	ISO/TMB/WG Risk Management Secretariat of ISO TMB WG on Risk Management E-mail: risk-management@jsa.or.jp
Doc. ISO/TMB/RMWG	N 47
Date: 2007-06-15	

Title:	Committee Draft of ISO 31000 “Risk management — Guidelines on principles and implementation of risk management”
Source:	ISO TMB WG on Risk Management Secretariat
TO	**Member bodies** that sent experts to the WG on Risk Management Circulated for comment and vote
TO	**Liaison organizations** Circulated for comment
CC	Experts
	Comments will be accepted through 15th September, 2007. **Comments received after 15th September, 2007 will not be circulated or considered** in the 5th meeting. Please send comments and votes by E-mail to risk-management@jsa.or.jp. To submit comments, please follow the instructions given in N 49. Explanations on the highlighted part of this document are also given in N49.
Medium:	ISO/Livelink www.iso.org/rm, folder “03.Projects”, under Sub-folder ”N047 2007-06-15 to 2007-09-15 Circulation of Committee Draft of ISO 31000”

COMMITTEE DRAFT ISO/CD 31000	
Date 2007-06-15	Reference number **ISO/TMB WG on Risk management** **N 47**
Supersedes document N29	

WARNING: This document is not an International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

ISO/TMB WG on Risk management Secretariat JISC	Circulated to member bodies that sent experts to this WG and organizations in liaison for: ☒ discussion at China on 2007-12-03 to 12-07 [venue/date of meeting] ☒ comments by 2007-09-15 [date] ☒ approval for registration as a DIS in accordance with 2.5.6 of part 1 of the ISO/IEC Directives, by 2007-09-15 [date] (members vote only: ballot form attached) **Members have an obligation to vote.** **Liaison members can comment but cannot submit a vote**

English title

Risk management — Guidelines on principles and implementation of risk management

French title

Reference language version: ☒ English ☐ French ☐ Russian

Introductory note

ISO/TMB WG on Risk management N 047

Date: 2007-06-15

ISO CD 31000

ISO/TMB WG on Risk management

Secretariat: JISC

Risk management — Guidelines on principles and implementation of risk management

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (30) Committee
Document language:E

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.

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 may affect the achievement of their objectives.

These objectives may relate to a range of the organization's activities, from strategic initiatives to its operations, processes and projects, and be reflected in terms of societal, environmental, safety and security outcomes, commercial, financial and economic measures, as well as social, cultural, political and reputation impacts.

All activities of an organization involve risks that must be managed. The risk management process aids decision making by taking account of uncertainty and the possibility of future events or circumstances (intended or unintended) and their effects on agreed objectives.

Risk management involves applying logical and systematic methods for:

— communicating and consulting throughout this process;

— establishing the organization’s context for identifying, analysing, evaluating, treating, and monitoring risk associated with any activity, product, function or process; 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. This International Standard sets out how an organization should understand the specific context in which it implements risk management.

Risk management can be applied across many areas, to specific functions and levels of an organization as well as to the entire organization.

When implemented and sustained in accordance with this standard, risk management should enable an organization to achieve, for example:

— awareness of the need to treat and manage risk in organizations;

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

— confident and rigorous basis for decision making and planning;

— definitions of controls to empower decision making and planning;

— effective allocation and use of resources for risk treatment;

— enhanced safety;

— improved corporate governance;

— improved financial reporting;

— improved identification of opportunities and threats;

— improved incident management and prevention;

— improved operational effectiveness and efficiency;

— improved stakeholder confidence and trust;

— loss reduction; and

— proactive rather than reactive management.

Achieving these aims should ensure that organizations have a balanced and proportionate response to the risks affecting them. Risk management should thus help avoid an over-reaction to risk that can unnecessarily prevent legitimate activity and/or seriously distort resource allocation.

To be effective within an organizational context, risk management should be developed by taking account of the organization's overall governance, management, reporting processes, policies, philosophy and culture. Indeed, the use of risk management can be expected to strengthen these areas.

The same risk management approach can be used within this wide variety of specific contexts such as a project, defined function, asset, product or activity. The adoption of this risk management approach will in turn strengthen the linkages between, and support *the aims of, a specific project, activity or function to the organization's overall objectives.*

This International Standard is intended to be used by all stakeholders such as:

— 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 their documents;

— those needing to evaluate an organization's practices in managing risk;

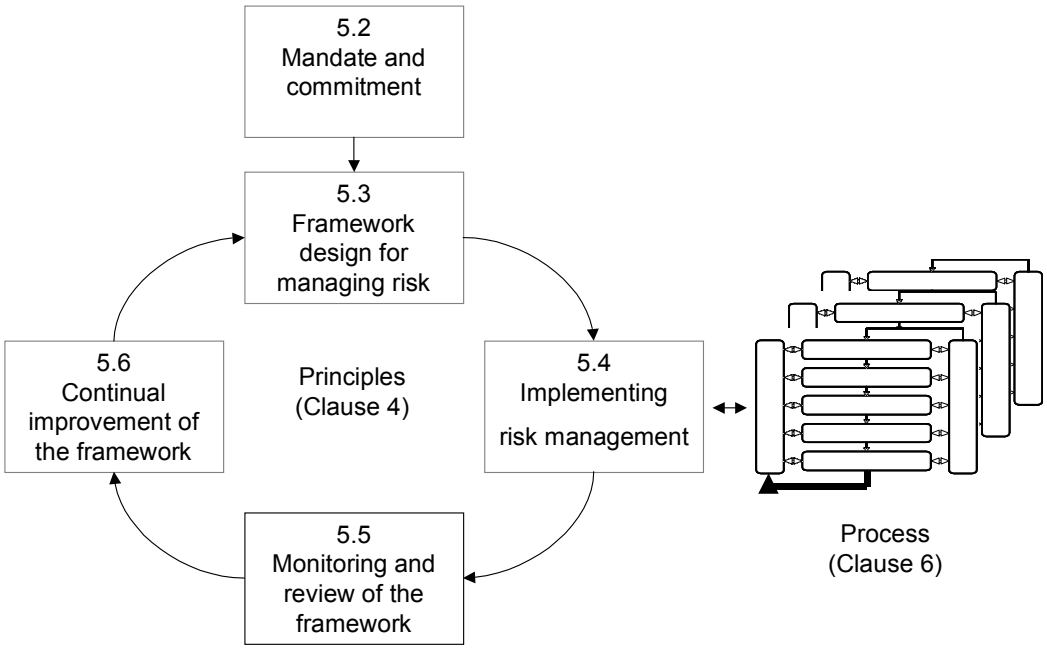
— those who need to ensure that an organization manages risk; and

— those within an organization who need to manage risk within a specific area or activity.

Although the practice of risk management has developed over time and within diverse sectors to meet diverse needs, a generic approach consisting of a framework of essential elements 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 these essential elements so as to manage risk within any scope and context with transparency and credibility.

Each specific sector or application of risk management brings with it individual needs, audiences, perceptions and criteria. A novel feature of this International Standard is the inclusion of "establishing the context" as a key activity at the start of this generic process. 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 may or may not be contained in legal, 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 be an aid to the management of compliance and performance. The relationship between the principles, framework and process described in this standard are shown in Figure 1.



146

147 **Figure 1 — Relationship between the principles, framework and process**

148

Risk management — Guidelines on principles and implementation of risk management

1 Scope

This International Standard gives generic guidelines for the principles and the adequate implementation of risk management. This International Standard also harmonizes risk management processes and definitions in existing and future standards.

This International Standard can be applied to a wide range of activities, decisions, and operations of any public, private or community enterprise, association, group or individual. Therefore, this International Standard is generic and not specific to any industry or sector. For convenience, all the different addressees of this International Standard are referred to by the general term “organization”.

This International Standard can be applied to all stages in the life cycle of an organization and its activity, process, function, project, product, service or asset.

This International Standard is a generic standard and intended to provide a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.

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

This International Standard is not intended to be used for the purpose of certification and cannot in itself be used for contractual purposes.

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 document, the terms and definitions given in Guide 73 apply.

4 Principles for managing risk

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

1) To be published.

a) Risk management should create value.

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

b) Risk management should be an integral part of organizational processes.

Risk management should be 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 should not be a stand-alone activity or be separate from the main activities and processes of the organization.

c) Risk management should be part of decision making.

Risk management can help prioritize actions and distinguish among alternative courses of action.

Risk management helps decision makers make informed choices. Ultimately, risk management can help with decisions on whether a risk is unacceptable and whether risk controls will be adequate and effective.

d) Risk management should explicitly address uncertainty.

Risk management deals with those aspects of decision making that are uncertain, the nature of that uncertainty, and how it may be treated.

e) Risk management should be systematic and structured.

Risk management approaches should ensure where practicable that the results are consistent, comparable and reliable.

f) Risk management should be based on the best available information.

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

g) Risk management should be tailored.

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

h) Risk management should take into account human factors.

The organization's risk management should recognize the capabilities, perceptions and intentions of external and internal people that may facilitate or hinder attainment of the organization's objectives.

i) Risk management should be transparent and inclusive.

Appropriate and timely involvement and inclusion of stakeholders and, in particular, decision makers at all levels of the organization, should ensure 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, stakeholders' perceptions and levels of tolerable risk.

j) Risk management should be dynamic, iterative and responsive to change.

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

k) Risk Management should be capable of continual improvement and enhancement.

Organizations should develop 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 and sustainable, risk management should be embedded in the organization and supported by management. A framework for managing risks aims to assist an organization to manage its risks effectively through the application of the risk management process at varying levels and within specific contexts of the organization. Such a framework should ensure that risk information derived from these processes is adequately reported and used as a basis for decision making at all relevant organizational levels.

This clause provides guidelines for designing, implementing, monitoring and improving a management framework within which the risk management process (see Clause 6) should be set and which should ensure that direction and implementation of the process are fully addressed.

The elements of the framework for managing risk are shown in Figure 2.

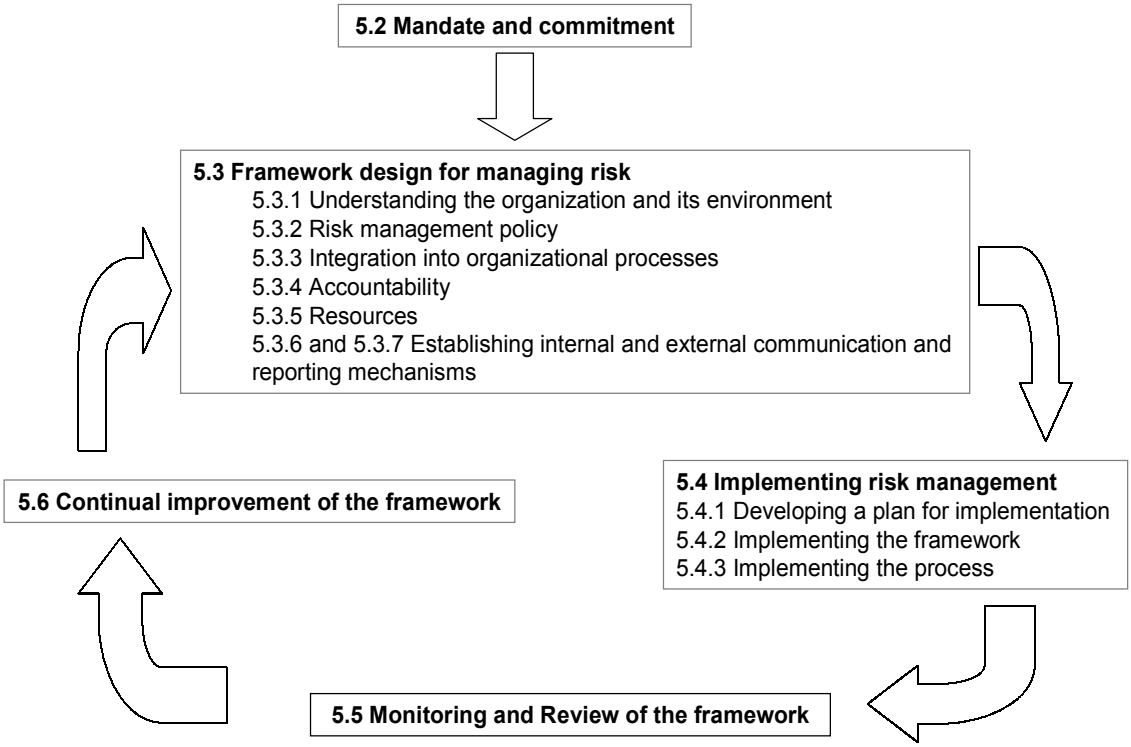


Figure 2 — Framework for managing risk

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 elements of the framework to their specific needs.

Many organizations' existing management practices and processes include elements of risk management and many organizations have already adopted a formal risk management process for particular types of risk or circumstances. These should be critically reviewed and assessed.

5.2 Mandate and commitment

Risk management requires strong and sustained commitment by management of the organization as well as strategic and rigorous planning. The management should:

— articulate and endorse the risk management policy;

— communicate the benefits of risk management to all stakeholders;

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

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

— ensure legal and regulatory compliance; and

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

5.3 Framework design for managing risk

5.3.1 Understanding the organization and its environment

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

Aspects of the organization's external environment that may be considered include the:

— cultural, political, legal, regulatory, financial, economic and competitive environment, whether international, national or regional;

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

— perceptions and values of external stakeholders.

It is also necessary to understand the organization in terms of, for example:

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

— information flows and decision making processes;

— internal stakeholders;

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

— perceptions, values and culture;

— policies and processes;

— 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 make clear the organization's objectives for and commitment to risk management and may specify the following:

— accountabilities and responsibilities for managing risk;

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

— links between this policy and the organization’s objectives;

— organization’s risk appetite;

— organization's rationale for managing risk;

— processes and methods to be used for managing risk;

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

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

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, efficient and sustained. In particular, risk management should be embedded into the policy development, business and strategic planning and change management processes.

5.3.4 Accountability

The organization should ensure that there is accountability and authority for managing risks, the adequacy and effectiveness of risk controls and the implementation as well as sustaining of the risk management process. This may be facilitated by:

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

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

— specifying risk owners or categories of risk for implementing risk treatment, maintenance of risk controls and internal reporting of relevant risk information; and

— specifying who is accountable for the development, implementation and maintenance of the framework for the management of risk.

5.3.5 Resources

The organization should develop the practical means by which it implements risk management including allocating appropriate resources for the risk management function.

Consideration should be given to the following:

— documented processes and procedures;

297 — information systems;

298 — people and skills; and

299 — resources needed for each step of the risk management process.

300 **5.3.6 Establishing internal communication and reporting mechanisms**

301 The organization should establish internal communication and reporting mechanisms to ensure that relevant
302 information derived from the application of risk management is available at appropriate levels in the
303 organization as a basis for decision making in support of the achievement of the organization's objectives.

304 These mechanisms should include processes to consolidate risk information where appropriate from a variety
305 of sources within the organization taking into account its sensitivity.

306 **5.3.7 Establishing external communication and reporting mechanisms**

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

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

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

311 — internal and external reporting due to legal, regulatory, and corporate governance requirements;

312 — internal reporting on the framework and its effectiveness and the outcomes;

313 — making disclosures as required by legalization;

314 — receiving feedback on communications; and

315 — using communication to provide transparency and build confidence in the organization.

316 **5.4 Implementing risk management**

317 **5.4.1 Developing a plan for implementation**

318 There should be an organization-wide plan for ensuring that the management of risk is embedded throughout
319 the organization, integrated with normal business practice, and maintained through monitoring and reviewing
320 of risks, controls, and changes in the internal and external environments.

321 **5.4.2 Implementing the framework for managing risk**

322 In implementing the organizations framework for managing risk, the organization should consider the
323 following:

324 — applying the risk management policy and process to the organizational processes according to its plan;

325 — communicating with stakeholders to ensure that its risk management framework remains appropriate;

326 — decision making, including the development and setting of objectives, aligned with the application of the
327 risk management process;

328 — designating a person accountable for implementation of the framework; and

329 — holding information and training sessions.

5.4.3 Implementing the 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 sustained, an organization should:

— periodically measure progress against 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 how well the risk management policy is being followed; and

— review the effectiveness of the risk management process including the adequacy of controls.

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, management culture. This will contribute to improvement in the organization's resilience, governance, and accountability.

6 Process for managing risk

6.1 General

The risk management process comprises the activities described from 6.2 to 6.7, and is shown in Figure 3.

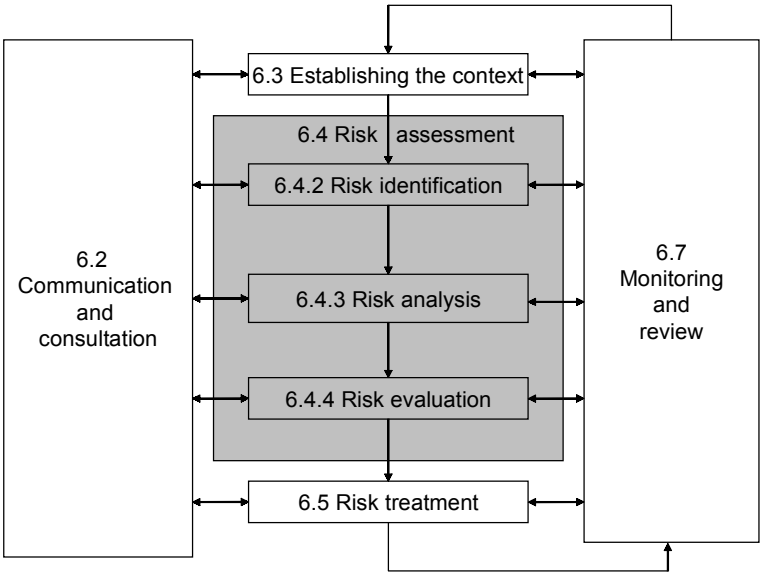


Figure 3 — Risk management process

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 be done to ensure that those accountable for implementing the risk management process and those with a vested interest, and thus a key contribution to make, understand the basis on which decisions are made, and the reason why particular actions are required to improve the organization's risk management culture.

A team approach is useful to:

— bring together different areas of expertise for analyzing risks;

— develop a communication plan;

— enhance appropriate change management during the risk management process;

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

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

— help define the context appropriately;

— help ensure that risks are adequately identified; and

— secure endorsement and support for a treatment plan.

Stakeholders may 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 perceptions are identified, recorded and taken into account in the decision making process.

The communication and consultation plan must be in accordance with the following:

— the communication and consultation should be an exchange and not a monolog of each stakeholder;

— the communication and consultation should convey messages which are honest and understandable and must not aim at manipulating but at convincing on basis of evidences; and

— the communication should be useful. The contribution of its use should be assessed.

6.3 Establishing the context

6.3.1 General

The risk management process should be aligned with the organization's culture, processes and structure.

Establishing the context defines the basic parameters for managing risk and sets the scope and criteria for the rest of the process. The context may 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 applying 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 anything outside the organization that may influence 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 risks management process.

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

- cultural, political, legal, regulatory, financial, economic and competitive environment, whether international, national or regional;
- 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 anything within the organization that may influence the way in which an organization will manage risk. It should be established because:

- a major risk for some organizations is failure to achieve their strategic, project or business objectives, and this risk affects ongoing organizational commitment, credibility, and value;
- objectives and criteria of a particular project or activity should be considered in the light of objectives of the organization as a whole; and
- risk management takes place in the context of the objectives of the organization.

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

- capabilities, understood in terms of resources and knowledge (e.g. capital, people, competencies, processes, systems and technologies);
- information flows and decision making processes;
- internal stakeholders;
- objectives, and the strategies that are in place to achieve them;
- perceptions, values and culture;
- policies and processes;
- standards and reference models adopted by the organization; and
- structures (e.g. governance, roles and accountabilities).

6.3.4 Establishing the risk management process context

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 may involve, but is not limited to:

— defining responsibilities;

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

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

— defining the project, process, function, activity and its goals 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, 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 and proportionate 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 the criteria against which risk is to be evaluated based on the context. Risk criteria express the organization's values, objectives and resources. Some criteria may be imposed by, or derived from, legal and regulatory requirements. 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 reviewed.

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

— how likelihood will be defined;

— how the level of risk is to be determined;

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

— the level at which risk becomes acceptable;

— the time frame of the likelihood and/or consequence;

— what level of risk may require 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

Risk identification seeks to identify the risks that are relevant to the objectives as established in 6.3.4. The organization should identify sources of risk, events or sets of circumstances, and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events and circumstances that might enhance, prevent, degrade or delay the achievement of the objectives. Comprehensive identification and recording is critical, because a risk that is not identified at this stage is excluded from further analysis. Identification should include risks whether or not they are under the control of the organization.

The organization should apply a set of risk identification tools and techniques which are suited to its objectives and capabilities, and to the risk the organization faces.

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 may occur. All significant causes should be considered.

In identifying the risks, it is also important to consider the risks associated with not pursuing an opportunity.

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 the most appropriate risk treatment strategies.

Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences may occur. Factors that affect consequences and likelihood may be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event or set of circumstances may have multiple consequences and may affect multiple objectives. Existing risk controls and their effectiveness should be taken into account.

The way in which likelihood and consequences are expressed and the way in which they are combined to estimate a level of risk will vary according to the type of risk 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 estimates 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 required. Factors such as divergence of opinion amongst experts or limitations on modelling should be stated and may need to be highlighted.

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

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

6.4.4 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 treatment priorities

Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered

The objectives of the organization and the extent of opportunity that could result should be considered. Where a choice is to be made between options, this will depend on an organization's context.

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 benefit from it. Decisions need to take into account constraints imposed by laws and other requirements.

If the level of risk does not meet risk criteria, the risk should be treated

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

6.5 Risk treatment

6.5.1 General

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

Risk treatment may involve a cyclical process of assessing a risk treatment, deciding that residual risk levels are not tolerable, generating a new risk treatment, and assessing the effect of that treatment until a level of residual risk is reached which is one within which the organization can tolerate based on the risk criteria.

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

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

b) seeking an opportunity by deciding to start or continue with an activity likely to create or maintain the risk;

c) changing the likelihood;

d) changing the consequences;

e) sharing the risk with another party or parties; and

f) retaining the risk, either by choice or by default.

6.5.2 Selection of risk treatment options

Selecting the most appropriate risk treatment option involves balancing the costs and effort of implementation against the benefits derived.

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

Decisions should take into account rare but severe risks that may warrant risk treatment actions that are not justifiable on strictly economic grounds. Legal and regulatory requirements and social responsibility override financial cost benefit analysis.

Risk treatment options should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them. Where risk treatment options may impact on risk elsewhere in the organization, these areas should be involved in the decision. Though equally effective, some risk treatments may 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. Full cost of not taking action should be compared against the budgetary saving.

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

Risk treatment might 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 may 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 record how the chosen treatment options will be implemented. The information provided in treatment plans may 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.

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

6.6 Recording the risk management process

Risk management activities should be traceable. In the risk management process, records provide the foundation for improvement in methods, 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 effort involved in creating and maintaining records;

— legal, regulatory, and operational needs for records;

— method of access, retrievability and storage media;

571 — retention period; and

572 — sensitivity of information.

573 ## 6.7 Monitoring and review

574 Monitoring and review is concerned with:

575 — analyzing and learning lessons from events, changes and trends;

576 — detecting changes in the external and internal context including changes to the risk itself which may
577 require revision of risk treatments and priorities; and

578 — ensuring that the risk control and treatment measures are effective in both design and operation.

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

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

584 It is not sufficient to rely only on occasional reviews and audits.

585 The results of monitoring and review should be recorded and internally or externally reported as appropriate
586 and may also be used as an input to the review of the risk management framework (see Clause 5).

587 Responsibilities for monitoring and review should be clearly defined.

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 programmes to maximise their opportunities and to control their threats.

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

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 in 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 systems, 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, database or information system. 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 fulfil that role by providing them with the authority, time, 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 elements 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 and highly visible, comprehensive and frequent internal and external reporting of risk management performance to all stakeholders as part of a governance process.

This is indicated by communication with interested parties as being clearly regarded as an integral and essential component of risk management so that communication takes place as part of each part 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.

Highly visible, comprehensive and frequent internal and external reporting of both significant risks to the organization and of risk management performance contributes substantially to effective governance within the 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 founded 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.