

a practical guide

for SMEs



ISO 31000

Risk management



ITC



a practical guide
for SMEs

ISO 31000

Risk management



ITC



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.

Contents

Page

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 framework	73
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 management	79
6.2	Continual improvement of the framework	81
6.3	Continual improvement of the implementation of the process	84
	Annex A – Risk management techniques for SMEs	87
	Annex B – Specific guidance for SMEs	105
	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

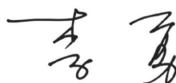
their objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment.

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⁾.

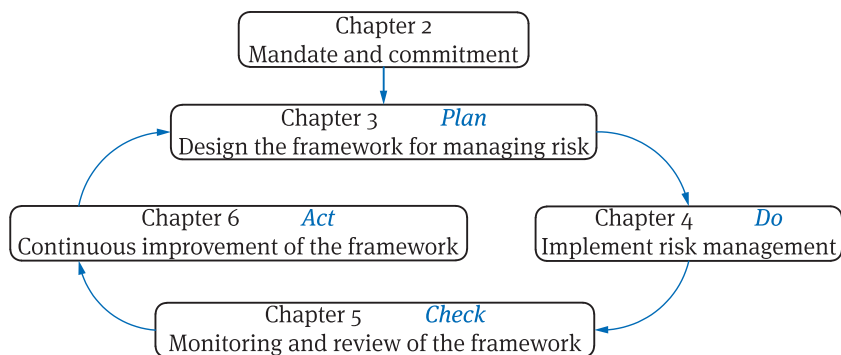


Figure 1 – The structure of this guide

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 time ³⁾.

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.

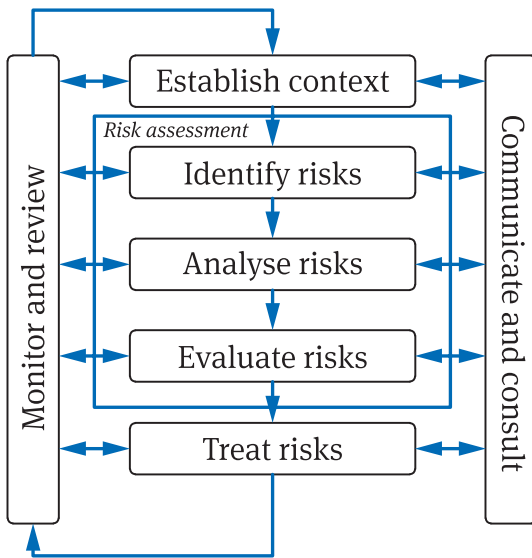


Figure 2 – The ISO 31000:2009 risk management process

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.