TECHNICAL REPORT

ISO/TR 31004

First edition
2013-10-15

Risk management — Guidance for the implementation of ISO 31000

Management du risque — Lignes directrices pour l'implementation de l'ISO 31000

Reference number
ISO/TR 31004:2013(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is Technical Committee ISO/TC 262, *Risk management*.

Introduction

0.1 General

Organizations use various methods to manage the effect of uncertainty on their objectives, i.e. to manage risk, by detecting and understanding risk, and modifying it where necessary.

This Technical Report is intended to assist organizations to enhance the effectiveness of their risk management efforts by aligning them with ISO 31000:2009. ISO 31000 provides a generic risk management approach that can be applied to all organizations to help achieve their objectives.

This Technical Report is intended to be used by those within organizations who make decisions that impact on achieving its objectives, including those responsible for governance and those who provide organizations with risk management advice and support services. This Technical Report is also intended to be used by anyone interested in risk and its management, including teachers, students, legislators and regulators.

This Technical Report is intended to be read in conjunction with ISO 31000 and is applicable to all types and sizes of organization. The core concepts and definitions that are central to understanding ISO 31000 are explained in Annex A.

Clause 3 provides a generic methodology to help organizations transition existing risk management arrangements to align with ISO 31000, in a planned and structured way. It also provides for dynamic adjustment as changes occur in the internal and external environment of the organization.

Additional annexes provide advice, examples and explanation regarding the implementation of selected aspects of ISO 31000, in order to assist readers according to their individual expertise and needs.

Examples provided in this Technical Report might or might not be directly applicable to particular situations or organizations, and are for illustrative purposes only.

0.2 Underlying concepts and principles

Certain words and concepts are fundamental to understanding both ISO 31000 and this Technical Report, and they are explained in ISO 31000:2009, Clause 2, and in Annex A.

ISO 31000 lists eleven principles for effective risk management. The role of the principles is to inform and guide all aspects of the organization's approach to risk management. Principles describe the characteristics of effective risk management. Rather than simply implementing the principles, it is important that the organization reflects them in all aspects of management. They serve as indicators of risk management performance and reinforce the value to the organization of managing risk effectively. They also influence all elements of the transition process described in this Technical Report, and the technical issues that are the subject of its annexes. Further advice is given in Annex B.

In this Technical Report, the expressions "top management" and "oversight body" are both used: "top management" refers to the person or group of people that directs and controls an organization at the highest level, whereas "oversight body" refers to the person or group of people that governs an organization, sets directions, and holds top management to account.

NOTE In many organizations, the oversight body could be called a board of directors, a board of trustees, a supervisory board, etc.

Risk management — Guidance for the implementation of ISO 31000

1 Scope

This Technical Report provides guidance for organizations on managing risk effectively by implementing ISO 31000:2009. It provides:

— a structured approach for organizations to transition their risk management arrangements in order to be consistent with ISO 31000, in a manner tailored to the characteristics of the organization;

— an explanation of the underlying concepts of ISO 31000;

— guidance on aspects of the principles and risk management framework that are described in ISO 31000.

This Technical Report can be used by any public, private or community enterprise, association, group or individual.

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

This Technical Report is not specific to any industry or sector, or to any particular type of risk, and can be applied to all activities and to all parts of organizations.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 31000:2009, *Risk management — Principles and guidelines*

3 Implementing ISO 31000

3.1 General

This clause provides guidance to organizations seeking to align their risk management approach and practices with ISO 31000 and to maintain those practices in alignment on an ongoing basis.

It provides a general methodology that is suitable for application, in a planned manner, by any organization irrespective of the nature of its current risk management arrangements. This methodology involves the following:

— comparing current practice with that described in ISO 31000;

— identifying what needs to change and preparing and implementing a plan for doing so;

— maintaining ongoing monitoring and review to ensure currency and continuous improvement.

This will enable the organization to obtain a current and comprehensive understanding of its risks, and to ensure that those risks are consistent with its attitude to risk and its risk criteria.

Regardless of the motive for implementing ISO 31000, doing so is expected to enable an organization to better manage its risks, in support of its objectives. All organizations manage risk to some extent. The strategy for implementing ISO 31000 should recognize how an organization is already managing risk.

The implementation process, as described in 3.2, will evaluate existing arrangements and, if necessary, adapt and modify to align with ISO 31000.

ISO 31000 identifies various elements of a risk management framework. There are several advantages that can arise when elements of that framework are integrated into an organization's governance, functions and processes. These relate to organizational effectiveness, sound decision making and efficiency.

a) The framework for managing risk should be realized by integrating its components into the organization's overall system of management and decision making, irrespective of whether the system is formal or informal; existing management processes may be improved by reference to ISO 31000.

b) The understanding and management of uncertainty becomes an integral component in the management system(s), establishing a common approach for the organization.

c) Implementation of the risk management process can be proportionately tailored to the size and requirements of the organization.

d) The governance (i.e. direction and oversight) of the risk management policy, framework and process(s) can be integrated into existing organizational governance arrangements.

e) Risk management reporting is integrated with other management reporting.

f) Risk management performance becomes an integral part of the overall performance approach.

g) Interaction and connection between the often separate risk management fields of an organization (e.g. enterprise risk management, financial risk management, project risk management, safety and security management, business continuity management, insurance management) can be ensured or improved, as the attention will now be primarily be focused on setting and achieving the organization's objectives, taking risk into account.

h) The communication on uncertainty and risk between management teams and management levels is improved.

i) Silos of risk management activity within an organization centre on the achievement of organizational objectives as a common focus. There may be indirect societal benefits as the organization's external stakeholders may be motivated to improve their respective risk management activity.

j) The risk treatment and controls can become an integral part of daily operations.

3.2 How to implement ISO 31000

Although ISO 31000 explains how to manage risk effectively, it does not explain how to integrate risk management into the organization's management processes. Even though organizations are different and their starting points may differ, a generic and systematic implementation approach is applicable in all cases.

The organization should determine whether changes are needed to its existing framework for the management of risk, before planning and implementing those changes, and then monitoring the ongoing effectiveness of the amended framework. This will allow the organization:

— to align its risk management activities with the principles for effective risk management described in ISO 31000:2009, Clause 3;

— to apply the risk management process described in ISO 31000:2009, Clause 5;

— to satisfy the attributes of enhanced risk management in ISO 31000:2009, Clause A.3;

— thereby to achieve the key outcomes in ISO 31000:2009, Clause A.2.

This approach is also applicable to organizations that are already consistent with ISO 31000, but that wish to continually improve their framework and the process for managing risk as recommended in ISO 31000:2009, 4.6 and 5.6.

All aspects of transition may be helped by drawing on the experience of other organizations which manage similar types of risks or have gone through a similar process.

3.3 Integration of ISO 31000 into the organization's management processes

3.3.1 General

ISO 31000 provides a framework and a generic process to manage risk in all or part of any type of organization. This subclause provides guidance for integrating the elements of ISO 31000 into an organization's management approach, including its activities, processes and functions. Organizations may choose to integrate ISO 31000 concepts with their existing processes, or they may choose to design and establish a new approach based on ISO 31000. This subclause describes the core elements of the framework and process, and the actions necessary for successful integration of these elements to meet its organizational objectives. There are many ways to integrate ISO 31000 into an organization. The choice and order of elements should be tailored to the needs of the organization and its stakeholders. Care should be taken when applying this guidance to ensure that integration supports the overall business management strategy. This drives the effort to meet the organization's objectives of protection and creation of value. The approach also needs to consider the organization's culture, as well as project and change management methodologies.

This subclause describes the core elements of the framework and process, and the actions necessary for successful integration of these elements to meet its organizational objectives.

Implementing ISO 31000 is a dynamic and iterative ongoing process. Furthermore, implementation of the framework is interconnected with the risk management process described in ISO 31000:2009, Clause 5. Success is measured both in terms of the integration of the framework and in terms of the continual improvement of risk management throughout the organization.

Integration takes place within a dynamic context. The organization should monitor both changes that are brought about by the implementation process and changes to its internal and external context. This may include the need for change to its risk criteria.

3.3.2 Mandate and commitment

Any business management activity begins with an analysis of the rationale and steps of the processes and a cost-benefit analysis. This is followed by a decision by top management and the oversight body to implement and to provide the necessary commitment and resources.

Typically, the implementation process includes the following:

a) acquiring mandate and commitment, if required;

b) a gap analysis;

c) tailoring and scale based on organizational needs, culture and creating and protecting value;

d) evaluating risks associated with transition;

e) developing a business plan:

   — setting objectives, priorities and metrics;

   — establishing the business case, including alignment with organizational objectives;

   — determining scope, accountabilities, timeframe and resources;

f) identifying the context of implementation, including communication with stakeholders.

3.3.3 Designing the framework

3.3.3.1 Existing approaches to risk management in the current organization should be evaluated, including context and culture.

a) It is important to consider any legal, regulatory or customer obligations and certification requirements that arise from any management systems and standards that the organization has chosen to adopt. The purpose of this step is to permit careful tailoring of the design of the risk management framework and the implementation plan itself, and to permit alignment with the structure, culture and general system of management of the organization.

b) It is important to consider both the process used to manage risks and the aspects of the existing risk management framework that enable this process to be applied.

c) Appropriate risk criteria should be established. Risk criteria need to be consistent with the objectives of the organization and aligned with its risk attitude. If the objectives change, the risk criteria need to be adjusted accordingly. It is important for effective risk management that the risk criteria are developed to reflect the organization's risk attitude and objectives.

For designing the new framework, specifically, the following should be evaluated:

— principles and attributes, as described in ISO 31000;

— the previous framework, the evaluation of which should compare in particular the current practices with the requirements of the following subclauses of ISO 31000:2009:

  — 4.3.2 (risk management policy);

  — 4.3.3 (accountability);

  — 4.3.4 (integration into organizational processes);

  — 4.3.5 (resources);

  — 4.3.6 and 4.3.7 (internal and external communication and reporting mechanisms);

— the process, the evaluation of which should compare the elements of the existing processes against those in ISO 31000:2009, Clause 5, as well as the underlying principles that drive and provide the rationale for the process with the principles set out in ISO 31000:2009, Clause 3 (e.g. whether this process is actually applied to decision making at all levels):

  — evaluate whether the current process provides decision makers with the risk information they need to make quality decisions and meet or exceed objectives;

  — evaluate whether the existing approaches for managing risk sufficiently address interrelated risks and risks that occur in multiple locations.

3.3.3.2 Framework design requirements should be identified.

On the basis of the evaluations described in 3.3.3.1, the organization should decide which aspects of the current risk management approach:

a) could continue to be used in future (possibly extended to other types of decision making);

b) need amendment or enhancement;

c) no longer add value and should be discontinued.

The organization should develop, document and communicate how it will be managing risk. The scale and content of the organization's internal standards, guidelines and models related to risk management should reflect organizational culture and context.

The documents can specify that:

— risks are managed throughout the organization using consistent approaches;

— there are different levels of accountability for managing risk;

— the competencies and duties of all persons with risk management accountabilities are clearly defined;

— both internal and external stakeholders are involved, as appropriate, through comprehensive communication and consultation;

— information about risks and the output from all applications of the risk management process are recorded in a consistent and secure manner, with appropriate access.

There should also be provision for periodic review of organizational requirements, tools, training and resources for the management of risk, if there are subsequent changes in the organization and its context, or if ongoing monitoring and review identifies weaknesses or inefficiencies.

3.3.3.3 The scope, objectives, targets, resources, measures for success and monitoring and review criteria for the implementation phase should be defined.

3.3.3.4 Internal and external communication and reporting mechanisms should be established.

3.3.4 Implementing risk management

A detailed implementation plan is needed to ensure that the necessary changes occur in a coherent order and that the necessary resources can be provided and applied. The plan should be supported by the resources required for its implementation, and this may require specific budget allocations, the development of which should be part of the planning process.

The plan itself should be subject to risk assessment in accordance with ISO 31000:2009, 5.4, and any necessary risk treatment actions implemented.

The plan should both require and allow progress to be tracked and reported to top management and the oversight body, and there should be provision for periodic reviews of the plan.

The plan should therefore:

— detail the specific actions to be taken, their sequence, by whom, and the timeframe for completion: these will include amending the internal standards and guidelines, explaining and training to build capability, and making adjustments in accountabilities;

— identify any actions that will be implemented as part of some wider actions associated with organizational development, or which are otherwise linked (e.g. development of training material and engagement of trainers);

— define responsibilities for implementation;

— incorporate a mechanism for reporting completion, progress and problems;

— identify and record any criteria that will trigger a review of the plan.

The implementation may take some time to complete and can be done in stages. The usual practice of giving priority wherever possible to those changes that have the biggest impact on achieving the end-purpose should be adopted. This implementation can occur at various stages of organizational maturity and structure. It may also be more effective to integrate implementation with other change programmes.

3.3.5 Monitor and review

Progress against the plan should be tracked, analysed and reported to top management on a timely basis (monthly, quarterly, etc.).

Reports of progress against the plan, and performance against measures, should be validated periodically in an unbiased, objective review process. Reviews should include examination of framework, processes, the risks themselves and change to the environment.

There should be a periodical review of the strategy for implementation, and measurement of the progress, consistency with and deviation from the risk management plan. Reviews may also occur if the review criteria set out in the plan are triggered.

Performance should be evaluated with regard to the effectiveness of change and managing risk, as well as to identify lessons learned and opportunities for improvement.

The significant issues from the monitoring should be reported to those who are accountable.

The results of this step will be fed back into the context and other functions, so that new risks can be identified, changes to existing risks can be discovered, and the execution status of the framework can be recorded for improvement (see ISO 31000:2009, 4.6 and 5.7).

3.4 Continual improvement

Both the risk management framework and the risk management process should be reviewed to assess whether their design is appropriate and whether their implementation is adding value to the organization as intended. If the results of monitoring and review show that improvement can be made, these should be implemented as soon as possible.

For organizations that have transitioned to ISO 31000, there should be a constant awareness and uptake of the opportunity for improvement. The same steps as used in the transition process are also useful for making periodic checks of whether there has been deviation from the process.

There are various triggers for continual improvement, including the following:

— routine monitoring and review of the risk management framework and the risk management process, which identify opportunities to improve;

— new knowledge becoming available;

— a substantive change to the organization's internal and external context.

Annex A
(informative)

Underlying concepts and principles

A.1 General

This annex explains certain words and concepts (e.g. "risk") that are in everyday use and can have several meanings, but that have a particular meaning in both ISO 31000 and this Technical Report.

ISO 31000 defines risk as the "effect of uncertainty on objectives".

NOTE It is advisable that readers familiarize themselves with the terms and definitions in this annex.

A.2 Risk and objectives

Organizations of all kinds face internal and external factors and influences that make it uncertain whether, when and the extent to which, they will achieve or exceed their objectives. The effect that this uncertainty has on the organization's objectives is risk.

The objectives referred to in ISO 31000 and this Technical Report are the outcomes that the organization is seeking. Typically, these are its highest expression of intent and purpose, and they typically reflect its explicit and implicit goals, values and imperatives, including consideration of social obligations and legal and regulatory requirements. In general, risk management is facilitated if objectives are expressed in measurable terms. There are often multiple objectives, however, and inconsistency between objectives can be a source of risk.

Likelihood is not just that of an event occurring, but the overall likelihood of experiencing the consequences that flow from the event, and the magnitude of the consequence in either positive or negative terms. Typically, there can be a range of possible consequences that can flow from an event, and each will have its own likelihood. The level of risk can be expressed as the likelihood that particular consequences will be experienced (including the magnitude). Consequences relate directly to objectives and they arise when something does or does not happen.

Risk is the effect of uncertainty on objectives, regardless of the domain or circumstances, therefore an event or a hazard (or any other risk source) should not be described as a risk. Risk should be described as the combination of the likelihood of an event (or hazard or source of risk) and its consequence.

The understanding that risk can have positive or negative consequences is a central and vital concept to be understood by management. Risk can expose the organization to either an opportunity, a threat or both.

Risk is created or altered when decisions are made. Because there is almost always some uncertainty associated with decisions and decision making, there is almost always risk. Those responsible for achieving objectives need to appreciate that risk is an unavoidable part of the organization's activities that is typically created or altered when decisions are made. Risks associated with a decision should be understood at the time the decision is made, and risk-taking is therefore intentional. Using the risk management process described in ISO 31000 makes this possible.

A.3 Uncertainty

The uncertainty which, together with the objectives, gives rise to risk originates in the internal and external environment in which the organization operates. This can be uncertainty that:

— is a consequence of underlying sociological, psychological and cultural factors associated with human behaviour;

— is produced by natural processes that are characterized by inherent variability, e.g. in weather, variation between observations in a population;

— arises from incomplete or inaccurate information, e.g. due to missing, misinterpreted, unreliable, internally contradictory or inaccessible data;

— changes over time, e.g. due to competition, trends, new information, changes in underlying factors;

— is produced by the perception of uncertainty which may vary between parts of the organization and its stakeholders.

A.4 Risk treatment and control

Controls are measures implemented by organizations to modify risk that enable the achievement of objectives. Controls can modify risk by changing any source of uncertainty (e.g. by making it more or less likely that something will occur) or by changing the range of possible consequences and where they may occur.

Risk treatment, as defined in ISO 31000, is the process that is intended to change or create controls, and includes retaining the risk.

A.5 Risk management framework

The risk management framework refers to the arrangements (including practices, processes, systems, resources and culture) within the organization's system of management that enable risk to be managed. The characteristics of a framework, and the extent to which it is integrated in the organization's system of management, will ultimately determine how effectively risk is managed.

The framework includes clear statements from top management on the organization's intent regarding risk management (described in ISO 31000 as mandate and commitment) and the necessary capacity (resources and capability) to achieve this intent.

This capacity does not exist as a single system or entity. This capacity comprises numerous elements integrated into the organization's overall management processes. They can either be unique to the task of managing risk (e.g. a specialized information system), or be aspects of the organization's system for management (e.g. its human resource practices).

A.6 Risk criteria

Risk criteria are the parameters established by the organization to allow it to describe risk and make decisions about the significance of risk that take account of the organization's attitude to risk. These decisions enable risk to be assessed and treatment to be selected.

A.7 Management, risk management and managing risk

Management involves coordinated activities that direct and control an organization in pursuit of its objectives.

Risk management is an integral component of management, as it involves coordinated activities concerned with the effect of uncertainty on those objectives. That is why, in order to be effective, it is important that risk management is fully integrated into the organization's management system and processes.

In this Technical Report, as in ISO 31000, the expression “risk management” generally refers to the architecture that organizations use (principles, framework and process) for managing risk effectively, and “managing risk” refers to applying that architecture to particular decisions, activities and risks.

Annex B
(informative)

Application of ISO 31000 principles

B.1 General

While all organizations manage risk to some degree, ISO 31000:2009 establishes eleven principles that need to be satisfied to make risk management effective. The principles provide guidance on the following:

a) the rationale for managing risk effectively (e.g. risk management creates and protects value);

b) the characteristics of risk management that enable risk management to be effective, e.g. Principle b), which specifies that risk management is an integral part of all organizational processes.

In ISO 31000, each principle is summarized in a few words by its heading, with the supporting text providing explanation and detail.

All eleven principles should be considered when designing the organization's risk management objectives, however, the significance of individual principles may vary according to the part of the framework under consideration and tailored to their specific application.

The successful implementation of these principles will determine both the effectiveness and efficiency of risk management in the organization. All eleven principles should be kept in mind at all times, even though the significance of individual principles may vary according to the part of the framework under consideration.

Although the principles are expressed succinctly, the implications of each needs to be thoroughly understood in order to give effect to them on a continuing basis.

Afterwards, the results of this kind of analysis should be reflected in the design or enhancement of the framework (e.g. in the allocation of accountabilities, provision of training, communication with stakeholders and the design of ongoing monitoring and review of risk management performance).

This annex provides guidance on how to apply each principle and in addition, for some principles, there are also practical help boxes.

B.2 The principles

B.2.1 Risk management creates and protects value

B.2.1.1 Principle

a) Risk management creates and protects value.

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

B.2.1.2 How to apply the principle

This principle explains that the purpose of risk management is to create and protect value by helping an organization achieve its objectives. It does this by helping the organization to identify and tackle the factors, both internal or external to an organization, that give rise to uncertainty associated with its objectives.

The linkage between the effectiveness of risk management and how it contributes to the success of the organization should be clearly demonstrated and communicated. The principle clarifies that risk should not be managed for its own sake, but so that objectives are achieved and performance enhanced.

Some attributes and values cannot be easily directly measured (e.g. in terms of money), but they also contribute strongly to performance, reputation and legal compliance. Human, social and ecological values are particularly important in managing safety, security and compliance related risks, as well as those associated with intangible assets, therefore value creation may need to be expressed using qualitative descriptors rather than quantitative measures.

B.2.2 Risk management is an integral part of all organizational processes

B.2.2.1 Principle

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

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

B.2.2.2 How to apply the principle

The activities of an organization, including the decisions it makes, give rise to risk. Changes in the external context that are beyond the organization's control and influence can also give rise to new risks. All of the organization's activities and processes take place in an internal and external environment, in which there is uncertainty. It follows that:

a) the framework for managing risk should be realized by integrating its components into the organization's overall system of management and decision making, irrespective of whether the system is formal or informal; existing management processes may be improved by reference to ISO 31000;

b) the process to manage risk should be an integral part of the activities that generate risk; otherwise, the organization will find it needs to modify decisions later when associated risks are subsequently understood;

c) if a formal management system does not exist, a risk management framework can serve this purpose.

If risk management is not integrated into other management activities and processes, it can be perceived as an additional administrative task, or viewed as a bureaucratic exercise that does not create or protect value.

The two main methods of applying the principle are as follows:

— in the development (including maintenance and improvement) of the risk management framework;

— in the application of the risk management process to decision making and related activities.

The method of expressing the organization's intent (i.e. mandate and commitment) about risk management should be similar to the way that it expresses its other intentions (see Annex C). Wherever possible, other components of the risk management framework should be embedded into components of existing management systems (further advice is provided in Annex E and in ISO 31000).

Auditing bodies can also play an important role, by questioning how management has arrived at a decision and testing whether this involved a suitable application of the risk management process.

B.2.3 Risk management is part of decision making

B.2.3.1 Principle

c) Risk management is part of decision making.

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

B.2.3.2 How to apply the principle

This principle states that risk management provides the foundation for informed decision making. Risk management should be integrated into activities supporting the achievement of objectives and the decision-making process. The decision-making process should consistently assess and, where necessary, treat risk. Taking or not taking decisions involves risk, and it is important to have an understanding of the associated risks in both situations.

Risk management should be applied as part of a decision, and at the time the decision is made (i.e. proactively), not after the decision has been made (i.e. reactively), e.g. as follows:

— decisions on strategic issues should take into consideration uncertainties concerning changes in environmental factors, as well as changes in the organization's resources;

— the innovation process should take into consideration not only the uncertainty which determines the success of the innovation, but also risks relating to human, social, safety and environmental aspects of the innovation, and treated according to legal requirements (e.g. product safety);

— plans for large investments should specify the decision-making milestones at which risk assessment will occur.

The organization's policy about risk management and the way it is communicated should reflect this principle.

The other parts of the framework should take into account the way that decisions are made, so that the process is applied in an effective and consistent way in all decision making, e.g. project management, investment appraisal, procurement.

Those responsible for decision making throughout the organization should understand the organization's risk management policy and should be specifically required to have competencies to apply the risk management process to decision making. This will require clear allocation of accountability, supported by skills training and performance review.

Practical help

In order to give effect to the principle, the following questions should be considered carefully from the start:

— How can this help create and protect value? [Principle a)]

— How and where in the organization are decisions made?

— Who is involved in decision making?

— What knowledge and skill is needed for those who make decisions to make risk management a part of their decision making?

— How will decision makers acquire the knowledge and skill they need?

— What direction and support are needed for existing staff?

— How will future staff be inducted to this method of decision making?

— How will external stakeholders be affected?

— What decision-making processes in the organization would need to change?

— How would progress in applying this principle be monitored?

B.2.4 Risk management explicitly addresses uncertainty

B.2.4.1 Principle

d) Risk management explicitly addresses uncertainty.

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

B.2.4.2 How to apply the principle

What makes risk management unique among other types of management is that it specifically addresses the effect of uncertainty on objectives. Risk can only be assessed or successfully treated if the nature and source of that uncertainty are understood.

Uncertainty of all types requires consideration, and care is needed not to overestimate or underestimate it.

Focus on uncertainty is also important when selecting risk treatments and considering the effect and reliability of controls. Similarly, there will be uncertainties associated with the supporting steps of the risk management process, e.g. whether information has been successfully conveyed when communicating and consulting with stakeholders, or whether the selected intervals for monitoring processes are sufficient to detect change.

Those involved in managing risk should have a sound grasp of the significance of uncertainty, and the types and sources of uncertainty. The number and types of risk assessment methods used to address uncertainty should be appropriate and relevant to the significance of the decision: multiple methods may be warranted.

Record assumptions when recording the risk management process (ISO 31000:2009, 5.7). Assumptions generally reflect some form of uncertainty, as well as any explicit uncertainties that have been factored into the various steps of the process.

When risk is being assessed, it is important to consider the uncertainty associated with estimating the ratings for likelihood and consequence.

When analysing risk and proposing treatments, sensitivity studies should be used to understand the actual influence of those uncertainties.

Practical help

— Decision makers should adopt the practice of always asking "What are the assumptions here?" and "What are the uncertainties associated with the assumptions?". This practice need not be limited to formal risk assessments, e.g. it could apply to all forecasts.

— When considering the internal and external environment as a part of establishing the context, any features likely to be associated with high volatility should be noted. This is a source of uncertainty and also informs the way in which the context is monitored and reviewed on an ongoing basis.

— If uncertainty signifies that a particular value is known only to exist within a certain range, that range should be communicated.

B.2.5 Risk management is systematic, structured and timely

B.2.5.1 Principle

e) Risk management is systematic, structured and timely.

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

B.2.5.2 How to apply the principle

A consistent approach to managing risk at the time decisions are made will create efficiencies in an organization, and can provide results that build confidence and success. This requires organizational practices that consider the risks associated with all decisions, and the use of consistent risk criteria that relate to the organizations objectives and the scope of its activities.

A timely approach signifies that the risk management process is applied at the optimum point in the decision-making process. In part, this depends on the design of the framework, to which this principle also applies. If the risk considerations are made too early or too late, either opportunities could be lost or there could be substantial costs of revising the decision. Time dependencies should be assessed and understood to determine the most effective risk management approach.

A structured approach signifies application of the risk management process in the manner described in ISO 31000:2009, Clause 5, including making appropriate preparations for these activities. Depending on needs, the method should be consistent with either a top-down or bottom-up approach, in order to address the appropriate level of management.

B.2.6 Risk management is based on the best available information

B.2.6.1 Principle

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

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

B.2.6.2 How to apply the principle

It is important to obtain the best available information in order to have a correct understanding of any risk. Consequently, risk management arrangements should include methods (e.g. research) to collect or generate information. However, despite best efforts, the information available may sometimes be limited, e.g. anticipating what will happen in the future may be limited to use of statistical projections.

The sensitivity of decisions to any uncertainties in the information should be understood. The reliability of risk evaluation will depend, in part, on the clarity and precision of the risk criteria. Collecting risk-related data (e.g. the occurrence of incidents and other experienced-based information) can assist statistical predications.

Although evidence-based decision making is the ultimate goal, this may not always be possible in the time or with the resources available. In such situations, expert judgement should be used, combined with the information that is available. However, care is needed to avoid group bias when applying such judgement. In addition, the evidence of the past may not accurately predict the future. In situations involving the potential for very high consequence events, the absence of information may prompt action if there is evidence of potential harm, rather than definitive proof of harm.

This principle is also applicable to the design (or improvement) of the risk management framework because there will be aspects of the framework (e.g. those that provide research capability or that collect, analyse, update and make available information to support application of the process) which will determine how well this principle is applied.

The reliability and accuracy of information should be regularly evaluated for relevancy, timeliness and dependability, with assumptions documented. The framework should provide for periodic review, and for the issue of updates or corrections.

Practical help

— When designing how incidents should be reported, there should first be careful consideration of which decisions this information could help, i.e. who the present and future end users are, how the information may be needed to sorted, how its integrity can be enhanced, and how it can be accessed. Once this has been done, the reporting form can be designed, keeping in mind that the quality supplied may be influenced by the time needed to input it.

— A description of the context (including the date it was written) should be included as part of the detailed and documented descriptions of the key risks faced (e.g. risk register). This allows users of the register to take account of any changes in context that may have occurred subsequently, with resulting changes in risk.

— Where assumptions have been made in an assessment, the rationale for those assumptions, including any limitations, should be clearly recorded and understood.

— When designing risk treatments, there should be consideration of how the performance of the resulting controls will be monitored and made available to future decision makers, who may be relying on those controls.

B.2.7 Risk management is tailored

B.2.7.1 Principle

g) Risk management is tailored.

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

B.2.7.2 How to apply the principle

ISO 31000 provides a generic approach to risk management that is applicable to all types of organizations and all types of risk. All organizations have their own culture and characteristics, risk criteria and contexts of operation. Risk management should be tailored to meet the needs of each organization.

There is no single, correct way to design and implement the risk management framework and processes, as they require flexibility and adaptation in every organization. Design can be determined by many aspects, including organizational size, culture, sector, configuration and management style.

Different areas of risk may require different tailored processes within the same organization. While all processes should be consistent with ISO 31000, there will be differences in the systems, models and level of judgment involved, e.g. between those involved in assessing information technology-related risks, treasury and investment risks, or competitor risks. Each process should be tailored to its specific purpose.

Since the purpose of the framework is to ensure that the risk management process will be applied to decision making in a way that is effective and reflects the policy, the design of the framework should reflect where and how decisions are taken, and should take into account any legislative or other external obligations to which the organization is committed.

It is important to keep in mind that tailoring does not imply that either the elements of the framework (as described in ISO 31000:2009, Clause 4) or the steps of the process (see ISO 31000:2009, Clause 5) should be varied. All are essential to the effective management of risk.

This principle is important during the design and improvement of the risk management framework, but it will also be relevant in the way that aspects of the process are structured.

This principle can also signify that the organization needs to consider internal issues, e.g. staff turnover (which, if quite high, may require appropriate adjustments to the scope of induction training, in order to ensure that all new employees are able to fulfil what is required of them regarding risk management).

Tailoring of the framework is necessary to achieve integration with the organization's decision-making processes. It is also possible that those decision-making processes will need to be modified to fit a structured risk management framework.

Practical help

— The design of the risk management framework should include seeking and taking account of the views of those who will be involved in its implementation.

— Building a deeper understanding of the underlying concepts of ISO 31000 will help ensure that tailoring both the framework and process will achieve the attributes of effective risk management, as listed in ISO 31000:2009, Annex A. Conversely, just ticking boxes will not achieve this.

B.2.8 Risk management takes human and cultural factors into account

B.2.8.1 Principle

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

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

B.2.8.2 How to apply the principle

This principle involves obtaining the views of stakeholders, as well as understanding that those views may be influenced by human and cultural characteristics. Factors to consider include social, political, and cultural, as well as concepts of time. Common types of error include the following:

a) failure to detect and respond to early warnings;

b) indifference to the views of others or to a lack of knowledge;

c) bias due to simplified information processing strategies to address complex issues;

d) failure to recognize complexity.

When designing the framework and when applying all aspects of the risk management process, specific actions are needed in order to understand and apply such human and cultural factors.

The design of the framework and communication about risk should take into account the cultural characteristics and levels of knowledge of the audience.

Practical help

— Managers should act in such a manner as to show that they promote and support respect and understanding of individual differences.

— People appreciate being asked their views.

— As a general rule, organizations reward what they value. If employee selection, promotion and remuneration are not overtly linked to actual risk management performance, it is unlikely that such performance will be to the expected standard. Efforts by individuals should be recognized appropriately.

— As a general rule, it is unwise to rely on a single human-dependent control to make a large modification to risk.

— Trans-national organizations will be wise to recognize the significance of culture in determining the way people behave.

Practical help

Examples of useful questions to ask regarding human and organizational factors include the following:

— Is the organizational structure appropriate to the needs of the organization?

— Are individuals with formal accountabilities clearly identified?

— Do all job descriptions contain clear specifications of the individual's authorities and responsibilities?

— Are all communication channels clear and effective?

— Is it occasionally checked whether communication is correctly understood and interpreted at all levels in the organization?

— Is the level of morale in the organization monitored?

— Are interfaces reviewed between teams?

— Are there mechanisms to recognize and respond to rumours within the organization before they impact in a negative way?

— Are there clear recruitment, remuneration and promotion policies?

— If policies are problematic, is there a process to review?

— Are policies and procedures adhered to? If they are not, is there an investigation? Are they enforced?

— Do internal and external auditors look for unsafe or unethical behaviour in the organization?

B.2.9 Risk management is transparent and inclusive

B.2.9.1 Principle

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.

B.2.9.2 How to apply the principle

This principle can be given effect at multiple levels. It may be reflected in the organization's risk management policy (e.g. "We will inform and consult stakeholders wherever possible in order that they understand our objectives and can contribute their knowledge and views to assist in our decision making").

Consultation with stakeholders as part of the application of the risk management process needs careful planning. It is here that trust can be built or destroyed. To be efficient and strengthen trust in the results, relevant stakeholders should be involved in all aspects of the risk management process, including the design of the communication and consultation process.

Implementation of this principle should consider issues of confidentiality, security and privacy, e.g. this may require that information in risk registers is segregated so that access to some information can be restricted.

Practical help

— Role playing should be included in relation to communication and consultation in risk management training.

— An assessment should be made of how those receiving information will perceive it.

— Periodic feedback should be provided to demonstrate how well what was promised or projected actually performed in practice.

— Unsolicited views should be encouraged, acknowledged and appreciated, and wherever possible, feedback should be provided about them.

B.2.10 Risk management is dynamic, iterative and responsive to change

B.2.10.1 Principle

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

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

B.2.10.2 How to apply the principle

Any change in the organization's objectives, or any aspect of the internal or external circumstances, will inevitably change the risk (e.g. an internal restructuring, a new major supplier, or a change in relevant law). Similarly, changes in the organizational context (e.g. the acquisition of another company, or securing a new major contract) may require changes in the framework (e.g. in training, risk specialists). Risk management processes should be designed to reflect the dynamics of the organization (e.g. speed of change).

ISO 31000 contains two monitoring and review regimes (for framework and process). Each is specific to its purpose, and each requires thought and implementation.

The framework should be monitored and reviewed to ensure it can continue to give effect to these principles of effective risk management, give effect to the organization's risk management policy and support the application of the process to decision making across the organization.

Monitoring and review should be incorporated into each of the core steps of the risk management process.

Controls should also be reviewed to ensure their on-going effectiveness in response to change. For example, controls that are dependent on the performance of particular people might not be as effective if there are changes in personnel.

Monitoring and review should be carefully tailored, in particular so that they will be sensitive to the factors of change that can have the most profound effects. Monitoring and review should evaluate the continual significance of the monitored indicators and, if necessary, the indicators will need to be adapted to changing or emerging circumstances.

Monitoring and review are distinctive activities, as explained in ISO 31000:2009, 4.5 and 5.6. Monitoring is concerned with the continual observation of key parameters to determine whether they are performing as intended or as assumed. Review occurs from time to time, is structured as to its purpose and is generally intended to determine whether the assumptions on which decisions were made (e.g.

the design of the framework) remain current, and therefore whether resulting decisions need review. Review should also take into consideration new knowledge and technologies.

Practical help

— When applying the risk management process and developing the statement of context, the components (e.g. features of the external environment) that are most likely to change should be identified, and they should be closely monitored for change. Any change could require reassessment of all or some of the documented risks.

— People should be encouraged to report concerns about the status quo (including whistle-blowers).

— Even small organizations should keep in mind global changes, e.g. the global financial crisis of 2008 had profound impacts on some small suppliers whose main customers were organizations impacted directly or indirectly by bank failures. Such external events or emerging circumstances may require proactive changes to the risk management framework.

B.2.11 Risk management facilitates continual improvement of the organization

B.2.11.1 Principle

k) Risk management facilitates continual improvement of the organization.

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

B.2.11.2 How to apply the principle

Continual improvement of organizational performance is interrelated with continual improvement of risk management performance. Improved risk management, based on risk-based decision making, can reduce uncertainty in achieving objectives, minimize volatility and increase agility. However, care should be taken not to overcomplicate risk management performance to the point of stifling the pursuit of opportunities and flexibility of response.

Instead, the importance of this principle lies in organizations remaining alert to new opportunities to improve. Such opportunities may arise internally (e.g. by learning from reported incidents) or externally (e.g. by the availability of new tools and knowledge that can improve risk management).

This principle is also relevant to continually looking for improvements in risk management efficiency, e.g. deploying new technologies that better connect decision makers to information.

The goal of continual improvement should be made clear in the organization's risk management policy and it should be continually communicated in both formal and informal ways. Continual improvement may include the following:

— improving the extent of integration of risk management activity into general activity;

— improving the quality of risk assessment;

— improving the framework, e.g. the quality of and access to information;

— improving the speed of decision making.

Continual improvement is based on qualitative and quantitative indicators of progress. Organizations that use phased approaches and maturity models should design these as drivers of continual improvement based on the resources and culture of the organization. They should recognize that in many human endeavours success breeds success. The purpose of managing risk effectively lies solely in increasing the likelihood that an organization will achieve its objectives in full. The more rapidly an organization can achieve effective risk management, the more efficiently it will realize its goals.

In purely practical terms, some improvements may take time to achieve, e.g. some may require allocation of a budget, or careful planning and roll out. Plans for improvement should consider priorities and relative benefits, and should allow for the monitoring of progress.

Practical help

— Using the monitor and review elements of the framework, an annual review should be conducted of performance against these risk management principles and design improvements.

— The adequacy, suitability and efficiency of the risk management framework should be evaluated and reviewed.

— The incident reporting system should be used to conduct root cause analysis, looking not only at the proximal causes of the incident, but also the features of the risk management framework that made it possible for the incident to occur.

— Success (e.g. an on-time/in-budget project) should be monitored so as to understand which features of the risk management framework most facilitated success, and this should be communicated to reinforce value.

Annex C
(informative)

How to express mandate and commitment

C.1 General

This annex provides guidance and strategies on how mandate and commitment can be expressed and communicated by an organization.

For mandate and commitment to be effective, top management and the oversight body of the organization should clearly express to stakeholders the approach to managing risk and document and communicate this, as appropriate. The mandate for risk management typically involves changes in behaviour, culture, policy, processes, and expected performance in managing risks which will be reflected in the risk management framework. The mandate and commitment might be a short policy statement that is widely communicated.

Developing the mandate involves deciding on the course of action required, as well as authorizing it to occur. Invariably, in existing organizations, this will necessarily involve authority to bring about change. There would be little point in identifying the preferred course of action unless, at the same time, there was a corresponding commitment to bring this about.

Mandate and commitment is a fundamental part of the risk management framework. It should be part of the organization's management and governance frameworks and should influence the design of both.

Mandate and commitment should reflect the eleven principles set out in ISO 31000:2009, Clause 3.

In practice, the organization's mandate, and its commitment to it, is expressed and perceived in both explicit and implicit ways. The implicit expressions (e.g. the day-to-day actions of top management and the oversight body within the organization's prevailing culture) typically provide a more powerful stimulus than do the explicit expressions (e.g. a written risk management policy).

C.2 Methods for expressing mandate and commitment

C.2.1 Key characteristics

The expression of the mandate and commitment should meet the following criteria:

a) it should be compatible with the organization's strategic plan, objectives, policies, styles of communication and management system;

b) it should be compatible with the risk criteria determined by the oversight body;

c) it should meet the principles of ISO 31000 as well as strive for excellence in risk management as outlined in ISO 31000:2009, Annex A;

d) it should be easy to communicate and be tested for comprehension inside and outside the organization;

e) it should have reasonable expectations of being successfully implemented;

f) it should address the responsibilities of risk owners.

If the existing risk management mandate and the organization's commitment to risk management does not already meet these criteria, both the explicit and implicit aspects of it will need to be changed.

EXAMPLE If the oversight body or top management have made decisions which have not been subject to thorough risk assessment, this is a clear indication that the organization is not committed to understanding its risks.

An essential part of adopting a revised mandate is the development of a plan to change the understanding of what is required. The aim of this plan will be to ensure that both the mandate and its benefits are widely understood and believed, and that the organization is consistently committed to the mandate and behaves accordingly. It will be the organization's behaviour and how this compares with explicit statements about the mandate that will have the greatest effect on whether the mandated is accepted by the various stakeholders.

C.2.2 Establishing and communicating risk management policy and commitment

One way of expressing and communicating the mandate in an explicit way is through establishing and then communicating risk management policy. ISO 31000:2009, 4.3.2, specifies that the organization should not only make its policy about risk management clear but should also communicate it, both inside and outside the organization. ISO 31000:2009, 4.3.2, also identifies specific issues that typically should be reflected in the policy.

Keeping in mind Principle g) (i.e. risk management is tailored), the expression of policy should be appropriate to, and consistent with, the general way in which the organization operates. Otherwise, it may not be regarded as relevant to, and part of, the general system by which the organization operates.

For larger organizations, establishing a policy will normally signify the development of a formal statement about the mandate for risk management that will form part of its overall suite of policies. Accordingly, it will be signed off by the governance body and then communicated and reinforced through the management system.

Practical help

Top management and oversight body involvement and commitment is key to the success of any risk management programme. The organization should consider the following questions when establishing its mandate and commitment to risk management:

— What are the strategic objectives of the organization? Are they clear? What is explicit and what is implicit in those objectives?

— Is top management clear about the nature and extent of the significant risks it is willing to take and the opportunities it is willing to pursue in achieving its strategic objectives?

— Does top management need to establish clearer governance over the risk attitude of the organization?

— What steps has top management taken to ensure oversight over the management of the risks?

— Do the managers making decisions understand the degree to which they (individually) are permitted to expose the organization to the consequences of an event or situation? Any risk attitude needs to be practical, guiding managers to make risk-based decisions.

— Do the executives understand their aggregated and interlinked level of risk so they can determine whether it is acceptable or not?

— Do top management and executive leadership understand the aggregated and interlinked level of risk for the organization as a whole?

— Are both managers and executives clear that risk attitude is not constant? It may change as the environment and business conditions change. Anything approved by top management needs to have some flexibility built in.

— Are risk decisions made with full consideration of consequences? The risk framework needs to help managers and executives take an appropriate level of risk for the business, given the potential for reward.

— What are the significant risks top management is willing to take and the opportunities it is willing to pursue? What are the significant risks top management is not willing to take? Whatever the form of the policy about managing risk, it should sit alongside the other policies that direct the way that the organization operates.

The policy should be supported in both explicit and implicit ways and reflected accordingly, and it should meet the six criteria in C.2.1.

C.2.3 Reinforcement

Top management and the oversight body should demonstrate and reinforce the organization's commitment to the mandate through a mix of explicit and implicit actions including:

— making it clear that risk management objectives are linked to and not separate from other management objectives;

— making it clear that risk management is about effective delivery of the organization's objectives;

— ensuring the type of risk management activities required by the mandate are integrated into existing governance and management processes, and into strategic, operational and project processes;

— requiring regular monitoring of and reporting on the organization's risk management framework and processes to ensure that it remains appropriate and effective;

— monitoring that the organization has a current and comprehensive understanding of its risks and those risks are within the determined risk criteria and taking corrective action where these criteria are not met;

— leading by example with respect to their own activities;

— renewing the commitment to the mandate as time, events and top management change.

Implementation of ISO 31000 can take place across an organization as a whole, or be achieved part by part, e.g. within subsidiary businesses.

C.3 Guidance on development of the mandate and commitment

Establishing the mandate for risk management requires careful thought, a strategic perspective and consultation between the oversight body and top management. This will help ensure that once adopted, the organization will follow the mandate.

Expression of mandate and commitment should be considered on both the tactical and strategic levels. The organization should define and assess competencies to meet its objectives and cultivate the necessary skills and expertise to achieve them.

The implications of changes required by a mandate will need careful consideration. This includes who would lead the change and who would need guidance or support. Sometimes changes may be quite radical in scope (e.g. changes in job specifications, performance monitoring and management processes) and so will absorb some of the organization's capacity for change. This will need to be considered in the context of other changes that are underway and whether there can be integration.

People who will be significantly affected by the changes should be consulted, in particular the custodians of any risk management silos within the organization (e.g. health and safety, security management), so that all the implications of change can be understood.

The mandate should be articulated in a policy statement which will demonstrate the organization's commitment to it.

Practical help

Some of the ways in which this can be achieved include the following:

— considering how the mandate will be explained to the organization and how those explanations will be reinforced by ongoing actions;

— considering the timeframe for giving effect to the mandate (this should respect and be integrated with the organization's other imperatives, although until the framework is complete, its full benefits will not be realized and the management of risk will not be as effective as it could be);

— identifying key roles to bring about necessary change in the approach to risk management and to direct and lead risk management activities;

— specifying what aspects of the risk management framework and activities will be monitored at top management, management and committee levels and how such information will be collected and presented;

— including risk management performance as a regular agenda item at all key oversight and top management meetings;

— developing effective methods for communicating about risk management performance (e.g. publication of a newsletter for staff in the style of a risk management report);

— considering what should be the triggers for review of the mandate.

Annex D
(informative)

Monitoring and review

D.1 Background

D.1.1 General

This annex provides advice on monitoring and review of the risk management framework and processes in accordance with ISO 31000:2009, 4.5, 4.6 and 5.6.

Monitoring and review are two distinctive activities intended to determine whether assumptions and decisions remain valid. The techniques are used in both the maintenance of an effective risk management framework and in each of the steps of the risk management process.

— Monitoring involves the routine surveillance of actual performance and its comparison with expected or required performance. It involves continual checking or investigating, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected, as well as changes in context.

— Review involves periodic or impromptu checking of the current situation, for changes in the environment, industry practices, or organizational practices. It is an activity undertaken to determine the suitability, adequacy, and effectiveness of the framework and process to achieve established objectives. Reviews should consider the outputs from monitoring activities.

— An audit is a process of evidence-based, systematic review against pre-determined criteria. While every audit is a review, not every review is an audit.

Together, monitoring and review provide assurance that risk management performance is as expected, whether it can be improved and whether change has occurred requiring adjustment or revision of either the framework or some aspect of the process.

Monitoring and review aim to provide reasonable assurance that risks are adequately managed, to identify deficiencies in risk management, and to identify opportunities to improve management of risks. Both are necessary in order to ensure the organization maintains a current understanding of its risks in relation to its risk criteria, consistent with its risk attitude. Both require a systematic approach integral to the organization's general management systems.

The monitoring and review activities and the actions taken in response to findings are often characterized as a system of assurance because they have the potential to detect and remedy weaknesses before adverse effects occur or to provide confidence that risks are still within the organization's criteria. These activities can also be used to provide internal and external stakeholders with reasonable assurance that risk is being managed effectively.

As the factors in the internal and external context change, so will the risk. Similarly, monitoring of the external context can alert the organization to changes that may present an opportunity for improved performance or a new activity. By remaining alert to such changes, to performance, to non-conformities, and to near-misses, the organization will be able to identify opportunities for improvement of the risk management framework and overall performance of the organization.

There should be a comprehensive programme in place to monitor and record risk performance indicators that align with performance indicators of the organization.

The programme should give early warning of adverse trends that may require preventive action and intervention.

A single monitoring or review activity may be directed at an individual risk or a number of related risks. It may focus on the risks or upon the controls addressing them.

D.1.2 Accountability for monitoring and review

The overall responsibility for monitoring and review activities lies with the oversight body and top management, not with assurance providers, e.g. internal audit. Quality assurance functions, independent review functions and regulatory monitoring are useful adjuncts to the process of line management reporting because these activities provide an alternative view.

The monitoring and review activities can be considered in terms of a hierarchy, with regular practice at the top: if properly designed, this provides the most powerful level of assurance. However, a monitoring and review programme should include all three elements.

The monitoring and review programme should verify that risk management policy is both implemented and effective. The way in which top management reacts to the results of monitoring programme may affect the behaviour of employees, and it is important that top management acts as role model.

D.1.3 Independent reviews

Whether conducted by internal or external parties, independence comes from the relationship of the reviewer/auditor to the engaging party.

Independence is the basis for the impartiality of the review and objectivity of the review conclusions. Reviewers and auditors should be independent of the activity being reviewed/audited wherever practicable, and should in all cases act in a manner that is free from bias and conflict of interest.

For internal audits, auditors should be independent from the operating managers of the function being audited. Reviewers and auditors should maintain objectivity throughout the review audit process to ensure that the findings and conclusions are based only on the evidence.

For small organizations, it may not be possible for reviewers and auditors to be fully independent of the activity being reviewed/audited, but every effort should be made to remove bias and encourage objectivity.

Independence of reviewers and auditors help to make reviews and audits an effective and reliable tool in support of risk management policies and controls, by providing information on which an organization can act in order to improve its performance.

Such reviews may focus on compliance with standards (internal or external), procedures or legislative requirements. Often they also consider the suitability, effectiveness and efficiency of controls, e.g. they may consider whether risk management activities deliver the values expressed in the principles of ISO 31000.

Many organizations have management review and advisory functions (such as risk management advisors, compliance officers, and quality assurance managers) that undertake routine reviews; internal audit typically reports its reviews to the oversight body and top management. The objective of these reviews is to provide assurance to the oversight body and top management of the organization that:

— its risk criteria are consistent with its objectives and the context in which it is operating;

— an appropriate and systematic process has been used to identify, assess and treat risks and there is confidence that this process will continue to operate;

— unacceptable risks are being addressed by appropriate risk treatment;

— controls believed to be modifying otherwise unacceptable risks are both suitable and effective;

— appropriate progress is being made with risk treatment plans.

The activities of an independent review process do not relieve line management of its monitoring and review responsibilities.

D.1.4 Obtaining suitable information

Like other aspects of risk management, monitoring and review requires the use of the best available information [see Principle f)]. To be suitable for the purpose, the information needs to be relevant to users and faithfully represent what it purports to represent. The usefulness of information is enhanced if it is comparable, verifiable, timely and understandable. Information can be obtained from two types of sources:

a) direct sources: observations and measurements of actual process operations or their outcomes;

b) indirect sources: measures that are derived from the processes or outcomes under consideration.

Combinations of measurements from the various sources are chosen for necessity (depending on availability) or for convenience (timeliness, cost, etc.).

D.1.5 Reporting the review process

Reporting should provide information to the oversight body and top management and the organization's stakeholders about whether the organization's risks are within its risk criteria or whether it has credible risk treatment plans that will ultimately lead to this result. Additionally it may provide information about new and emerging risks.

Any collection of risk information (e.g. in a risk register) should be updated periodically. The type and frequency of reporting will depend on the nature, size, and scope of the risk assessment.

The output of a review or an audit will be a report summarizing findings and providing conclusions of the assessment against pre-determined criteria. The report may provide recommendations for system improvements based on what the reviewers have observed. Occasionally, the reviewer will make broader suggestions, directed at the criteria themselves. Response to any review should be focused on improving the system and addressing root causes of problems.

D.1.6 Corrective action and continual improvement

Processes should be established to ensure that recommendations are actively considered by organizational management and that agreed responses are actioned. Action in response to reviews should be reported to the oversight body and routinely monitored until implemented

D.2 Monitoring and review of the framework

D.2.1 General

The purpose of monitoring and review is to keep the risk management framework current and consistent with the organization's risk management intentions. The framework refers to the components and processes within the organization's system of management that enable risk to be managed.

ISO 31000:2009, Clause 4, contains guidance on the necessary components of a framework and notes that these should have regard to the internal and external context of the organization.

As changes occur to the internal or external context of the organization, it may be necessary to adjust the framework to ensure it remains effective.

Even if there have not been internal or external changes that would require change in design, it is still necessary to ensure that at any time, the framework is functioning as designed. For organizations transitioning to align with ISO 31000, this may involve checking on the framework components of the implementation plan to ensure they have been correctly implemented. For organizations that have already implemented ISO 31000 it will involve ensuring that framework components continue to exist and function as planned.

D.2.2 Accountability

Management is responsible for ensuring that the framework is periodically reviewed and monitored against performance indicators. As part of allocating responsibilities for risk management, either a person (e.g. a senior manager) or an organizational function (e.g. the corporate risk management support function) should be made custodian for the framework, and a key responsibility should be to ensure that the framework remains effective.

D.2.3 Establish a baseline

A baseline for risk management in the organization should be established. The baseline can be described in various ways but should include:

a) the components of the framework (as described in ISO 31000:2009, 4.3) that provide the capability to enable this intent to be achieved;

b) the extent of support provided by the oversight body and top management in the mandate and commitment for risk management (often expressed in the form of a risk management policy).

The intended form and architecture of the framework would generally have been recorded when it was designed, and information such as that shown in Table D.1 will be available. This forms a baseline or reference point for comparisons made during monitoring and review.

Table D.1 — Example of a table to list the components of the framework

Component	Where deployed	Objective	Key actions	Responsibility and scheduling	Performance measures	Status of implementation
Accountability	Organization level	Maintain current organization risk management policy	• Determine criteria • Document reporting • Delegate authority	• Publish policy • Formalize delegations schedule • Next review: xx/xx/xx	...	...
...						
Resources: Training	Division level	Provide risk management components for all induction training Make refresher training available	• Obtain advice • Design training • Train trainers	• Design: Corporate risk management • Roll out: Divisional management • Next review: xx/xx/xx	• Done: Monthly reports • Quality: Training debrief and audit	...

The organization should also establish performance indicators that are linked to the organizational objectives to give an indication of the effectiveness of the overall framework for managing risk. Indicators of performance, sometimes referred to collectively as lagging indicators, include the following:

— incidents, accidents and near-misses;

— actual losses;

— non-alignments;

— customer complaints;

— outstanding debt;

— system availability;

— the extent to which organization objectives are being met;

— the extent to which the risk management objectives are being met.

D.2.4 Assess whether the characteristics and context of the organization have changed

Determine whether the internal or external context of the organization has experienced material change since the risk management framework was developed or modified.

Practical help

The internal characteristics that might have changed include:

— structure;

— governance practices and requirements;

— policies, internal standards and models;

— contractual requirements;

— strategic and operational systems affected by internal or external factors (e.g. legal regulatory changes);

— capability and resources (e.g. financial and reputational capital, time, people, processes, systems and technologies);

— knowledge, skills and intellectual property;

— information systems and flows;

— social, environmental and cultural behaviour;

— other organizational priorities and imperatives that can be perceived to compete with the organization's intentions for managing risk.

Leading indicators, which might point to changes in the external context, are frequently found in reports and surveys, which reflect changes and trends in the industry in which the organization operates. Examples include:

— commodity pricing, bank interest rates, bond yields, exchange rates, stock market indices, consumer price index (trend);

— index (trend);

— level or incidents of fraud in similar organizations;

— market size and growth figures, and sudden changes in order volume;

— political and social stability, societal discontent and activism.

If the organizational context has changed since the risk management framework was developed, the risk management framework should be reassessed and aligned so as to account for these changes. The purpose of this activity is to confirm that the framework and processes are fit-for-purpose and consistent with the objectives and priorities of the organization.

As a consequence of this review, the organization may need to change its baseline.

EXAMPLE 1 A change in the structure of an organization might require some revision of the risk management policy and a reallocation of accountabilities and resources to permit risk to continue to be managed effectively. If the organization has increased in size, e.g. due to a merger or acquisition, the ongoing adequacy of risk management resources will require consideration, as will careful analysis of any difference between the organizations in approach to risk management. It might be necessary to develop a transition plan to implement any changes arising from the analysis.

EXAMPLE 2 If new legislative requirements have been enacted, aspects of the framework that concern accountabilities, training and information-capture or reporting might need amendment or expansion.

D.2.5 Review of the framework

Once the assessment of the characteristics and external context has been completed, a more comprehensive review of the framework should be conducted to determine whether:

a) the risk management plan is being carried out as planned;

b) the framework and processes adopted are operating as planned;

c) the level of risk is within the criteria;

d) core organizational objectives are being positively influenced by the management of risk;

e) relevant stakeholders are receiving sufficient reporting to enable them to discharge their roles and responsibilities in the governance structure;

f) people across the organization have sufficient risk management skills, knowledge and competence to carry out their responsibilities as they have been identified;

g) the risk management resources are adequate;

h) lessons have been learned from actual outcomes, including losses, near-misses and opportunities, that occurred;

i) the objectives set out for risk management are being achieved.

There should be an agreed regular review schedule, with the ability to carry out reviews for a specific purpose if circumstances change, e.g. where the consequences of risks are sudden or severe.

Deliverables from such a review should include:

— an overall report on the performance of the risk management framework;

— a report on progress of implementation of the risk management plan (including analysis of any delay in implementation);

— a report outlining the organization's maturity position with respect to best practices;

— recommendations of changes that are necessary to improve risk management and its effectiveness in the organization;

— updates to risk management policy, objectives and plan as necessary;

— updates to the description of the context in which the organization operates, as appropriate;

— a report on trends in key risk indicators;

— an action plan to address changes required to meet risk management objectives.

D.3 Monitoring and review of the process

D.3.1 General

The purpose of monitoring and review of the risk management process is to ensure that it is:

— suitable for the business activity;

— working as planned.

The risks, their underlying controls and treatments may alter over time, and those accountable for the management of risk need to be aware of the implications of these changes. Failures in treatments may lead to the risk being unacceptable. In addition, the controls whose purpose is to modify risks may change in terms of suitability and effectiveness, so unless risk is monitored and reviewed, the risks may not remain within the organization's acceptable risk criteria and the organization may not have a current understanding of its risks.

The results of monitoring and review will be fed back into the establishing the context phase, providing the basis for renewed risk assessment, fulfilling the iterative and dynamic nature of the risk management process and the risk management framework design.

D.3.2 Accountability

Monitoring should be an integral part of management. Risks and controls should be allocated to owners, who are responsible for monitoring them. This responsibility should be recorded in role or position descriptions.

Organizations should consider incorporating risk management performance indicators, which reflect the range of key organizational drivers, in formal reviews of employees, e.g. so that financial, stakeholder, internal efficiency and learning and growth objectives are considered. Performance against the same set of indicators can be measured at all levels of the organization and then reported as appropriate.

Risk treatment plans should also be monitored to make sure that progress is being made and that actions are completed on time.

D.3.3 Learning from experience

The organization should learn from actual outcomes. These should include losses, near-misses, non-conformities and opportunities that were identified in advance, occurred, and yet were not acted on. Points that may be considered in such a review include:

— what happened;

— how and why the outcome came about;

— whether any assumptions need to be reviewed as a result of the outcome;

— what action has been taken (if any) in response;

— the likelihood of the outcome happening again;

— any additional responses or steps to be taken;

— key learning points and to whom they need to be communicated.

D.3.4 Monitoring

D.3.4.1 Typical approaches for monitoring include the following.

a) Risk owners can scan the environment to monitor changes in context. The frequency of this activity will depend upon the level of risk and the dynamics of changes in the context. In some cases, exception reporting of indicators may be sufficient. The risk owner compares the relevant external or internal factors against the statement of context to determine if a material change has taken place. This may involve periodic communication and consultation with stakeholders to determine if their views or objectives have changed.

b) Risk owners should also monitor risk treatment plans for timely actions and response to changes in the environment.

c) Control owners are responsible for monitoring controls assigned to them, which may involve periodic checking or continual monitoring. Because risk management is most effective when it is fully integrated with the normal decision making and system of management of the organization, the organization's performance management should be used to monitor risks and the effectiveness of the risk management process. Performance indicators should reflect the range of key organizational objectives defined when the context was established at the start of the process. They may also be developed that relate to specific risks and controls and the application of the risk management process.

NOTE As is the case with risks, it is advisable that controls are also owned by someone who is responsible for their operation. The control owner or operator would normally be the person who executes the control on a daily basis and can be someone other than the risk owner. This does not affect the overall responsibility of the risk owner for the proper modification of that risk, and for the design, implementation, application, monitoring, and evaluation of the corresponding controls.

D.3.4.2 Performance indicators may measure outcomes (e.g. specific losses or gains) or processes (e.g. timely completion of risk treatment plans). Normally a blend of indicators can be used, but outcome performance indicators usually significantly lag the changes that give rise to them. As a result, in a rapidly changing environment, process indicators (lead indicators) are likely to be more useful.

In choosing performance indicators, it is important to check that:

— they are measurable;

— their use is efficient in terms of demands on time, effort and resources;

— the measuring process or surveillance encourages or facilitates desirable behaviour and does not motivate undesirable behaviour (e.g. fabrication of data);

— those involved understand the process and expected benefits and have the opportunity to give input to setting the indicators;

— the results are captured and performance analysed and reported in a form that will facilitate learning and improvement across the organization.

D.3.4.3 In applying performance management to the risk management process, it should be noted that:

— effective measurement of performance requires resources, which should be identified and allocated as part of the development of the performance indicators;

— some risk management activities may be difficult to measure, which does not make them less important, but it may be necessary to use surrogate indicators, e.g. resources devoted to risk management activities may be a surrogate measure of commitment to effective risk management;

— any variance between performance indicators measurement data and instinctive feel is important and should be investigated, e.g. if management remains concerned that risks are not being properly managed, despite numerous risk assessments indicating low levels of risk, these concerns should be investigated and not dismissed;

— while sudden deterioration in indicators will usually attract attention, progressive deterioration can be equally problematic, and trends in performance indicators should be monitored and analysed.

D.3.5 Review

Management should periodically review processes, systems and activities to ensure that:

a) new risks have not arisen;

b) controls and risk treatments remain suitable and effective.

Such reviews should be programmed (see programme and risk based audit approach and how to select reviewers, as outlined in ISO 19011).

These reviews may use the same techniques as ongoing monitoring, but if they are conducted by someone who is not directly involved in the operation of the processes, they may provide a more objective analysis. The frequency of review may be influenced by the level of risk, the business planning cycle, the dynamics in the environment/context, or a meeting of a governance body that is responsible for the oversight of risks and risk management.

If problems are found, the organization should consider how these came about and why they were not detected before.

Controls should be assured through the actions of accountable managers (risk owners) as part of their normal jobs and roles. The allocation of specific controls to control owners facilitates implementation of controls, but those owners will require training in control assurance processes in order to be effective.

When organizational changes are planned, or external changes are detected, there may be changes in:

— the external or internal environment or stakeholders and their views;

— the risk management context, the organization's objectives and its risk criteria;

— risks and levels of risk;

— the need for risk treatments;

— the effect and effectiveness of controls.

For this reason, it is essential for organizations to review their risks, risk treatments and controls when developing or revising business or strategic plans. In addition, because business and strategic plans may create or revise an organization's objectives, it is valuable to use the risk assessment process to stress test the draft plans in order to ensure the proposed objectives are achievable, and also to define the risk treatment measure required to ensure successful outcomes. Those carrying out the risk management process should also regularly review their experiences, outputs, and results to identify opportunities to improve.

Annex E
(informative)

Integrating risk management within a management system

E.1 General

Risk management is an integral part of an organization's management system. ISO 31000 advises organizations to develop, implement and continually improve a framework whose purpose is to integrate risk management into the organization's system of management (including governance and strategy). Specifically, the integration should ensure that information about risk is used as a basis for decision making at all levels of the organization. People and organizations manage risk each day as part of how they make decisions. Risk management is already integrated naturally in what we all do before we decide to do something. Some are better at this than others, but all can improve the quality of risk management and decision making, resulting in improvement in achieving objectives and improved confidence. If the purpose of integrating risk management is to add value, it logically signifies adopting ways to influence what already takes place, to enhance and improve it, rather than replacing it with something different. It cannot signify adding or forcing something different into what already occurs as a natural function of decision making.

Integration does not simply involve introducing established and standardized risk management tools and processes into (an) existing management system(s), it requires the adaptation and alteration of those tools and processes to suit the needs of the decision makers and their existing processes for decision making.

This annex provides some practical examples of how risk management can be integrated into the existing management system(s).

E.2 What is a management system?

All organizations use some kind of management system. In recent times, formalized management systems consisting of a variety of requirements have been created, which provide a framework in which the organization can establish management practices and procedures to direct and control its activities. Many international standards deal with management systems in general or with regard to specific content.

A management system is a set of interrelated or interacting elements of an organization to establish policies and objectives, as well as processes to achieve those objectives. From a business management perspective, efficiency is gained by having one, integrated system of management.

For example, quality management as addressed in ISO 9001 has a broad approach directed towards customer satisfaction, while risk management deals with the effects of uncertainty on objectives that may not only be relevant to customers, but also to a variety of other stakeholders. Many organizations have implemented a quality management system based on ISO 9001 requirements, and risk management can be integrated in those management systems, creating synergies and avoiding duplication.

E.3 Integrated management system and risk management

As well as integrating risk management with core business processes, there is a need to create interaction between all the management system approaches, e.g. quality management, environmental management, safety management, security management, compliance, financial and reporting management, and even with insurance management dealing with events that may be financially transferred to other organizations.

These individual management systems should form an integrated management system, based on the policy and strategy of any organization. Even where an organization has individual management systems to manage particular risks, the risk management framework should extend to, and incorporate, those systems.

Such a cross-organizational risk management approach can:

a) increase the focus of top management on the organization's strategic objectives;

b) enable all risks in the integrated management system to be handled according to the principles and guidelines of ISO 31000.

This approach can involve the following:

— the application in the quality management system of risk management techniques that concern primarily product and project risk management;

— dealing with the uncertainties in environmental management, e.g. incidents and potential accidents in hazardous premises, the disposal of hazardous material and substances;

— the treatment of risks combined with operations such as safety at work;

— handling security risks, e.g. acts of violence against the organization or its employees or customers;

— handling information technology (IT) security risks, e.g. the breakdown of IT operations, loss of data, breach of confidentiality and assuring business continuity;

— managing business continuity risks that ensure preparation for, and quick response to, disruptive events;

— establishing controls to protect the organization's assets, to ensure correct reporting, to ensure compliance with legal requirements, or to manage insurable risks in a way that minimizes premiums.

E.4 Implementing risk management into a quality management system framework

E.4.1 General

The risk management process should be integrated into an organization's decision-making processes, irrespective of the level and function at which those decisions are made.

E.4.2 Identification and awareness of decision taking

The following methods help in recognizing when and where decisions are being made, in line with the Plan-Do-Check-Act cycle.

a) Identify all forms of formalized decision-making practices that already exist within the organization. In large organizations, there are likely to be numerous procedures that require formal approvals for a wide range of decisions, e.g. approval of the annual strategic plan, capital expenditure, employment of new staff, modification of process controls, staff travel.

b) Use flow-charting, or some other technique, to map the main decision-making practices and sequences that are applicable to both specific projects and all aspects of business. This can be considered on a division or a function basis, and should extend to governance as well as management decision making. If there are activities that are being managed through application of a formalized management system (e.g. managing quality through the application of ISO 9001), the decision points in such systems should form part of this analysis. Similarly, if the organization has any form of delegated decision-making authority, such delegations should be included in the analysis. The end result should be a coherent and documented picture of where decisions are made, who makes those decisions, and the existing processes applicable to such decisions.

A combination of the above techniques should create a high degree of both organizational and personal awareness of decision-making.

E.4.3 Risk assessment

In some types of decision (e.g. development and realization of a new product, or planning and implementation of a major project), it will be appropriate to include formal risk assessment at various stages of the project. For example, most projects have multiple decision points, i.e. feasibility, business case, detailed budgeting and planning, implementation, and handover. At each of these points, a formal risk assessment is appropriate to decide between options. This increases the likelihood of project success and also improves efficiency.

For risk assessment of operational decisions, simple standardized forms of the risk management process can be developed for use by the staff involved. Such methods are especially suitable in situations where people work without direct supervision. A key component of these methods is creating awareness of assumptions as inputs to decisions. By definition, assumptions are a source of uncertainty.

Such standardized processes can be specific to the type of decision making involved, to the particular group of people performing a particular task, and to the typical context in which they occur. Simple systems can be codified on a pocket-sized, checklist instruction card and carried by all those involved in that type of work.

E.4.4 Implications for the risk management framework

Implementation of the techniques described in this clause will require appropriate provision or adjustment of the risk management framework, e.g.

— amendment of the organization's risk management policy;

— arrangements to carry out the initial investigation and mapping of decision-making practice;

— making amendments to procedure manuals;

— training of managers and staff;

— specific training of those whose work is carried out in accordance with a specific management system (e.g. those that are concerned with management of particular types of risk);

— adjustments to the organization's system of assurance and risk management information capacity;

— effective internal communication and consultation.

Bibliography

[1] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

[2] ISO 9001, *Quality management systems — Requirements*

[3] ISO 19011, *Guidelines for auditing management systems*

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

[5] IEC 31010, *Risk management — Risk assessment techniques*

ICS 03.100.01

Price based on 37 pages

This page has been left intentionally blank.