

a practical guide

for SMEs



ISO 31000

Risk management



ITC
AVA

UNIDO
Documents
Document Sharing Hub

a practical guide

for SMEs

ISO 31000

Risk management



Copyright protected document

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means without permission from ISO.

Views expressed in this publication are those of the author(s) and contributors and do not necessarily reflect those of the International Trade Centre or the International Organization for Standardization or the United Nations Industrial Development Organization.

The designations employed and the presentation of material do not imply the expression of any opinion whatsoever on the part of the International Trade Centre or the International Organization for Standardization or the United Nations Industrial Development Organization concerning the legal status of any country, territory, city or area, or of its authorities; or concerning the delimitation of its frontiers or boundaries; or its economic system or degree of development. Designations such as “developed”, “industrialized” and “developing” are intended for statistical convenience and do not necessarily express a judgment about the stage reached by a particular country or area in the development process.

Mention of names of firms and organizations and their websites, commercial products, brand names, or licensed process does not imply endorsement by the International Trade Centre or the International Organization for Standardization or the United Nations Industrial Development Organization.

© ISO 2015. Published in Switzerland

ISBN 978-92-67-10645-8

ISO copyright office
CP 401 • CH-1214 Vernier, Geneva
Tel. +41 22 749 01 11
Fax. +41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

About the Author

John Lark is the Managing Principal at Coherent Advice Inc., a Canadian firm offering risk management services to public and private sector organizations both domestically and internationally. Mr. Lark has over 35 years' experience in management, 15 years' experience in risk management as well as Bachelors and Masters degrees in Science. He has served on the Risk Management Committee at the Standards Council of Canada, the Canadian Standards Association and at ISO (TC 262 and Working Groups). Mr. Lark gratefully acknowledges the valuable insights into ISO 31000:2009 and risk management that have been generously provided by Grant Purdy and John Fraser.

About the Reviewer

Valentin Nikonov has over 15 years' experience in risk management, compliance and business intelligence within financial institutions and international organizations. Mr. Nikonov is coordinator of an international group of experts on risk management at the United Nations Economic Commission for Europe. As an International Expert on Risk Management of the United Nations Industrial Development Organization, Mr. Nikonov implemented risk management tools and methods into regulatory frameworks of developing countries. He is experienced in designing, implementing and running risk management systems in business and regulatory environments.

Acknowledgements

The International Organization for Standardization, the International Trade Centre, and the United Nations Organization for Industrial Development jointly developed this publication.

ISO, ITC and UNIDO wish to thank John Lark and Valentin Nikonov for their expertise in developing this handbook, as well as ISO/TC 262.

Khemraj Ramful and Hema Menon at ITC led and coordinated the development of this guide. Juan Pablo Davila at UNIDO oversaw the technical review of this guide. Laurent Galichet and Brian Stanton at ISO guided the publication's planning, editing, and design.

The International Trade Centre (ITC)

Trade Impact for Good

The International Trade Centre (ITC) is the joint agency of the World Trade Organization and the United Nations.

ITC mission

ITC enables small business export success in developing and transition countries by providing, with partners, sustainable and inclusive trade development solutions to the private sector, trade support institutions and policymakers.

ITC objectives

- Strengthen the international competitiveness of enterprises through ITC training and support.
- Increase the capacity of trade support institutions to support businesses.
- Strengthen the integration of the business sector into the global economy through enhanced support to policymakers.

Please visit our website www.intracen.org for more information.

About UNIDO

The United Nations Industrial Development Organization (UNIDO) is the specialized agency of the United Nations that promotes industrial development for poverty reduction, inclusive globalization and environmental sustainability. UNIDO's vision is of a world where economic development is inclusive and sustainable and economic progress is equitable. UNIDO aspires to reduce poverty through inclusive and sustainable industrial development. All countries should have the opportunity to grow a flourishing productive sector, to increase their participation in international trade and to safeguard their environment.

For knowing more about UNIDO please visit www.unido.org.

About ISO

ISO (International Organization for Standardization) is an independent, non-governmental membership organization and the world's largest developer of voluntary International Standards.

We are made up of our 162 member countries who are the national standards bodies around the world, with a Central Secretariat that is based in Geneva, Switzerland.

Please visit our website www.iso.org for more information.

Foreword **8**

0 Introduction **10**

1 Objectives and governance **19**

1.1 Clear objectives 19

1.2 Mapping and assessing current governance arrangements 20

2 Mandate and commitment **23**

2.1 Defining your commitment 23

2.2 Setting objectives for implementing ISO 31000:2009 25

2.3 Develop performance measures for risk management 26

2.4 Internal and external stakeholders 27

2.5 Communicate risk management commitment to stakeholders 28

3 Designing the framework for managing risk **31**

3.1 Risk management framework 31

3.2 Compare your current risk management to ISO 31000:2009 37

3.3 Risk management principles 38

3.4 Understand the internal and external contexts of your organization 39

3.5 Risk management policy 42

3.6 Alignment between risk management policy and the organization 44

3.7 Risk attitude 45

3.8 Risk criteria 47

4 Implementing risk management **51**

4.1 Understand your organization’s capability, capacity and culture with respect to risk 51

4.2 Planning the transition to ISO 31000:2009 53

4.3 Implementing the risk management framework 55

4.4 The risk management plan 57

4.5 Resources to implement the risk management plan 59

4.6 Establishing the context of the risk management process 61

4.7 Risk management methodologies 63

4.8 Communication of and consultation on the risk management process 69

5 Monitoring and review.....73

5.1 Monitoring and review of the risk management framework73

5.2 Monitoring and review of the risk management process.....75

6 Continuous improvement of the framework 79

6.1 Determining the effectiveness of risk management79

6.2 Continual improvement of the framework81

6.3 Continual improvement of the implementation of
the process 84

Annex A — Risk management techniques for SMEs 87

Annex B — Specific guidance for SMEs105

Annex C — Guides, handbooks and references for SMEs..... 131

Foreword

Risk is intrinsic to doing business. With empirical evidence showing that 50 % of small and medium-sized enterprises (SMEs) close down before completing their fifth year, it is clear that operating a business can be a risky endeavour. Risk has consequences in terms of economic performance and professional reputation, but there are also environmental, safety and social considerations. These risks may be internal or external, direct or indirect. Despite the underlying element of uncertainty, it is often possible to predict risks, and to set in place systems and design actions to minimize their negative consequences and maximize the positive ones. Those risks that arise from disorder can be controlled through better management and governance. In this manner, businesses that adopt a risk management strategy are more likely to survive and to grow.

Large firms are better equipped and relatively well structured to deal with risks while maximizing benefits. By contrast, due to various limitations, SMEs are more exposed to the negative aspects of risks. However, due to their flexibility, and if provided with the right tools, they can tap into opportunities to increase their market share, grow and manage risk more effectively.

It is well known that SMEs constitute the vast majority of enterprises around the world, and serve as the mainstay of trade and economic growth. They serve as key drivers of innovation, social integration, and employment, representing 60 % of private sector jobs. Given the importance of SMEs to economic growth and development, attention to the issue of SME risk management becomes quite essential.

SMEs have little guidance on how best to manage risk and where to turn to for advice. Studies find that while most SMEs adopt some form of loss prevention and reduction measures, they do not engage in a formal risk management process and a vast majority totally ignore risk treatment.

ISO 31000:2009 — *Risk management — Principles and guidelines*, provides a set of principles, a framework and a process for managing risk. Using ISO 31000:2009 can help organizations of all sizes increase the likelihood of achieving

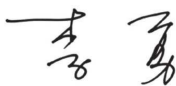
their objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment.

With a view to helping SMEs improve their preparedness and effectively manage risks, ISO, ITC and UNIDO have decided to join efforts and develop this guide on ISO 31000:2009. This publication aims to help SMEs better understand the requirements of ISO 31000:2009, compare their risk management practices with the internationally recognized benchmark, and align their practices according to the international standard.

We hope this guide will serve as a practical and beneficial resource for SMEs in their efforts to improve their competitiveness and increase their participation in international trade through better recognizing and managing their risk portfolio.



Arancha GONZALEZ
Executive Director
ITC



LI Yong
Director General
UNIDO



Kevin McKinley
Acting Secretary-General
ISO

0 Introduction

0.1 Purpose

This guide has been prepared as a brief overview of how to implement risk management in alignment with ISO 31000:2009 in a small-to-medium-sized enterprise (SME), and follows a “question, followed by guidance” format.

ISO 31000:2009, referred to as the standard throughout this document, is a brief and high-level set of principles and guidelines on how to implement risk management. The standard is 23 pages long and presents 11 principles, a framework, and a process that can be tailored to fit an organization of any type and of any size.

This guide is to assist decision-makers in SMEs in understanding the standard and in implementing risk management that is tailored for the size and complexity of SMEs in both developed and developing countries.

The standard, in Clause 1 states

“Although this International Standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed”.

This guide is a checklist and a supplement to the standard and has been written assuming the reader has access to the full standard. The purpose of this guide is to provide clarification, guidance and brief introductory explanations for all the elements of ISO 31000:2009, copies of which can be purchased from ISO or through your national standards organization.

0.2 The value of implementing risk management

This brief summary outlines the value of making an explicit commitment to implementing risk management as a core value of your organization. Businesses of any size have to manage risks, and this is true from creation of the business and during its lifetime. Individuals or groups who perceive

the presence of a risk that can have a positive effect on the organization's objectives, for example a demand for a product or service, may treat this risk by opening a new store or office. In order to commence operations, business owners must manage other risks related to: the acquisition of a location; the identification of skills valuable to the enterprise; and the attraction and recruitment of employees who have these skills, the acquisition of financing, raw materials, machinery, etc. This list is a few examples of risks relevant to an SME.

Risk management is an essential business activity for enterprises of all sizes. Enterprises that manage risks effectively will thrive and produce high quality products or services where these are the organizational objectives.

Implementation of risk management that is aligned with ISO 31000:2009 is done with the primary objective of successfully achieving objectives. It is for this reason that the commitment to implement risk management must exist at all levels in the company. Owners and the Board of Directors (if there is one) as well as managers at all levels should understand the benefits that coherent and reliable risk management can bring, and communicate that understanding to staff by implementing it.

0.3 The value of following this guide

Enterprises both small and large need to identify, understand and manage the uncertainties or risks that are critical to achieving success. ISO 31000:2009 provides a proven, robust and reliable approach to managing risk. Enterprises must understand and manage risks to develop and thrive. By aligning risk management with ISO 31000:2009 organizations will implement risk management consistently and effectively.

This guide is designed to help organizations build on the risk management that enabled the organization to come into existence by supporting a move from anecdotal, event-driven risk management, to risk management that is strategic, focused on actual goals, reliable and cost effective. Risk management is more than taking or avoiding risks. Risk management is the development of a clear understanding of the risks that are important to the enterprise and managing them as the organization evolves and the operating environment (physical, environmental, financial and social) changes through time.

0.4 Structure of the guide

The structure of this guide is aligned with [Figure 1](#) and has a chapter for each of the five elements of a risk management framework as well additional more specific guidance in the annexes.

The structure of this guide is aligned with the sequence of steps: “plan, do, check, act”. The four steps are: **plan** what you will do, **do** – execute this plan, **check** that the plan has allowed you to achieve your organization’s objectives, and **act** to identify areas for improvement in the next business cycle. These four steps are found in many management systems. This process has been called a “virtuous circle”, the “Deming Cycle” ¹⁾ or the “Shewhart Cycle” ²⁾.

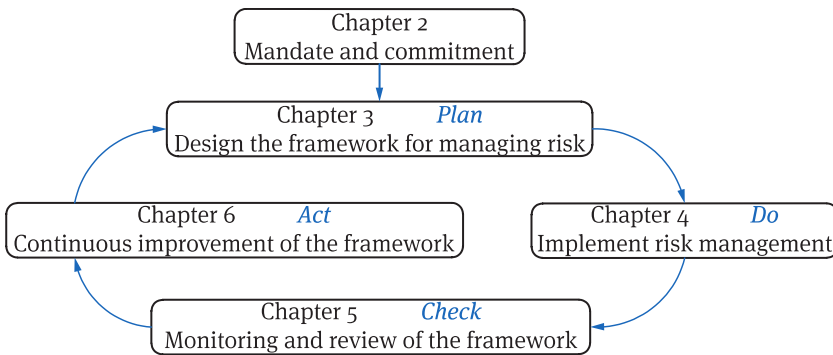


Figure 1 – The structure of this guide

The standard is aligned with this sequence of steps and supports continuous improvement. The standard proposes the four steps of Plan-Do-Check-Act (PDCA) as: **design** (of the risk management framework); **implementation**; **monitoring and review**; and **continual improvement**. This guide follows this sequence to assist users in developing and implementing risk management in a way that it continues to improve the achievement of objectives and which allows risk management respond to changes in order to remain effective.

1) Deming, W.E. 1950. Elementary Principles of the Statistical Control of Quality, Japanese Union of Scientists and Engineers.

2) Deming, W.E. 1986. Out of the Crisis. MIT Press. Cambridge, MA, 88 pp.

This guide recommends that you implement risk management by

- **Developing** a clear plan,
- **Implementing** the plan as it was designed,
- **Verifying** that the plan is delivering the objectives that have been set (in this case the objectives for implementing risk management), and then
- **Acting** to modify the plan in response to the information developed during the monitoring and review stages on what is working well and what should be adjusted to improve the results.

0.5 Risk, definition and interpretation

Risk is a term that has been defined many times and in many ways. In ISO 31000:2009 “risk” has a very specific meaning and in order to understand the standard it is important to understand the definition.

Risk is defined as the “*effect of uncertainty on objectives*”

NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 Risk is often characterized by reference to potential events and consequences, or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequences or likelihood.

[ISO 31000:2009, Clause 2.1]

Risk in ISO 31000:2009 is neutral; the consequences associated with a risk can enhance the achievement of objectives (i.e. positive consequences) or can limit or diminish the achievement of objectives (i.e. negative consequences). Managing risk can be simplified by grouping risks by their relevant business

activity such as “finance-related risks” so that they can be managed more effectively.

Uncertainty, a key element of the definition, can exist as the product of variability of natural systems, and can also arise from information that:

- Is not available,
- Is available but not accessible,
- Is of unknown accuracy,
- Is subject to differing interpretations, or
- Involves a range of possibilities, including changes over time³⁾.

In many organizations, the management of risks with positive consequences is separate from the management of risks with negative consequences. ISO 31000:2009 is clear that the risk management process (shown in [Figure 2](#) below) is the same for risks regardless of the nature of their consequences.

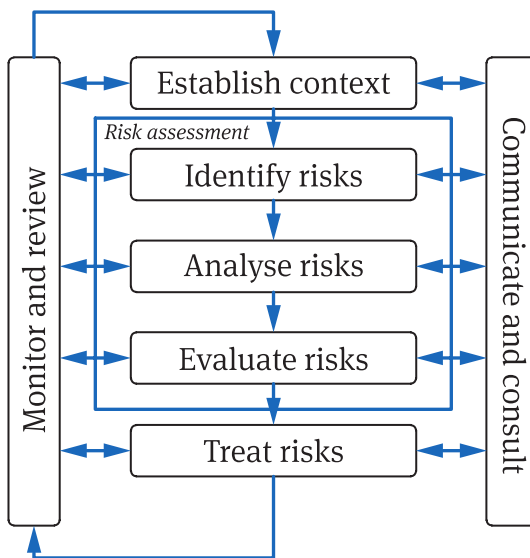


Figure 2 – The ISO 31000:2009 risk management process

3) Derived from Clause 2.2 of SA/SNZ HB 436:2013.

While ISO 31000:2009 does not use these terms, risks with positive consequences for organizational objectives may be referred to as “opportunities”. Examples of opportunities include uncertainty over the presence of oil or minerals in an area, or sufficient market potential to merit expansion. These risks with positive consequences can be treated by testing to determine if commercial quantities of oil or minerals are present, or by evaluating the apparent new market. Managing the uncertainty of these “opportunities” would be accomplished by using ISO 31000:2009. It is more effective for an organization to manage all risks by aligning its risk management with ISO 31000:2009, notwithstanding the nature of the consequences.

Example

Positive or Negative is dependent on context

There may be a risk of a severe storm event that has the capacity to damage infrastructure, delay the transportation of goods the delivery of services. For many residents and businesses, the storm event may have negative impacts on employees arriving at work, the delivery of services or important infrastructure (e.g. factories, bridges). However, if an organization provides emergency services, or repairs, the storm event would have positive impacts on the organization.

In areas where there are hurricanes, businesses have a large inventory of plywood to cover windows, sand and sandbags, tarpaulins and canned food, so that they are in a position to sell large volumes of these products when a storm occurs.

For a business to realize these positive impacts, it has to have large inventories on hand in advance. The uncertainty of the storm is the same for everyone that may be affected. The nature of the uncertainty and its potential impact on objectives is very dependent on the context of the business. The ability of suppliers to benefit from the uncertainty of a severe storm will depend on the degree to which they have treated the risk of a dramatic increase in demand with little advance notice by keeping large inventories of disaster-related goods on hand.

Throughout this guide, the term risk is used to describe an uncertainty that has positive or negative consequences; or both positive and negative consequences. Many risks have both positive and negative consequences.

Example

A decision where risks have both positive and negative consequences on the achievement of the objective

A person is successfully operating a single store selling an array of specialized goods in a moderately sized city. The owner has noted that a similar city in an adjacent country lacks a store selling the range of goods that the current store offers. The uncertainty (risk) that the owner is assessing is whether there is a sufficient market to operate the new store profitably.

If the owner wishes to treat the “market potential risk” (or opportunity) by opening a new store, there is a need to identify and assess *all* risks related to the decision to open a new store. Risks could relate to a different system of taxes and tariffs in that country affecting the ability to make a profit. Also the cost of land, labour, transportation, storage and utilities could be higher than in the current location. Further, the owner cannot be in two places at once and so the direct oversight of inventory and cash management, customer service and sales will have to be delegated in one of the stores.

The current control the owner has over these aspects of the business by being physically present is not possible in both locations at the same time.

The storeowner will need to identify, analyse and evaluate the risks, each in their own context, in order to assess the overall impact on the objective of operating a retail store that can reliably produce a profit. The risk management process can assess the magnitude of all risks so that the owner can determine whether opening a second store in the new location will be a sound business decision.

The term “risk treatment” is defined as “a process to modify risk” and is described in detail in Annex [B.4](#). The standard includes the following note: risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” or “risk reduction”.

The definition of “risk attitude” is defined as “an organization’s approach to assess, and eventually pursue, retain, take or turn away from risk”. When a risk has a positive consequence the “pursuit” of the risk is a logical course of action in order to enhance the achievement of objectives. This term is more fully explained in Chapter [3.7](#).

0.6 ISO 31000:2009 and supporting standards

This guide has been developed based on the assumption that the reader has acquired and read the standard, ISO 31000:2009. The standard is supported by both a formal vocabulary of definitions, found in ISO Guide 73:2009 and an analysis of risk assessment techniques found in IEC 31010:2009. The acquisition of all three of these standards is recommended for readers of this guide.

Standards — ISO

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

IEC 31010:2009, *Risk management — Risk assessment techniques*

ISO Guide 73:2009, *Risk management — Vocabulary*

Technical Report — ISO

ISO/TR 31004:2013, *Risk management — Guidance for the implementation of ISO 31000*

Additional guidance on implementing ISO 31000:2009 can be found in the international guides listed in Annex [C.1](#).

1 Objectives and governance

1.1 Clear objectives

Do you have clear objectives for your organization?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

The word objective is defined by Webster's dictionary as "something you are trying to do, or achieve, a goal or purpose". Another definition is "something that one's efforts or actions are intended to attain or accomplish; a purpose; a target." The objectives of an organization are its reason for being. Objectives must be measureable and tangible.

Such objectives may be found in the organization's strategic plan, or less formally in a document from the senior management team to staff indicating what will be achieved in the coming year (or other time period). In many cases, if formal objectives have not been set, it is useful for the management of the organization to meet and agree on the objectives that they see as critical to the organization being successful.

The owner or managing partners should work with the management team to identify clear objectives for the company and identify a specific date when these objectives will be achieved and maintained. Objectives can take the form of revenue targets, position with respect to competitors, financial reserves, compliance requirements, or other outcomes that are important for the organization to survive and to grow.

Management should identify, approve and communicate the objectives of the organization to all employees.

1.2 Mapping and assessing current governance arrangements

Do you have a clear management framework or a document that describes the governance of your organization?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

Governance is how and when decisions are made and includes accountability as a key consideration. Governance provides clarity over roles and responsibilities and identifies the processes that are essential for the organization to continue and to function effectively. Governance documents describe how management (including the Board of Directors if there is one) directs the company.

Governance functions include planning and budgeting, performance measurement, assurance and auditing, procurement, hiring, assessing and dismissing staff as well as control over all day-to-day operations.

The management of an organization, enabled by its governance arrangements, can be described as “coordinated activities to direct and control an organization”. Risk management is defined as “coordinated activities to direct and control an organization **with regard to risk**”. The parallels between these two statements demonstrate how closely risk management and governance are linked.

Reporting relationships are often shown in an organization chart that identifies the flow of authority in the organization. While such a chart may be a first step, it is only the beginning of mapping the governance of an organization. If the organization is legally incorporated there will be a Board of Directors and a Chief Executive Officer. For very small organizations, there may simply be an owner and governance relationships that are not written down. It is a best practice to develop, approve and communicate the governance arrangements

to employees, and to periodically review them to ensure that they are relevant as business conditions evolve.

Documenting the organization's governance includes identifying approval pathways and criteria for decisions, the span of control for each major division or manager, the documentation required to support business planning as well as how strategic and tactical targets are established and progress is monitored. Governance-related documentation should also reference applicable legislation, regulations, guidelines, as well as internal and external policies that relate to governance and control.

It is critical that the description of governance reflects current arrangements and the levels of authority that have been established. The presence of current, clear and effective governance is essential to creating an effective risk management framework.

2 Mandate and commitment

2.1 Defining your commitment

Do you have a clear commitment from the organization's top management to implement risk management?

- ☐ **Yes** → Go to next question and ensure that this commitment includes clear objectives for the implementation of risk management and explicitly authorizes the investment of the human and financial resources necessary for effective implementation
- ☐ **No** → See guidance below

A clear commitment to risk management from the senior managers of the firm is essential to successful implementation. Without a firm commitment, the implementation of risk management will be constrained and may not be possible. Effective implementation of risk management in an organization is a “top down” process that encompasses the entire organization. Partial or pilot implementations should be avoided as they communicate a weak or tentative commitment to risk management that generally prevent it from becoming a part of the organization's culture and values.

The mandate and commitment to risk management is normally captured in a risk management policy. Such a policy may currently be implicit and unwritten, but in order to be effective it must be explicit and approved by senior management or the Board of Directors. Once a risk management policy has been developed and approved, compliance with the spirit and letter of the risk management policy by the management team is essential. It should also be

communicated to all staff and made available on an ongoing basis to existing and new employees.

When a policy has been developed and approved, the managers in the company should abide by it. If the owners or senior management make exceptions, then these exceptions become the rule and the policy soon becomes meaningless.

Example

The organization has a policy that all proposals for new projects are to be accompanied by a risk analysis. If senior management implements a new project without such an explicit risk analysis, staff will note that this is contrary to the policy and soon the policy will no longer have any effect.

A risk management policy should include:

- A commitment to consider risk in all decision making.
- A commitment to implement risk management in a way that gives effect to the 11 principles for effective risk management found in the standard.
- A clear statement of the objectives that are sought through the implementation of risk management and how the performance of risk management will be measured.
- A clear statement that the implementation of risk management will align fully with ISO 31000:2009.
- A statement regarding roles and responsibilities, especially for the individual or group that will monitor and review the implementation of risk management.
- A clear commitment that the resources (money and people) to implement risk management will be provided or specifically reallocated to deliver risk management tasks.

In a small organization, this can be recorded as a management decision and should be communicated to all staff.

To be effective, risk management must become a recognized and fully integrated element of decision-making in your organization, not a separate activity or an “add-on”. An effective test for the commitment to risk management is to evaluate the commitment in the risk management policy and determine

if it is: Specific; Measureable; Attainable; Results-based and Time-bound (SMART).

2.2 Setting objectives for implementing ISO 31000:2009

Do you have clear, measureable objectives for aligning your risk management with ISO 31000:2009?

- ☐ **Yes** → Go to next question and ensure that these are in writing and have been approved by senior management. They are normally found in the organization's risk management policy
- ☐ **No** → See guidance below

Clearly stating the objectives that you wish to achieve by making this change is critical to successful implementation because aligning your risk management with ISO 31000:2009 will require an investment of money, time and effort. Examples of objectives or expected benefits for implementing risk management are shown below. Monitoring the achievement of these objectives will provide a way to monitor progress.

The benefits of aligning your risk management with ISO 31000:2009 include: improved achievement of organizational objectives; greater stability in the face of a changing environment; an increased return on investment; greater coherence and alignment with the organization's goals and objectives. Understanding the objectives for implementing risk management will help the organization's managers to identify the level of investment that is appropriate to enable this transformation.

The objectives for implementing risk management should align with the organization's objectives. The objectives for risk management should clearly reflect that ISO 31000:2009 will be the framework for implementation and that the framework, process and definitions used in your organization will be based on ISO 31000:2009 and ISO Guide 73:2009. Reviewing the 31 risk assessment techniques that are set out in IEC 31010:2009 and choosing ones that best fit your needs, can be key to successful risk management. Annex [A.3](#) has examples of risk assessment techniques and guidance on how these can be used.

Risk management objectives can include:

- Completing a comprehensive identification and characterization of internal and external risks that have the capacity to materially impact on objectives.
- Establishing clear accountabilities for monitoring key risks and ensuring that changes in the internal and external environment are monitored and where these changes are a source of risk, that these risks are identified, assessed and treated.
- The achievement of core organizational objectives in a manner that is consistent with investment and market conditions and are not diminished by unforeseen or untreated risks.
- Identifying, monitoring and responding to business risks so that organizational targets and objectives are normally achieved.

The risk management objectives, in order to be effective, should be specific, approved by senior management and communicated to all employees.

2.3 Develop performance measures for risk management

Do you have specific, measurable and time-bound performance measures for risk management that are aligned with your organization's objectives?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

Risk management should be fully integrated into management and decision-making and never be seen as an end in itself, or an activity that is somehow different from managing the organization. Risk management should become one of the many corporate processes in the organization. As with other processes it is important to ensure that it achieves the desired performance targets, and that actions are taken on the performance information that has been gathered.

It is important to have measures that account for both *results* (performance) as well as *activities* (processes or inputs) and that the performance being measured is aligned with the organization's objectives.

Risk management measures that are based on inputs or activities, such as recording the number of risks identified, or workshops held, should be supplemented with results-based measures as described below.

Results-based measures for risk management include determining whether the desired outcome of a risk treatment has been achieved (i.e. a change in the consequence or likelihood levels of the risk). Other results-based measures include the degree to which managers indicate that they understand risk and use risk information when making decisions and whether they monitor the performance of the risk management framework. Other measures including the achievement of revenue, profit, growth or market-share objectives, are linked to the effective management of risk.

There are three categories of performance measures ⁴⁾:

- indicators of overall success (e.g. achievement of organizational outcomes),
- process indicators (e.g. completion of steps in risk management process, implementation of monitoring), and
- outcome indicators (e.g. implementation of planned treatment of risks, assessments of control effectiveness).

When you have identified specific, measurable and time-bound measures to assess the performance of risk management, this step is complete.

2.4 Internal and external stakeholders

Have you identified your internal and external stakeholders?

☐ **Yes** ➡ Go to next question

☐ **No** ➡ See guidance below

The term stakeholder is defined in Clause 2.13 of the standard as a “person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity” of the organization.

Stakeholder identification is an important process because communication with, and consultation of, stakeholders should be ongoing throughout the risk management process.

4) Based on SA/SNZ HB 436:2013 Table 3.

Internal stakeholders include the staff and management of the organization, as well as owners or shareholders. Often, key employees are able to identify persons or groups who are external stakeholders. External stakeholders can include regulators, customers, creditors, non-governmental organizations and others.

It is important to note that external stakeholders often identify themselves. They may be people who live near the organization or its operations or people whose lives are otherwise affected by the organization as it operates. When identifying stakeholders, it is important to identify the objectives that specific stakeholders or stakeholder groups have in regard to the organization and their relevant perceptions ⁵⁾. These perceptions can influence or colour the information that is provided by the organization and should be well understood if communications and consultations are to be effective.

External stakeholders include, but go beyond, clients of the organization, and may include suppliers, partners, banks, creditors, government regulators, non-government organizations, local population and the media.

2.5 Communicate risk management commitment to stakeholders

Have you communicated your organization's risk management commitment to internal and external stakeholders?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

Internal and external stakeholders (see Section [2.3](#) above) are key to every organization. As risk management is directed at improving the achievement of organizational objectives, it is critical that stakeholders are involved in risk management at every stage. By allowing stakeholders to participate in risk management, it is possible to avoid the errors that can occur if the organization attempts to guess the risks that may be important to the stakeholder rather

5) Additional analysis of risk and perception can be found in this book: The perception of risk. Risk, Society, and Policy series. Slovic, Paul (Ed) London, England: Earthscan Publications. (2000). 473 pp.

than gathering accurate information from the stakeholders themselves. This communication with stakeholders is a way of opening the ongoing communication and consultation that is a critical element of risk management as described in the standard.

Communication and consultation are processes that continue through all stages of risk management and should include reporting on the performance of the risk management function in reports prepared by the organization (e.g. Annual Reports).

Communication and consultation with stakeholders needs to be tailored. In some cases, information will need to be translated into a different language, in other cases there may be a need to remove or explain technical jargon.

Communication includes choosing the channels or pathways that are most appropriate, and while Internet, social media and email are effective for some groups, for others a different approach, like the distribution of printed materials, public meetings, interviews or media releases may be more effective.

3 Designing the framework for managing risk

3.1 Risk management framework

Are you clear what a risk management framework includes and how it operates?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

The purpose of a risk management **framework** is to enable effective implementation of the risk management **process**.

[Figure 3](#) identifies the relationship between the risk management framework and the risk management process. A detailed graphic setting out the risk management process used in ISO 31000:2009 is included as [Figure 4](#). A risk management **framework** is made up of two parts. The first is the organization's intent to manage risks and how it will be done. This part is often accomplished by a risk management policy. The second part of the framework identifies the resources available, the governance arrangements and management commitment that enable the effective implementation of the statement of intent, the risk management policy. This second part often consists of: tools; the capability to use them as a part of decision-making; arrangements to confirm that intentions have been satisfied; and an ability to continuously adapt, respond to change, and improve ⁶⁾.

6) Extracted from "Hearing over the cacophony", a paper delivered by G. Purdy to the RISKNZ conference in October 2014 and available from Broadleaf Capital International Inc.

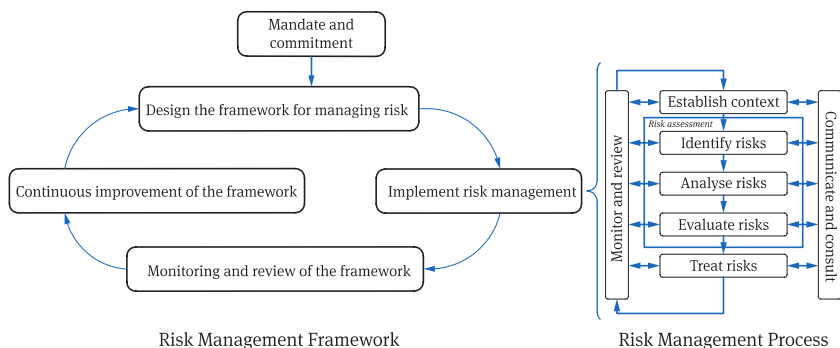


Figure 3 — The relationship between the framework and the process

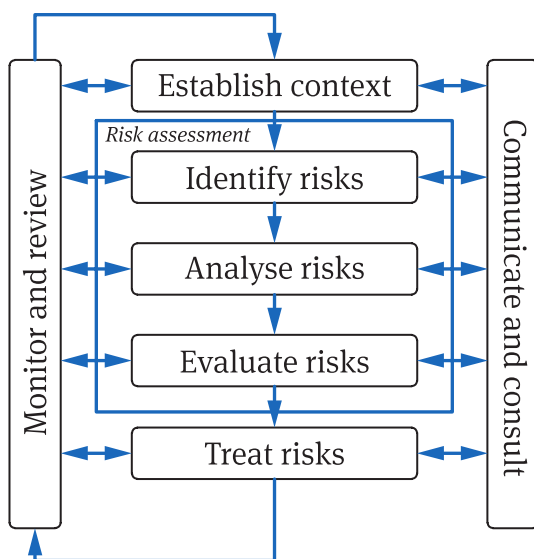


Figure 4 — The ISO 31000:2009 risk management process

The risk management framework may not be a specific single document. It will include a risk management policy and a series of commitments that are designed to ensure that risk management is fully integrated into the management of the organization. The elements of a risk management framework

should operate in an integrated and effective way to ensure that the risk management process is implemented for all decisions in the organization.

In some organizations, there is a clear list of risk management responsibilities for each senior manager, the manager for risk management (the individual or group that is charged with the oversight of the risk management function) as well as managers, other decision makers and employees. [Table 1](#), below, has been added in order to provide examples of risk management responsibilities at all levels of an organization. This table is simply a guide, and in accordance with Principle G that risk management is tailored, the management team should review this table and tailor it so that it aligns with the governance arrangements and culture of the organization.

Table 1 — Examples of assignment of risk management responsibilities

Position	Examples of risk management responsibilities
Chief Executive Officer	<ul style="list-style-type: none">• Identify and support the organization’s commitment to risk management.• Approve the risk management framework and risk management policy.• Set the objectives to be achieved by implementing risk management.• Approve the risk criteria.• Approve a mechanism that escalates risk within the organization in accordance with the organization’s risk tolerance.
Senior Managers	<ul style="list-style-type: none">• Integrate risk management into organizational strategy and into management frameworks.• Always consider risk information as an input to decision-making.• Provide managers and employees with clear information on the organization’s oversight of the risk management function.• Ensure that there is an effective risk management process and that the risk treatment plan is in place and monitored.

Table 1 (continued)

Position	Examples of risk management responsibilities
Managers	<ul style="list-style-type: none"> • Always consider risk information as an input to decision-making. • Support staff in developing an understanding of risk management.
Office of Risk Management Oversight	<ul style="list-style-type: none"> • Monitors and reviews the implementation of risk management in the organization in the context of quality assurance. • Supports management and staff by identifying appropriate and relevant risk management tools and training. • Provides quality assurance oversight of risk management practices and products.

The completeness of the risk management framework can be evaluated by preparing a table that identifies all the components of the framework, [Table 2](#), below, is an example. This table should also include the person or position that is accountable and how performance of the component will be measured. This table can serve as a valuable reference during the implementation of risk management and will ease the task of monitoring the implementation of risk management.

Table 2 — Risk management accountabilities and performance measures

Framework element	Accountability	Example of performance measures
Designing		
Risk management Commitment	Chief Executive Officer (CEO) and Board	An explicit commitment to implement risk management as a core value and to use it to inform decision-making and planning.
Risk Management Mandate (the authority to carry out an activity)	CEO and Board	A clear approved mandate that establishes a risk management function, describing both accountability and authority.
Risk Management Policy	CEO and Board	An approved Policy that clearly sets out the objectives for implementing risk management, the commitment of resources, and the performance measures.

Table 2 (continued)

Framework element	Accountability	Example of performance measures
Risk Management Objectives	CEO and Board	A clear statement of the objectives that the senior management team has set for the implementation of risk management, including how performance towards these objectives will be measured.
Establishing the Context	Risk manager accountable for oversight	A clear, dated statement of the context for risk management in the organization that includes all information considered for the External Context and the Internal Context.
Risk Criteria	Risk manager accountable for oversight to develop and CEO or Board to approve	Clear risk criteria that reflect the organization, its culture and risk attitude. Both risk criteria for impact (or consequences) and risk criteria for likelihood are required.
Accountability for Risk Management	Risk manager accountable for oversight to develop and CEO or Board to approve	Clear accountabilities at the Senior management, management and operational levels of the organization, including accountabilities for action, performance expectations and how performance will be recognized and responded to.
Implementing		
Integration	Risk manager accountable for oversight	Evidence that risk management is an input to decision-making at all levels of the organization.
Resources	to develop and CEO or Board to approve	A clear allocation of staff and funding to support the conduct of risk management and to provide staff with the training in risk management that aligns with their role in risk management.

Table 2 (continued)

Framework element	Accountability	Example of performance measures
Internal Communication and Reporting	Organizational communications function	Surveys, interviews, meetings or other assessments of internal stakeholders to ensure the messages (including results) that have been communicated internally have been clear and are understood. This evaluation will determine whether the communication has been effective and has provided internal stakeholders with a good understanding of how risk information is being used as an input to decision-making in the organization.
External Communication and Reporting		Surveys, interviews, meetings or other assessments of external stakeholders to ensure the messages (including results) that have been communicated internally have been clear and are understood. This evaluation will determine whether the communication has been effective and has provided external stakeholders with a good understanding of how risk information is being used as an input to decision-making in the organization.
Monitoring, Reviewing and Improving		
Monitoring	Risk manager accountable for oversight and managers to review and improve	Evidence confirming that the internal and external contexts are being monitored.
Reviewing		Evidence confirming that the monitoring reports are being reviewed to determine the effectiveness of risk management and the need to update risk information when the context changes.
Improving		Evidence that performance measures are being tracked and that improvements in the risk management process are being implemented in response to monitoring and review.

3.2 Compare your current risk management to ISO 31000:2009

Have you identified the differences between your current implementation of risk management and an implementation that is aligned with ISO 31000:2009 that clearly shows what changes will be required in order to align with ISO 31000:2009?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

As a first step, you should gather information on your current practices for risk management. If you are unsure what to look for, the documentation of the following practices should be analysed. The standard, in Clauses 3 and 4, identifies key aspects of risk management. An excellent outline for a review can be found in SA/SNZ/HB 436:2013 which has been used to develop the list below. To understand your implementation of risk management, analyse documents that identify:

- principles that guide risk management,
- any relevant policy,
- accountabilities,
- guidance on where and when risk management will be done and how the results will be used,
- risk management resources (including financial resources, people, training, tools, including software), and
- guidance on communication and reporting.

A “gap analysis” between these documents, where they exist and the guidance in the standard will form the basis for both the risk management framework (see Section [3.1](#)) and the risk management plan (see Section [4.4](#)).

As noted in ISO/TR 31004:2013⁷⁾, Clause 3.3.3.1, it is critical to compare and contrast the risk management policy, accountabilities for risk management, integration of risk management into organizational processes, resources allocated to facilitating and overseeing risk management as well as the communication and reporting mechanisms with the appropriate sub-sections of Clause 4.3 in the standard.

7) Guidance for the implementation of ISO 31000.

This analysis, when complete, will enable you to develop a risk management framework and a risk management plan that is tailored to your organization.

3.3 Risk management principles

Do you have a clear understanding of the 11 principles set down in Clause 3 of ISO 31000:2009?

- ☐ **Yes** → Go to next question
- ☐ **No** → See guidance below

The 11 principles of risk management that are included in Clause 3 of the standard provide both the rationale for managing risk and the attributes that risk management should have in order to be effective. They are intended to guide the implementation of risk management at every stage and provide tests (e.g. risk management is part of decision-making) that can be used to guide the implementation of risk management and also to monitor its effectiveness.

Evaluating your implementation of the 11 principles of risk management is a transparent and effective way of assessing whether your implementation of risk management is aligned with the standard.

Your implementation of risk management should actively pursue alignment with each of these principles on an ongoing basis. All aspects of the risk management framework and the risk management plan should be developed with these principles in mind.

The 11 principles are set out below; additional clarification is provided for each in the standard:

- a)** Risk management creates and protects value.
- b)** Risk management is an integral part of organizational processes.
- c)** Risk management is part of decision-making.
- d)** Risk management addresses uncertainty.
- e)** Risk management is systematic, structured and timely.
- f)** Risk management is based on the best available information.
- g)** Risk management is tailored.
- h)** Risk management takes human and cultural factors into account.

- i) Risk management is transparent and inclusive.
- j) Risk management is dynamic, iterative and responsive to change.
- k) Risk management facilitates continual improvement of the organization.

Detailed guidance on how each of these can be implemented can be found in Annex [B.1](#). As you move forward with the implementation of risk management, at each major stage, from establishing the commitment to designing the risk management framework and risk management plan, you should assess whether your implementation gives effect to these principles. A table or checklist that requires consideration of each principle at every critical stage will provide a clear and valuable way of ensuring that you are implementing the principles.

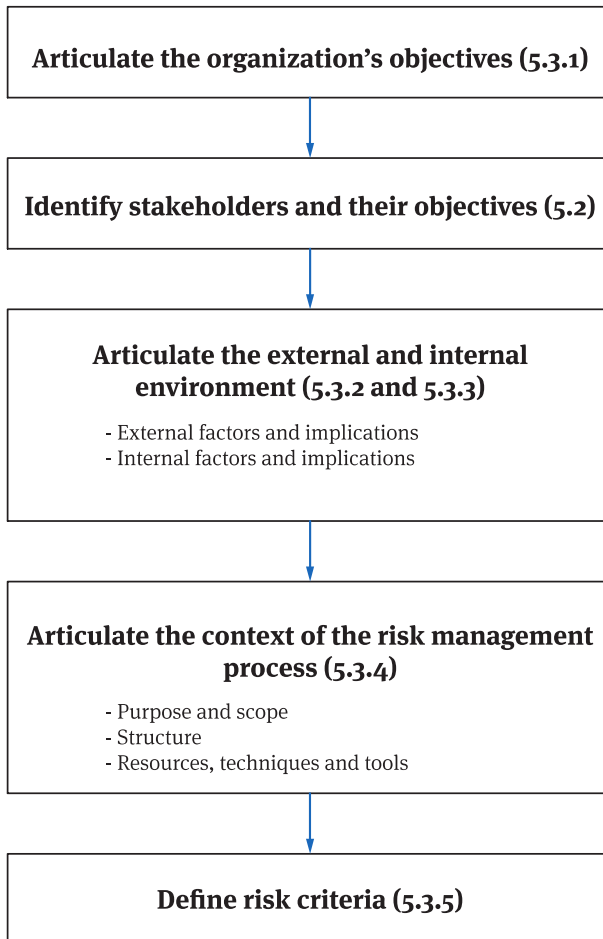
If you have an explicit and structured approach to risk management now, testing your current approach against these principles can serve as a first step in the analysis seeking to identify gaps that you will need to address in order to implement risk management that is aligned with ISO 31000:2009.

3.4 Understand the internal and external contexts of your organization

Do you have clear, accurate and current information about the internal and external contexts of your organization?

- ☐ **Yes** → Go to next question
- ☐ **No** → See guidance below

The standard, in Clause 2.8 defines context as ‘the [internal or external] environment in which the organization seeks to achieve its objectives’. The context is not **ALL** elements of the organization’s environment, only those that could influence the organization’s achievement of its objectives. [Figure 5](#), below clearly identifies how to establish the context for your organization. The numbers in the figure refer to the relevant Clause numbers in ISO 31000:2009.



SA/SNZ HB 436:2013 Figure 3
Establishing the Context
(Clauses of Standard in parentheses)

Figure 5 — Establishing the context
(Reproduced with permission from Grant Purdy)

The handbook, SA/SNZ/HB 436:2013 suggests that questions like ‘What constrains [the organization]?’ or ‘What enables [the organization]?’ can elicit the required contextual information from informed internal stakeholders. Certain