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.