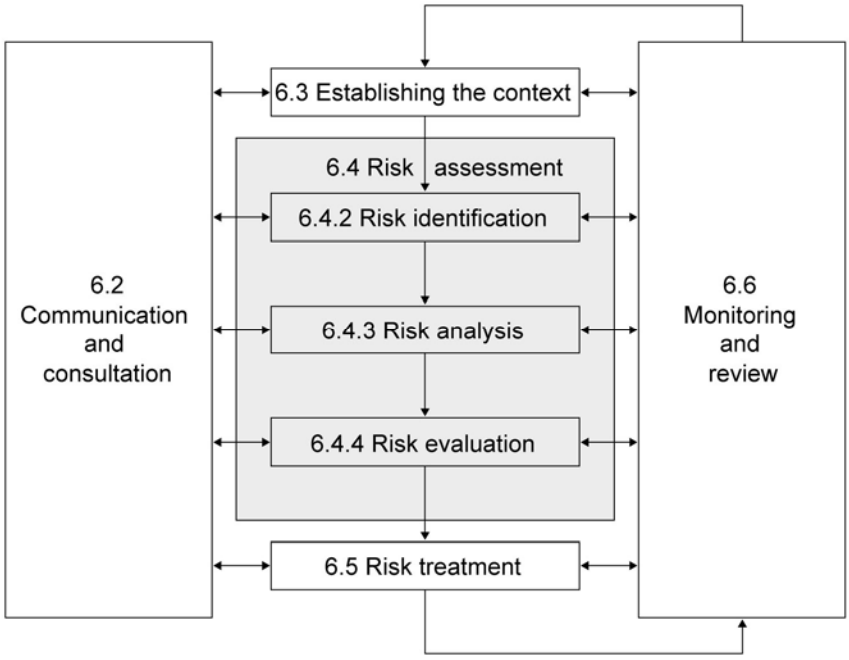

Figure 3 — Risk management process

6.2 Communication and consultation

Communication and consultation with internal and external stakeholders as far as necessary should take place at each stage of the risk management process.

Therefore, a plan to communicate and consult with both internal and external stakeholders should be developed at an early stage. This plan should address issues relating to the risk itself, its consequences (if known), and the measures being taken to manage it.

Effective internal and external 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 reason why particular actions are required.

A consultative team approach is useful to, but not limited to:

— help define the context appropriately;

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

— bring different areas of expertise together for analyzing risks;

— help ensure that risks are adequately identified;

— ensure that different views are appropriately considered in evaluating risks;

— enhance appropriate change management during the risk management process;

— secure endorsement and support for a treatment plan; and

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

Communication and consultation with stakeholders is important as they make judgements about risk based on their perceptions of risk. Perceptions of risk 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, it is important that the stakeholders' perception is identified, recorded, and taken into account in the decision making process.

The communication and consultation plan should:

— be an exchange of information between stakeholders;

— convey messages which are honest, accurate, understandable and based on evidence; and

— be useful; and the value of the contributions be assessed.

6.3 Establishing the context

6.3.1 General

By establishing the context the organization defines the internal and external parameters to be taken into account when managing risk, and setting the scope and risk criteria for the remaining process. The context should include both internal and external parameters relevant for the organization. While many of these parameters are similar to those considered in the design of the risk management framework (see 5.3.1), 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.

6.3.2 Establishing the external context

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

Understanding the external context is important to ensure that external stakeholders, their objectives and concerns 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 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

— perceptions and values of external stakeholders.

6.3.3 Establishing the internal context

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 and structure. Internal context is anything within the organization that can influence the way in which an organization will manage risk. It should be established because:

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

— objectives and criteria of a particular project or activity should be considered in the light of objectives of the organization as a whole; and

— a major risk for some organizations is failure to achieve their strategic, project or business objectives, and this risk affects ongoing organizational commitment, credibility, trust and value.

It is necessary to understand the internal context, in terms of, for example:

— 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) ;

— internal stakeholders;

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

— perceptions, values and culture; and

— standards and reference models adopted by the organization.

— structures (e.g. governance, roles and accountabilities).

6.3.4 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 responsibilities for 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 as well as its goal and objectives;

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

— defining the risk assessment methodologies;

— defining the way performance 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 situation of the organization and to the risks affecting the achievement of its objectives.

6.3.5 Developing risk criteria

The organization should develop criteria that are used to evaluate the significance of risk. The criteria can reflect the organizations 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 5.3.2). Risk criteria should be developed at the beginning of any risk management process and continually be reviewed.

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

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

— how likelihood will be defined;

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

— how the level of risk is to be determined;

— the level at which risk becomes acceptable or tolerable;

— what level of risk requires treatment; and

— whether combinations of multiple risks should be taken into account.

6.4 Risk assessment

6.4.1 General

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

6.4.2 Risk identification

The organization should identify sources of risk, areas of impacts, events 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 enhance, prevent, degrade or delay the achievement of the objectives. It is also important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis. Identification should include risks whether or not their source is under control of the organization.

The organization should apply risk identification tools and techniques which 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 suitable background information where possible. People with appropriate knowledge should be involved in identifying risks. After identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes should be considered.

6.4.3 Risk analysis

Risk analysis is about 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 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 risk controls and their effectiveness should 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 will vary according to 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 risk and their sensitivity to preconditions and assumptions should be considered in the analysis, and communicated effectively to decision makers and other stakeholders if

501 required. Factors such as divergence of opinion among experts or limitations on modelling should be stated
502 and may be highlighted.

503 Risk analysis can be undertaken with varying degrees of detail depending on the risk, the purpose of the
504 analysis, and the information, data and resources available. Analysis can be qualitative, semi-quantitative or
505 quantitative, or a combination of these, depending on the circumstances. In practice, qualitative analysis is
506 often used first to obtain a general indication of the level of risk and to reveal the major risks. When possible
507 and appropriate, one should undertake more specific and quantitative analysis of the risks as a following step.

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

512 #### 6.4.4 Risk evaluation

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

515 Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria
516 established when the context was considered. If the level of risk does not meet risk criteria, the risk should be
517 treated.

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

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

525 ### 6.5 Risk treatment

526 #### 6.5.1 General

527 Risk treatment involves selecting one or more options for modifying risks, and implementing those options.

528 Risk treatment involves a cyclical process of assessing a risk treatment; deciding whether residual risk levels
529 are tolerable or not; if not tolerable generating a new risk treatment; and assessing the effect of that treatment
530 until the residual risk reached complies with the organization's risk criteria.

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

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

534 — seeking an opportunity by deciding to start or continue with an activity likely to create or enhance the risk;

535 — removing the source of the risk;

536 — changing the nature and magnitude of likelihood;

537 — changing the consequences;

538 — sharing the risk with another party or parties; and

539 — retaining the risk by choice.

6.5.2 Selection of risk treatment options

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived having regard to legal, regulatory, and other requirements, social responsibility and the protection of the natural environment. Decisions should also take into account risks that can warrant risk treatment actions that are not justifiable on economic grounds e.g. severe (high negative consequence) but rare (low likelihood) risks. A number of treatment options can be considered an applied either individually or in combination. The organization can 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, these areas should be involved in the decision. Though equally effective, some risk treatments can be more acceptable to stakeholders than others.

If the resources for risk treatment are limited, 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, and the link between the two risks should be identified.

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 document how the chosen treatment options will be implemented. The information provided in treatment plans should include:

— expected benefit to be gained;

— performance measures and constraints;

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

— proposed actions;

— reporting and monitoring requirements;

— resource requirements; and

— timing and schedule.

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

6.6 Monitoring and review

Monitoring and review should be a planned part of the risk management process.

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:

- analyzing and learning lessons from events, changes and trends;
- detecting changes in the external and internal context including changes to the risk itself which can require revision of risk treatments and priorities;
- ensuring that the risk control and treatment measures are effective in both design and operation; and
- identifying emerging risks.

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

Monitoring and review can involve regular checking or surveillance of what is already present or can be periodic or ad hoc. Both aspects should be planned.

The results of monitoring and review should be recorded and internally or externally reported as appropriate and should also be used as an input to the review of the risk management framework (see 5.5).

6.7 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 the overall process.

Decisions concerning the creation of records should take into account:

- 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

The ability to manage risk is one of the core competencies of any organization and its employees. Risk management methods and tools assist any organization to plan and implement concrete actions and programs to maximize their opportunities and to control their threats.

The organization has greater control of its own growth and development when risk management is applied.

All organizations should aim at the highest 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 Attributes

A.2.1 An emphasis 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 would 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 could be published and communicated. Normally, there would 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.2.2 Comprehensive, fully defined and fully accepted accountability for risks, risk controls and risk treatment tasks. Designated individuals fully accept, are appropriately skilled and have adequate resources to check risk controls, monitor risks, improve risk controls and communicate effectively about risks and their management to internal and external stakeholders.

This would be indicated by all members of an organization being fully aware of the risks, risk 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 introduction programs.

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

A.2.3 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 is indicated through the examination of the records of meetings and decisions to show that explicit discussions on risks took place. Also, it should be possible to see that all components of risk management are represented within key processes for decision making in the organization; for example, 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 and prudent governance.

A.2.4 Continual communications with internal and external stakeholders including comprehensive and frequent reporting of risk management performance is part of good governance.

This is indicated by communication with stakeholders being clearly regarded as an integral and essential component of risk management so that communication with stakeholders can take place as part of each activity of the risk management process. Communication is rightly seen as a two way process so 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 internal and external reporting on both significant risks and on risk management performance contributes substantially to effective governance within an organization.

A.2.5 Risk management is viewed as central to the organization's management processes so that risks are considered in terms of effect of uncertainty on objectives. The organization’s 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 statement is also normally reflected in the organization’s statements of policy, particularly that 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/IEC Guide 73, *Risk management — Vocabulary*

[2] ISO/IEC Guide 51:1999, *Safety aspects — Guidelines for their inclusion in standards*

[3] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

[4] ISO 13702:1999, *Petroleum and natural gas industries — Control and mitigation of fires and explosions on offshore production installations — Requirements and guidelines*

[5] ISO 14050:2002, *Environmental management — Vocabulary*

[6] ISO 14121-1:2007, *Safety of machinery — Risk assessment — Part 1: Principles*

[7] ISO/TR 14121-2:2007, *Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods*

[8] ISO 14971:2007, *Medical devices — Application of risk management to medical devices*

[9] ISO 15265:2004, *Ergonomics of the thermal environment — Risk assessment strategy for the prevention of stress or discomfort in thermal working conditions*

[10] ISO 15544:2000, *Petroleum and natural gas industries — Offshore production installations — Requirements and guidelines for emergency response*

[11] ISO 17776:2000, *Petroleum and natural gas industries — Offshore production installations — Guidelines on tools and techniques for hazard identification and risk assessment*

[12] ISO 12100-1:2003, *Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology*

[13] ISO 13215-3:2005, *Road vehicles — Reduction of misuse risk of child restraint systems — Part 3: Prediction and assessment of misuse by Misuse Mode and Effect Analysis (MMEA)*

[14] ISO 13232-5:2005, *Motorcycles — Test and analysis procedures for research evaluation of rider crash protective devices fitted to motorcycles — Part 5: Injury indices and risk/benefit analysis*

[15] ISO/IEC 15408-1:2005, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

[16] ISO/IEC 15408-2:2005, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*

[17] ISO/IEC 15408-3:2005, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*

[18] ISO/IEC 31010 *Risk management – Risk assessment guidelines, to be published*

[19] ISO 16312-1:2006, *Guidance for assessing the validity of physical fire models for obtaining fire effluent toxicity data for fire hazard and risk assessment — Part 1: Criteria*

[20] IEC 60812:2006, *Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)*

[21] IEC 60300-1:2003, *Dependability management — Part 1: Dependability management systems*

[22] IEC 60300-2:2004, *Dependability management — Part 2: Guidelines for dependability management*

[23] IEC 61508-2:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

[24] IEC 61882:2001, *Hazard and operability studies (HAZOP studies) — Application guide*

[25] IEC 62198:2001, *Project risk management — Application guidelines*

[26] IEC 62305-2:2006, *Protection against lightning — Part 2: Risk management*