

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 review73

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

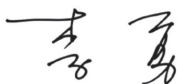
their objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment.

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⁾.

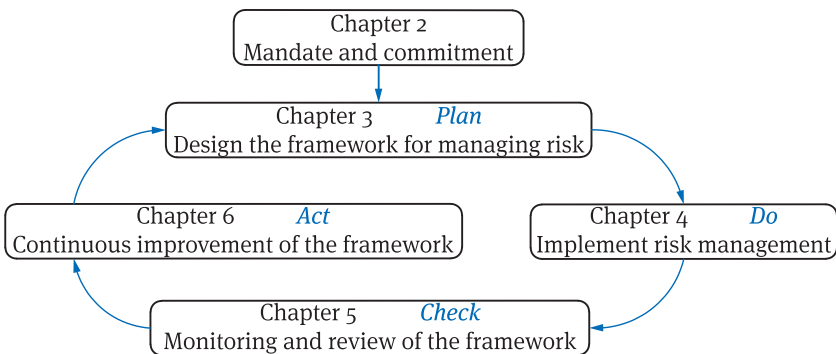


Figure 1 – The structure of this guide

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 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.

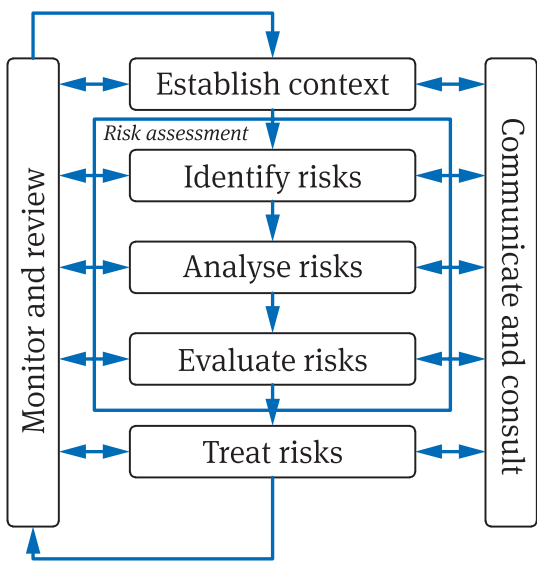


Figure 2 – The ISO 31000:2009 risk management process

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.

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.

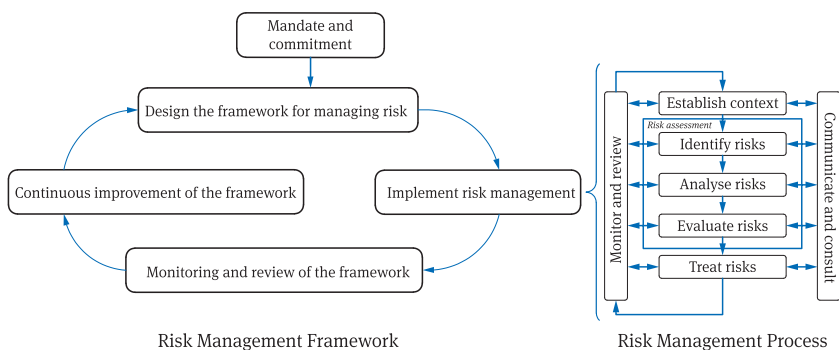


Figure 3 – The relationship between the framework and the process

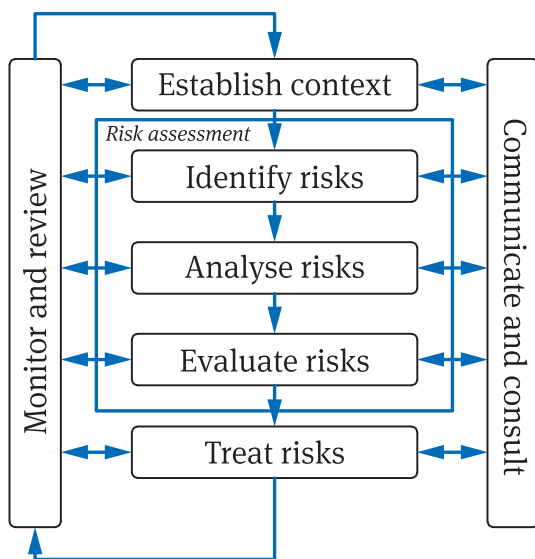


Figure 4 – The ISO 31000:2009 risk management process

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 to develop and CEO or Board to approve	Evidence that risk management is an input to decision-making at all levels of the organization.
Resources		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.

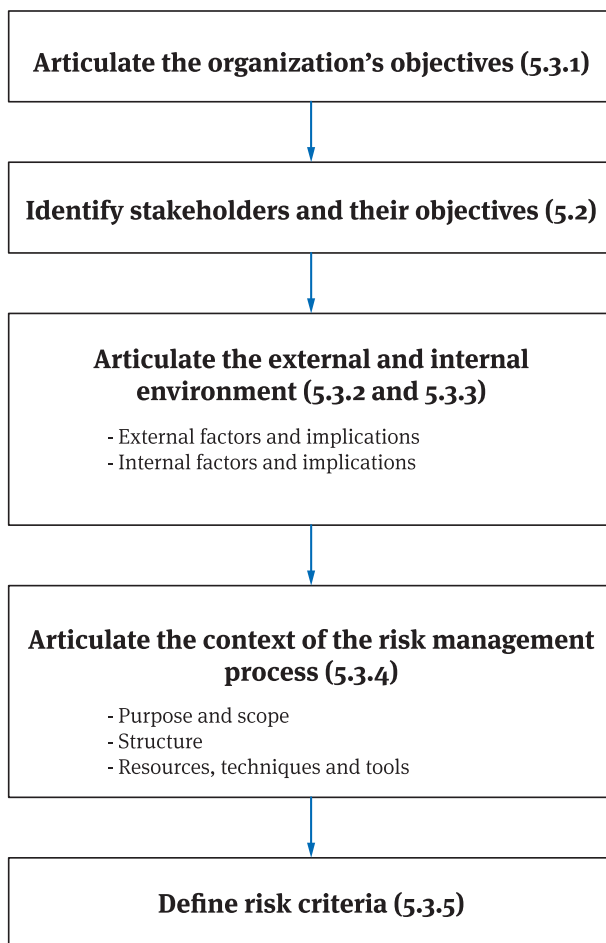
If you have an explicit and structured approach to risk management now, testing your current approach against these principles can serve as a first step in the analysis seeking to identify gaps that you will need to address in order to implement risk management that is aligned with ISO 31000:2009.

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

fairly common prompt-based analyses like identifying strengths, weaknesses, opportunities and threats, also known as a SWOT analysis and identifying the political, economic, social and technological, environmental and legal aspects of the context (known as PESTEL) can serve as a useful first step in identifying the context.

Capturing the context accurately and completely is critical to implementing risk management effectively.

Establishing the context is the “first step” in the ISO 31000:2009 risk management process and one that sets the stage for all subsequent steps.

The standard in Clause 4.3.1 states that the **external** context may include but is not limited to:

- the social, cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment whether international, national regional or local,
- key risk sources and trends that impact on the objectives of the organization, and
- relationships with, and perceptions and values of, external stakeholders.

Questions like the following, from SA/SNZ/HB 436:2013, can be used to identify relevant aspects of the internal and external context:

- 1) What will constrain us from reaching our objectives?
- 2) What will enable us to realize our objectives?
- 3) What will we be dependent on?
- 4) What changes could occur that would impact on our ability to achieve our objectives?

The standard also identifies that the **internal** context will include information on the internal governance of the organization, including its structure, roles and responsibilities, capacity and capabilities, internal systems, internal stakeholders and their characteristics, and the organization’s culture.

A detailed summary of the context for the risk management process should be captured in a specific document. This document, called a “statement of context”⁸⁾, should be provided to senior management for approval and retained for

8) Section 5.3.6 of SA/SNZ HB 436:2013.

the purposes of monitoring and review. This detailed summary of the internal and external contexts can be used as a reference for the ongoing monitoring and review of risk management. When an element of the context (e.g. for example tariffs or taxes) changes, this should be identified by the risk monitoring process so that risks that are relevant to this change can be updated.

The “statement of context”, should contain information on:

- Organizational objectives and success measures.
- Important factors within the internal and external environments, including the velocity at which change can be expected.
- Relevant stakeholders and their objectives.
- Risk criteria.
- Documents and people consulted in establishing the context.
- The date the statement was developed and recorded, the author or authors, and the scope and setting of the particular risk management activity.
- The structure for the risk management activity.
- The resources, techniques and tools needed for the risk management activity.

While the preparation of a statement of context may be completed by a contractor, it is critical that internal and external stakeholders are involved and that the final information is reviewed and approved by management of the organization.

3.5 Risk management policy

Do you know how to develop a risk management policy?

☐ **Yes** ➞ Go to next question

☐ **No** ➞ See guidance below

A policy is a statement that guides decision-making. The Webster dictionary defines policy as “a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions”. A policy regarding payment may be “the organization will pay all outstanding invoices within 20 days of receipt”. Policies can be simple

and straightforward and should provide clear guidance when the condition relating to the policy arises, in this case, payment.

A risk management policy is a statement of intent regarding where and how risk management will be implemented in the organization. If you have an existing risk management policy you will need to transform it so that it aligns with ISO 31000:2009. This transformation should be based on making a comparison between your current policy and the elements described in this chapter. This analysis of gaps and overlaps can guide the development of a risk management policy that is aligned with ISO 31000:2009. This analysis can identify how your organization can transition from your current implementation of risk management to one that aligns with the standard.

The standard, in Clause 4.3.2 indicates that the risk management policy should clearly state the organization's objectives for risk management.

There are six areas that can be addressed in this policy. These are:

- 1) people, skills, experience and competence,
- 2) resources needed for each step of the risk management process,
- 3) the organization's processes, methods and tools to be used for managing risk,
- 4) documented processes and procedures,
- 5) information and knowledge management systems, and
- 6) training programmes.

The risk management policy should also be aligned with the culture of your organization and its environment (see Section [3.4](#) of this guide relating to internal and external contexts). To align with the culture, review the internal context of the organization. Decide if your organization has a culture where change is a constant and decisions must be made quickly and with little direct guidance or one where there are clear written policies to cover most aspects of the operation and which are implemented consistently across the organization. In highly regulated organizations, there may be a comprehensive list of policies that guide such things as investment, recruitment, disclosure, compliance with legislation, regulations and policies and other matters identified by statute.

The risk management policy should reflect legal and regulatory obligations and clearly assign responsibilities to your staff at the appropriate levels in

your organization (normally those with decision-making power). The policy should also clearly identify who is responsible for developing and obtaining approval for the organization's risk criteria (see Section [3.8](#)).

The risk management policy should also make reference to the human and financial resources that will be made available and as well the objectives and performance expectations for risk management in the organization.

There should also be a clear commitment to review and improve the risk management policy and framework periodically and in response to an event or change in circumstances. The risk management policy should be approved by the Board and/or the Chief Executive Officer and be communicated to all staff.

As noted above, to align with the objectives for implementing risk management, the risk management policy should clearly reflect that ISO 31000:2009 will be the framework for the implementation and that the framework, process and definitions used in your organization will align with ISO 31000:2009 and use the definitions found in ISO Guide 73:2009. The risk management policy should also commit to using risk assessment techniques that are set out in IEC 31010:2009.

3.6 Alignment between risk management policy and the organization

Are you clear on how the risk management policy should align with the organization, its characteristics and culture?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

The objective of this step is to ensure that the risk management policy is drafted so that its implementation will lead to risk management becoming a part of the organization. The standard includes reference to these characteristics in its discussion of context (Clause 4.3.1) where it implies that the risk management policy should be aligned with the organization's social, cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment.

It should also be aligned with the perceptions and values of stakeholders.

There is no quantitative test that can be conducted to evaluate this. A qualitative evaluation can be conducted to determine whether all staff understand the risk management policy and believe that the policy is relevant and attainable. In its essence, it is an assessment of whether or not the policy “fits” the organization. If it does not fit the organization, it should be revised so that it does.

Example of non-alignment

A primary objective of the company is to implement strong and effective controls over risks that can have negative impacts on the environment.

The company’s purchase, installation and use of fuel storage tanks that do not have adequate safeguards to prevent leaks and spills would be an activity that is out of alignment with business objectives. In order to align with its business objectives, the company needs a new control (e.g. a policy or specific procedure) over the procurement process that supports the objective of having effective controls to protect the environment.

3.7 Risk attitude

Have you identified your organization’s risk attitude in a way that allows you to decide whether risks will require additional treatment?

☐ **Yes** ➡ Go to next question

☐ **No** ➡ See guidance below

Risk attitude is defined in Clause 2.5 of the standard as an “organization’s approach to assess, and eventually pursue, retain, take or turn away from risk”. A related term, “risk tolerance” is defined in ISO Guide 73:2009 as “organization’s or stakeholder’s readiness to bear the risk **after risk treatment** in order to achieve its objectives”. The important objective is to identify when the risk will be accepted, treated, or avoided.

Table 3 — Examples of pursue, retain or turn away from risk

Action	Example
Pursue, take	<ul style="list-style-type: none">• Pursue an uncertainty that would have a positive impact on the achievement of objectives. A decision is taken that the magnitude of the potential positive impact on objectives is sufficient to warrant pursuit of the risk.• Where there is an objective of operating a profitable retail store, an example would be opening a store where information suggests that there is sufficient positive uncertainty of a market for the goods that an adequate market exists to support a retail store. The entrepreneur opens a store to pursue the market-related risk (uncertainty).
Retain	<ul style="list-style-type: none">• Decide that the magnitude of the risk is within the risk criteria (i.e. tolerable) and proceed without additional risk treatment. Accept the risk.• An example is a farmer who has an objective of producing a crop to realize a profit. Retaining the risk would occur if there is uncertainty regarding whether there will be sufficient rain in the coming summer to produce a crop, and a farmer decides to accept or retain that risk and plant seeds, accepting the risk that the plants may not produce a crop if there is insufficient rain.
Turn away	<ul style="list-style-type: none">• Decide that the magnitude of the risk is outside the risk criteria (i.e. intolerable) and stop conducting the activity associated with the risk.• An example would be a farmer considering raising crops that have a high value and that may be stolen before they can be harvested. Turning away would be choosing to produce lower valued crops where the likelihood of theft before harvest is lower.

The organization's risk attitude forms the basis for the development of risk criteria and will assist the organization to determine what risk levels will be "retained", that is, accepted without further treatment or treated or modified so that they are within the organization's risk criteria. The risk attitude identifies the risk level (or severity) that will require action to modify the consequences or likelihood of the risk, or to avoid the risk entirely if it cannot be modified so that, after risk treatment, it is within the risk criteria.

3.8 Risk criteria

Have you developed clear risk criteria that can be used to determine and assess the magnitude of risk and judge its significance to organizational objectives?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

Webster's dictionary defines *criteria* as “standards on which a judgment or decision may be based”⁹⁾. Risk criteria are used to evaluate the significance of risk.

Criteria articulate the organization's objectives, values and resources as well as its legal and regulatory obligations. They should be consistent with the risk management policy described earlier in this document. The standard describes how to define risk criteria in Clause 5.3.5 and states that risk criteria should include the following:

- the nature and types of causes and consequences that can occur and how they will be measured,
- how likelihood will be defined,
- the timeframe(s) of the likelihood and/or consequence(s),
- how the level of risk is to be determined,
- the views of stakeholders,
- the level at which risk becomes acceptable or tolerable, and
- whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

Risk criteria are used in two ways. The first is to determine the significance of risks. The second is to provide the basis for comparisons of risk level (or severity) across the entire organization and also through time. In order for managers to make consistent decisions on risk treatment it is important that the determinations of risk severity are based on common, clear and approved criteria. They determine the significance of the risk to the organization.

9) This is adapted from the definition of “criterion”, the singular of the term.

The handbook SA/SNZ/HB 436:2013 sets out the three critical characteristics that risk criteria should include. These are:

- 1) The method(s) to be used to express and measure the consequence and likelihood (whether qualitative or quantitative).
- 2) The method(s) to be used to combine consequences and their likelihoods and then to express the resulting level of risk.
- 3) The organization's internal rules for accepting (or tolerating) particular risks as well as risk in the aggregate.

Developing risk criteria is best handled with the assistance of an experienced expert in risk management. It is a complex step and one that is critical to implementing risk management so that it is reliable and contributes to improving the achievement of objectives. SA/SNZ/HB 436:2013 makes the important observation that “combining [consequence and likelihood assessments] by multiplying them will produce unreliable or illusory results”. [Table 4](#) has been included as an example of how to determine the severity or magnitude of a risk after the impact and likelihood have been determined.

Example

If risk severity is determined by multiplying likelihood by impact, illusory results can occur. An example is the condition where a rare but catastrophic risk (Impact 5, likelihood 1) is of the same significance to the organization as a trivial risk that is highly likely (impact 1, likelihood 5). The product of each calculation is 5 creating the illusion that a catastrophic event that is considered to be rare is of the same significance as a trivial event that is almost certain to occur. The first risk can destroy the organization, the second risk has no impact at all.

Appendix C of SA/SNZ/HB 436:2013 provides helpful advice on how to combine the consequence and likelihood assessments. One of the possible methods is a table that describes the risk severity based on the combination of consequence and impact, as shown in [Table 4](#).

Table 4 — Example of a risk severity matrix

C O N S E Q U E N C E	5 (highest)	Very High	Extreme	Extreme	Extreme	Extreme
	4	High	Very High	Very High	Extreme	Extreme
	3	Moderate	High	High	Very High	Very High
	2	Low	Low	Moderate	Moderate	Moderate
	1 (lowest)	Low	Low	Low	Low	Low
		1 (lowest)	2	3	4	5 (highest)
	Likelihood					

Decisions regarding risk treatment can be based on these risk severity determinations which can be used to identify the urgency for action as well as what level of management authority is required in order to decide to accept a specific risk severity.

4 Implementing risk management

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

Do you have a good understanding of your organization's capability ¹⁰⁾, capacity ¹¹⁾ and culture ¹²⁾ with respect to risk?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

This step is directed at obtaining a good understanding of your organization's "readiness" for risk management. This step is included so that the risk management framework can be designed to integrate with your organization's culture. This step will also help you to identify areas where additional effort may be required in order for risk management to be successful.

Understanding the nature of your organization will assist you in identifying the most effective path to implementing risk management. Some organizations have staff with the training and experience to implement risk management for the organization. These experienced staff may be assigned to specific aspects of the organization's business, for example financing, market development, or

10) The definition of capability is "the quality or state of being capable" and usually relates to specialized training or experience.

11) The definition of capacity is "the potential for ... accommodating" and usually relates matching demand with available resources, i.e. the number of people available for a task.

12) The definition of culture is "the integrated pattern of human knowledge, belief and behaviour" i.e. what would be accepted and implemented by your managers and staff.

stakeholder relations. If people with these skills and experience are available in the organization, it is important to determine if you can expand the scope of their responsibilities to include risk management for the organization as a whole.

If you do not have staff with risk management skills and experience, Section [4.5](#) of this document describes putting the resources in place to manage risk. Options include training employees, retaining specialists from outside the organization or a mix of these strategies.

The culture of an organization can diminish or enhance its ability to implement risk management. An organization's culture reflects the attitudes of its employees and the way that they respond to information. Organizations with clear accountabilities and good internal communication often have a culture that is receptive to the implementation of risk management. Cultural aspects that can be seen as supportive of risk management include a high level of coherence within the organization, where all staff understand and are working towards the achievement of the organization's objectives. A supportive culture is one where risks that are identified are quickly addressed and where management is prepared to accept and investigate risks that they are not familiar with or risks that indicate that management may have made errors. Another supportive aspect of culture is a commitment to continuous or ongoing improvement of the achievement of organizational objectives.

Cultures where there is intense individual competition (e.g. an “us versus them” culture) or where findings that are not aligned with expectations (i.e. “bad news”) are suppressed will hinder the implementation of effective risk management. In these cases, the culture itself may be a source of risk. The assessment of your organization's capability, capacity and culture is an important input to the development of your risk management framework and risk management plan and may help you to decide whether to retain outside experts to enable the initial implementation.

4.2 Planning the transition to ISO 31000:2009

Do you have a plan to transition your current risk management framework to one that is aligned with ISO 31000:2009?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

The work in Chapter 3 of this document and the response to the question in Section 4.1 have provided you with detailed information on:

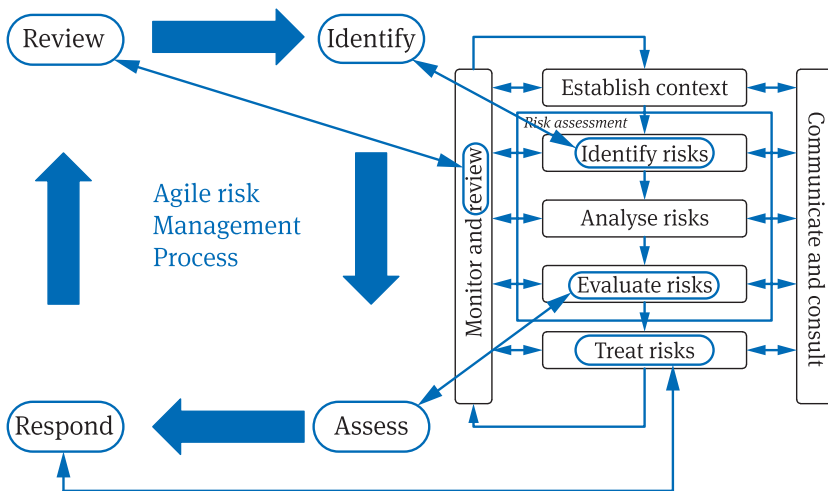
- The elements of your current approach to risk management that can be **retained without change**.
- The elements of your current approach to risk management that will **need modification** in order to align with ISO 31000:2009.
- The elements of your current approach to risk management that will need to **be stopped**.

This transition should follow the same course as any well-planned business transformation. The transition plan should identify clear steps from the current state to one where ISO 31000:2009 is fully implemented. This plan should have performance measures, clear accountability for each element of the plan, a budget and most importantly the clear support of senior management.

The plan should include a clear identification of the objectives of this transformation and describe the attributes of the organization that have been improved by the implementation of ISO 31000:2009. In many organizations, approaches such as tables, registers or Gantt Charts¹³⁾ provide a way to track the implementation and to identify when problems with the transition are arising. There is an emerging interest in newly described methodologies with specialized terminology (e.g. Agile, Scrum).

These approaches often mask the value of simplicity and clarity, in helping an organization to manage its risks effectively. The methodology for “Agile”, as shown in the Figure 6 below, is simply a derivation of the risk management process set down in ISO 31000:2009. It is easier and simpler to use ISO 31000:2009 as it has been written.

13) [Wallace Clark](#) and [Henry Gantt](#) (1922): The Gantt chart, a working tool of management. New York, Ronald Press.



**Figure 6 — Contrast agile risk management process¹⁴⁾
with ISO 31000:2009**

The transition of your risk management so that it aligns with the standard is a project and the best practices of project management will apply. Implementing risk management leads to a high level of alignment with the organization's objectives. It is a cultural change that will require behaviour changes especially around decision-making. Your plan should account for the current culture of your organization and their readiness for the changes that are proposed.

Risk management should be viewed as central to management of the organization. The risks of transition should be managed using the process set down in Clause 5 of the standard. There should be a plan to manage the risks of transition, including performance measures, specific milestones and remedial actions that will be taken when milestones are not achieved.

Support from the organization's senior managers is essential and is demonstrated not only by approving the plan, but also by implementing all aspects of the risk management policy in their priority setting and decision-making.

¹⁴⁾ <https://www.scrumalliance.org/community/articles/2014/april/risk-and-issue-management-in-scrum-process>.

Guidance on how to transition your current risk management so that it aligns with ISO 31000:2009 is provided in Annex [B.2](#).

4.3 Implementing the risk management framework

[Figure 7](#) describes the risk management framework in the standard. Have you developed a comprehensive and effective way to implement your risk management framework?

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

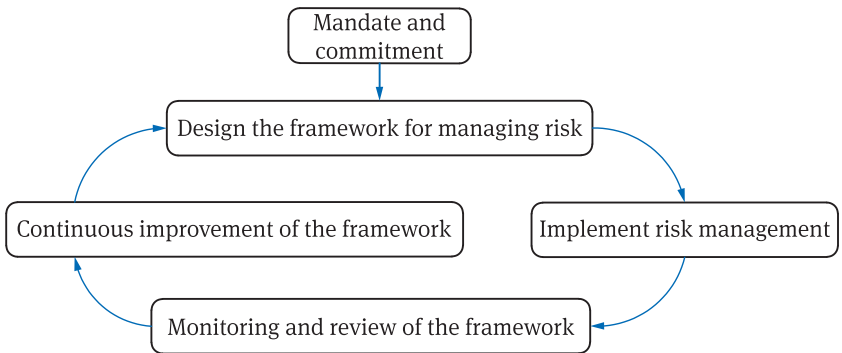


Figure 7 — The risk management framework from ISO 31000:2009

To implement risk management effectively, it is critical that the risk management implementation plan is executed properly. Clause 4.4.1 of the standard identifies six steps that should be followed. These are:

- 1) define the appropriate timing and strategy for implementing the framework,
- 2) apply the risk management policy and process to the organizational processes ¹⁵⁾,

15) An example is, if the risk management policy requires that risk be explicitly considered in decision-making, then documents outlining decision-making processes should explicitly reflect this requirement.

- 3) comply with legal and regulatory requirements,
- 4) ensure that decision-making, including the development and setting of objectives, is aligned with the outcomes of risk management processes,
- 5) hold information and training sessions, and
- 6) communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.

In order to implement the risk management framework so that it is fully integrated into the organization, it is necessary to act on the information developed in Section 3.6. The implementation of the risk management framework should build on existing management framework, governance arrangements and all planning and priority-setting processes and procedures.

The handbook SA/SNZ/HB 436:2013 has extensive guidance on implementing the framework and includes two detailed appendices (Appendices A and D) to explicitly address transformation and integration. The following paragraph from that handbook provides a helpful glimpse of how the framework should relate to the organization.

*“Because risk arises when the organization makes, and acts on decisions, implementation of the framework needs to take into account where and when, in the organization’s activities, decisions are actually made and acted on. In that way, appropriate aspects of the framework (such as training of the decision makers and the design of each decision making method) can be incorporated at those points.”*¹⁶⁾

The implementation of the risk management framework should result in the organization applying the ISO 31000:2009 risk management processes for all decision-making. The graphic describing the risk management process is shown in Figure 8. The relationship between the risk management framework and process is shown in Figure 9 and explained in Section 4.4.

16) SA/SNZ HB 436:2013 Clause 4.4.1.

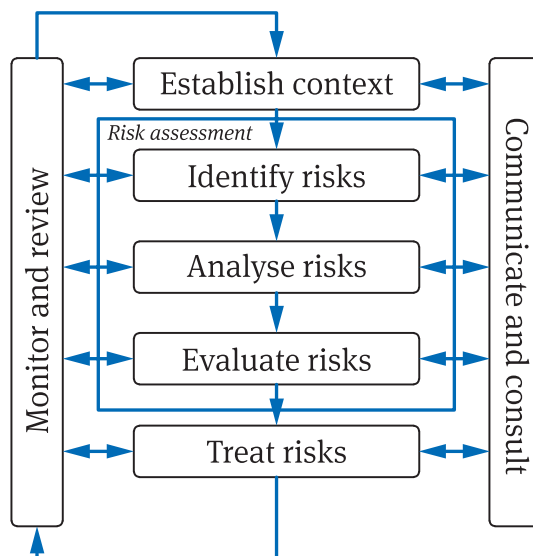


Figure 8 – The risk management process from Clause 5 of ISO 31000:2009

4.4 The risk management plan

Do you have a specific plan for the implementation of risk management on an ongoing basis that is aligned with your objectives and risk management framework?

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

The standard defines a risk management plan as the “scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk”. The standard includes a specific note that the plan typically includes procedures, practices, the assignment of responsibilities, and the sequence and timing of activities. The risk management plan should implement the risk management process in Clause 5 of the standard. The relationship between the framework and the process is shown in [Figure 9](#) below.

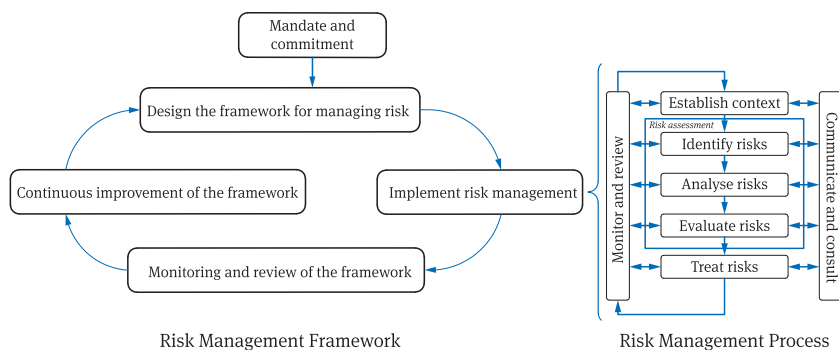


Figure 9 – Relationship between framework and process

The risk management plan will go into effect after you have transitioned the risk management practices in your organization so that they align with ISO 31000:2009¹⁷⁾. The risk management plan specifies how risk management will be implemented on an ongoing basis when the transition is complete.

Clause 4.3.4 of the standard provides a brief summary that indicates that risk management should be integrated into practices and processes in a way that is relevant, effective and efficient. The risk management plan should ensure that the risk management policy is implemented and that risk management forms an integral part of all decision-making.

The process used to develop the risk management plan needs to include inputs from internal and external stakeholders in order to be successful. Internal stakeholders are essential to implementing risk management and external stakeholders need to understand how risks will be managed.

Communication with external stakeholders should identify the objectives of the plan and the process by which it will be implemented. Internal stakeholders should be invited to provide guidance on how the plan can leverage the culture and practices currently in place (see Section 4.1) and also provide information on the pace of change that can be accommodated with the current capacity and organizational culture.

17) This alignment with ISO 31000:2009 is the sole objective of this guide.

The risk management plan should be designed so that the objectives set for the transformation to ISO 31000:2009 that are described in Section [2.2](#) will be achieved. Progress towards the achievement of these objectives should be monitored as a part of the plan.

4.5 Resources to implement the risk management plan

Have you identified and made available the financial and human resource requirements to support implementation of ISO 31000:2009?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

An appropriate commitment of resources is essential to implement risk management. Clause 4.3.5 in the standard identifies six areas for consideration when allocating resources to implement ISO 31000:2009. The six areas for consideration are:

- 1) people, skills, experience and competence,
- 2) resources (e.g. financial and human) needed for each step of the risk management process,
- 3) the organization's risk processes, methods and tools to be used for managing risk,
- 4) documented processes and procedures,
- 5) information and knowledge management systems, and
- 6) training programs.

These resources can be supported by the preparation and use of checklists (see Annex [B.5](#) of this guide). Internal audit (if such a function exists as some SMEs contract out this activity) reviews controls and their effectiveness. While internal audit can identify areas where the execution of controls is weak, it is not a tool that can replace ongoing monitoring and review. The ongoing monitoring of the organization's internal and external contexts to determine when to review and update risk lists is a best practice. Adequately resourcing risk management includes establishing a monitoring function to ensure that risk management works effectively.

There are two distinct steps in aligning your risk management with ISO 31000:2009. The first step is to transition from your existing methods, to approaches that are aligned with ISO 31000:2009. This will include the development, approval and communication of a Risk Management Framework as well as the clarification of risk management responsibilities for all staff.

The second step in aligning your risk management with ISO 31000:2009 will be to ensure that it is functioning effectively, delivering the objectives sought by management, and responding to changes in context as they occur.

In both cases (transformation and ongoing implementation), there will be costs to the organization in terms of staff and time. These costs should be identified to senior management and their agreement to provide these resources should be recognized in the risk management framework. When risk management becomes a fully integrated part of the organization's culture, these costs will no longer be explicit, but rather will be included as a normal management cost.

An approach that many organizations have found to be effective for aligning with ISO 31000:2009 is the use of experienced experts to manage this realignment. In order to implement a self-sustaining, internal, risk management capability, staff from the organization should work closely with the expert implementation team.

Regardless of the size and complexity of the organization, a single person or group should be charged with the responsibility of monitoring and reviewing the implementation of risk management. Details are provided in Sections [5.1](#) and [5.2](#). It is important to ensure that risk management practices do not degrade and become implemented without attention to their effectiveness. Such routine or habitual implementation will make risk management a “tick box” activity. If this occurs, the effectiveness of risk management becomes severely diminished as processes that are not well understood are implemented as an obligation, rather than as a business critical function.

Depending on the size and complexity of the organization, this central role for risk management can be assigned to one person or to a group. A critical success factor is the skill level of the individual or individuals involved and their ability to continue to tailor the implementation of risk management so that it remains a relevant and valued input to decision-making.

4.6 Establishing the context of the risk management process

[Figure 10](#) shows where in the risk management process that the context is established. Have you established the context for your risk management?

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

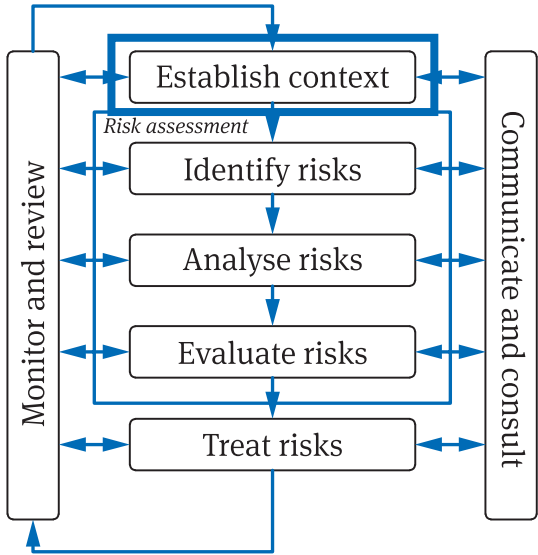


Figure 10 — The ISO 31000:2009 risk management process — Context

While it is critical to establish the context for the risk management framework, it is also critical to establish the context for each implementation of the risk management process. The risk management process may be implemented across the organization, on major activities, service lines or product groups. It may also be used to assist a project manager who is implementing a small-scale project to support the organization’s goals.

Information on the context for the organization is described in Section [3.4](#). It is important to establish the context for the risk management process each time it is implemented. The context for the risk management process acts as

a control to ensure that the risk management activities remain relevant to the context throughout the process. Many of the parameters of context that have been considered for the organization are considered in greater detail when establishing the context for the risk management process.

The summary of the organization's internal and external contexts captured in Section 3.4 should be reviewed to determine the context for the risk management process. Clause 5.3.4 of the standard states that context of the risk management process includes defining:

- the goals and objectives of the risk management activities,
- responsibilities for and within the risk management process,
- the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions,
- a particular activity, process, function, project, product, service or asset in terms of time and location that will be included,
- the relationships between a particular project, process or activity and other projects, processes or activities of the organization,
- the risk assessment methodologies,
- the way performance and effectiveness is evaluated in the management of risk, and by:
 - identifying and specifying the decisions that have to be made, and
 - identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.

In line with the practice described in Section 3.4, a **statement of context** should be prepared for each application of the risk management process. This statement of context should accompany any reporting of results so that the risk information that is developed can be seen in the context in which it was prepared. Risks to one area, function or project may not apply to other areas of your organization. Having a clear, written statement of context will facilitate the identification of risks and the development of effective risk treatments.

4.7 Risk management methodologies

[Figure 11](#) shows where in the risk management process, specific methodologies are required. Have you decided on a methodology to conduct risk identification, risk analysis, risk evaluation and risk treatment?

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

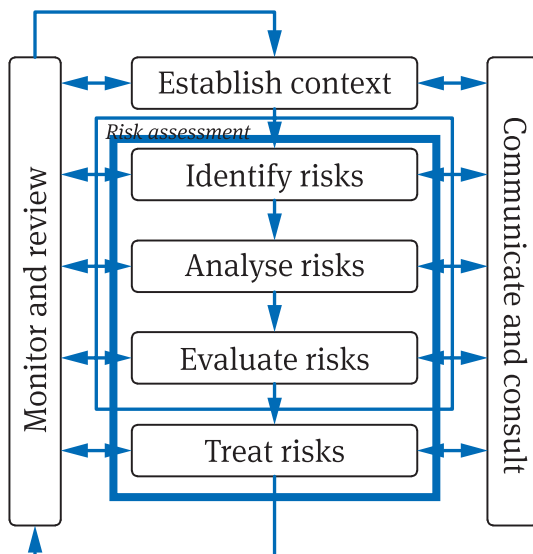


Figure 11 — The ISO 31000:2009 risk management process — Methodologies

Once the context for risk management has been established, the next step is risk assessment, which includes three separate components. These are outlined below.

Risk identification

Risk identification is a critical step in risk management, as risks that are not identified will be omitted from consideration at all subsequent steps. Annex [A.3](#) of this document analyses several risk assessment techniques that can be

used and explains in detail how four of these can be used by an SME for risk identification.

The standard provides clear guidance on risk identification in Clause 5.4.2 where it clearly states, “The aim [of risk identification] is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.”

A good starting point is to conduct a review of the external and internal contexts information. The contexts should include information on uncertainties that can impact on the achievement of objectives. This initial step can be supplemented by a review of studies, evaluations, and audits. In some cases, reports on or investigations of “near hits” (also called “near misses” or “close calls”) can also provide important information on risks to the organization.

The review of documents is usually followed by a series of interviews. Interviewees are drawn from all levels of the organization. The interviews should have “open ended” questions that allow the interviewee to describe the key uncertainties; special efforts should be made to avoid leading the discussion or suggesting what the risks might be. In order for risk identification to be effective, it should be systematic; based on the best available information; collaborative, and properly recorded.

For each risk there should be clear information which identifies: the objective or objectives affected by the risk; the context for the risk and how this context relates to the context of the organization; the sources or conditions which give rise to conditions where a risk event can occur; the potential consequences of an event resulting from this risk; the current controls which are in place to reduce either the likelihood or the consequences of the risk; and a brief summary which links potential consequences of the risk to effects on the organization’s objectives.

A review of the foregoing should assist you in identifying a methodology for risk identification that is suited to the circumstances in your organization.

Additional and more specific guidance on risk identification techniques can be found in Annex A.3.¹⁸⁾

18) SA/SNZ HB 89:2012 provides a high-level overview of 30 risk assessment techniques including the four described in Annex A.3.

Risk analysis

Risk analysis is described in Clause 5.4.3 of the standard. The objective of risk analysis is to develop an understanding of the risk. The method of assessing the consequences of the risk and the likelihood of those consequences occurring is described in the risk management framework. The standard has an accompanying methodology standard, IEC 31010:2009, *Risk management – Risk assessment techniques*. The most common approach to assessing the level of risk (which may be identified as severity) is covered in Clause 5.3.3 of IEC 31010:2009, consequence analysis. Clause 5.3.4, describes likelihood analysis and probability estimation.

The ways in which consequence and likelihood can be combined to determine the severity will normally be addressed in your risk management framework. This will include the methodology for conducting the assessment. One approach that provides useful information is the use of a workshop with the participation of knowledgeable internal stakeholders from both the management and operational or delivery ranks of the organization. You will need to determine the scales (i.e. criteria) used to assess consequence and likelihood. There are four types of scales that can be used. [Table 5](#) below has been extracted from SA/SNZ/HB 436:2013 and provides information on the four types of scale.

Table 5 — Types of measurement scales and applicability

Type of scale	Description	Limitations/ Freedom	Level of risk example	Conceptual explanation
Nominal	Assigns data into categories.	No mathematical operation can be performed.	Lists or classifications of wildlife, cultural patterns, land use, etc.	Heat, colour, texture.
Ordinal	Comparative scales. Can be judged as more than or less than a given level.	<ul style="list-style-type: none">• Not measures of absolute magnitude, only relative.• Summation is arbitrary in absence of zero points.	Rankings such as High, Medium, Low or 1, 2, 3, 4, 5, where numerical value does not relate to value or quantity (i.e. level 2 might not be twice as big as level 1).	Cold, warm, hot.

Table 5 (continued)

Type of scale	Description	Limitations/ Freedom	Level of risk example	Conceptual explanation
Interval	Quantitative intervals between units of measurement are constant (10 exceeds 9 as 2 exceeds 1).	<ul style="list-style-type: none">• Can add/subtract or divide/multiply by a constant only.• Amalgamation possible only if defined equal points on all scales (e.g. a deficit of 2 is not twice 1 since redefining the zero point could transform value 2 to 5 and value 1 to 4).	A scale such as 1, 2, 3, ..., 9, 10, where numerical value has some meaning but zero point is arbitrary.	10° of temperature 20° of temperature 30° of temperature (but set point [0°] is not defined).
Ratio	Quantitative. Similar to Interval Scale but with set or non-arbitrary set point.	Measures magnitude not significance. Can be mathematically combined provided units are same or suitable conversion applied.	A measure of effect where zero point is set as no effect.	A scale such as “no loss”, “\$1 loss”, “\$2 loss”, etc.

It is critical that the methodology to assess the consequences and likelihood of risk uses the organization’s approved risk criteria. In addition, anonymous methods such as electronic voting provide for independent assessment of the consequence and likelihood to ensure that risk levels are based on the independently held views of participants and are not swayed by organizational culture or management expectations.

Risk evaluation

This final step in risk assessment is conducted to support decision-making about risk. This step, addressed in Clause 5.4.4 of the standard leads to a determination of whether the risk levels derived by the risk analysis, can be accepted or should have additional or modified controls in place to alter the

magnitude or severity of the risk. These decisions will be made in the light of the organization's risk attitude that is described in Section 3.7 and which is defined in Clause 2.4 of the standard as “the organization's approach to assess, and eventually pursue, retain, take or turn away from risk”. Examples of these terms are given in [Table 3](#).

Risk treatment

When risk evaluation determines that a risk is intolerable notwithstanding current risk treatments then additional treatment is required, [Figure 12](#) below (reprinted from SA/SNZ/HB 436:2013) describes a risk treatment process and identifies the options available to the organization at each step.

When selecting risk treatments, ensure that the treatments chosen are cost-effective and are in accordance with the external environment, including legal, regulatory, social, environmental and cultural elements. The risk treatment plan should be prioritized so that the manner in which risk treatments will be implemented, either sequentially or simultaneously, is clear.

Example of risk treatment

A history of evolving risk treatments.*

Driving a car has always included accepting the risk that an injury can occur if there is a collision. In 1947, Tucker, a US car manufacturer first introduced a seat belt that had two points of contact with the frame of the car and crossed the lap of occupants, which allowed drivers to protect themselves from injury if they chose to. In 1964, these became standard in all cars manufactured in the US. In 1967, seat belts became mandatory in the US. In 1968, seat belts that had three points of contact were developed crossing both the lap and shoulder of occupants, these became mandatory the same year. Accident statistics determined that seat belts were not being worn even though the law required them to. In 1974, automated “air bags” were developed to automatically deploy in a collision to protect occupants from injury. In 1991, air bags became mandatory. Each risk treatment proved to reduce risk.

Increasingly effective measures were developed, and eventually required by law as the tolerance for injury occurring as a result of a collision diminished. This risk treatment reduced the likelihood of serious injury in a collision but did not reduce the likelihood of a collision. Other risk treatments (e.g. driver training and testing in support of licensing drivers, speed limits, stop lights, prohibitions against drinking and driving, etc.) were developed to reduce the likelihood of collisions.

* Waters, W., McNabb, M.J. and Brown, B. A Half a Century of Attempts to Resolve Vehicle Occupant Safety: Understanding Seatbelt and Airbag Technology, 1998, Proc. 16th International Technical Conference on the Enhanced Safety of Vehicles (ESV).

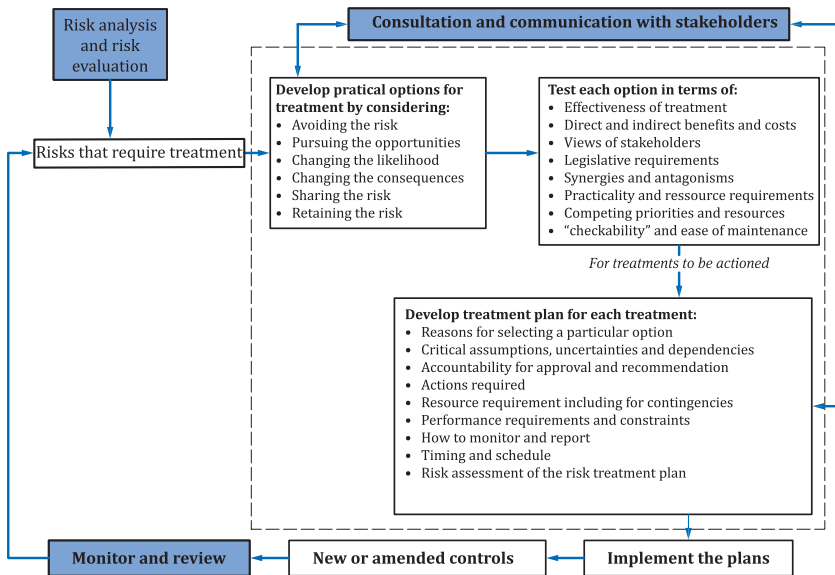


Figure 12 — Risk treatment process
(Reproduced with permission from Grant Purdy)

Risk treatment can be a source of risk and this should be taken into account. Ensure that the effect of the risk treatment is aligned with the objectives of the organization and that “unintended consequences” are avoided. [Figure 12](#) above, extracted from SA/SNZ/HB 436:2013, shows a summary of the entire risk treatment process. The ultimate objective of this process is a change in

the magnitude of the risk (e.g. a reduction in risks that have a negative effect on the achievement of objectives or an increase in risks with a positive effect on the achievement of objectives).

4.8 Communication of and consultation on the risk management process

Have you developed effective and comprehensive approaches to communication and consultation with internal and external stakeholders?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

Communication and consultation is a key element of risk management and continues through all stages of risk management from setting the context to risk treatment. Communications and consultations involve stakeholders, defined as a “person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity”.

Clause A.3.4 of the standard confirms that communication and consultation should be continuous through the entire risk management process. This includes frequent and comprehensive reporting on the performance of risk management. Communication and consultation are carried out with both internal and external stakeholders and the process is “two-way” where stakeholders participate in making risk management effective. This consultation and communication should include internal stakeholders (e.g., managers and staff) and also key external stakeholders (e.g., customers, suppliers, regulators, creditors, nearby residents).

Clauses 4.3.6 and 4.3.7 of the standard deal respectively with internal and external communication. In all cases, the sensitivity of the information (e.g. proprietary information on the performance of the organization’s products or services) as well as legal considerations related to privacy need to be taken into account.

Communicating and consulting with internal stakeholders

Internal stakeholders include the managers and decision-makers who receive the risk information and identify and treat risks as a part of their decision-making and priority setting. Employees in all parts of the organization are also internal stakeholders and need to understand the risk management process and organizational objectives so that they can contribute to the development of a risk culture. The implementation of risk management is a transformation, where risk management moves from an informal or anecdotal process to an explicit process that uses the organizations risk criteria and is directed at delivering management's objectives for the organization.

Ongoing communication and consultation can assist staff in understanding the objectives of risk management and can also provide a mechanism where risks that are evident at the working level can be considered for assessment and treatment in all parts of the organization. In addition, the communication of the risk criteria internally will help to create a coherent understanding of the organization's approach to risk, its risk attitude. This should be a formal process that uses communications methods and mechanisms that have proven to be effective.

Communicating and consulting with external stakeholders

In Section [2.4](#), information on how to identify your external stakeholders was provided. You need to understand who the external stakeholders are and their specific interest in your organization (e.g. nearby residents, clients, organizations interested in the environment, trade or working conditions). In addition, there should be information on how best to communicate and consult with each group. It may be necessary to provide materials in several languages, or in a manner (e.g. public meetings, notices in newspapers, handbills or electronic mail) that is appropriate and effective for each stakeholder group.

There may be business reasons for not sharing sensitive or confidential information (e.g. costs, margins, proprietary processes and arrangements), however, advising external stakeholders that: your organization is formally implementing a structured approach for risk management; your objective for this implementation; and how they will be involved, can improve relations and provide the basis for a level of trust.

All communication and consultation is a dialogue. Communication goes beyond the simple transmission of information and includes responding to questions and suggestions. During consultations, it is important to clarify at the outset the nature of the consultation and the disposition of inputs. Confusion can arise when a stakeholder or stakeholder group interprets consultation as the organization seeking direction, rather than seeking their views. The perspective or interest of each stakeholder should guide all communication and consultation activity.

In both communication and consultation, it is important to establish a mechanism that encourages respect and deals effectively with anger, frustration and misunderstanding.

Additional guidance on communication and consultation is found in Annex [B.3](#).

5 Monitoring and review

5.1 Monitoring and review of the risk management framework

Monitoring: “continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected”.

Review: “activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives”.

Have you developed effective and comprehensive approaches to monitoring and review of the risk management framework?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

Both the risk management framework and the risk management process should be monitored and reviewed on an ongoing basis. This focuses on the best way to monitor and review the risk management framework.

Quality assurance of your risk management framework is supported by your investment in monitoring and review. The process for monitoring and review that forms a critical component of ISO 31000:2009 is the “Plan-Do-Check-Act” cycle referred to throughout this guide. It is critical to monitor the performance of the risk management framework both when it is initially implemented, and regularly afterwards. If the risk management framework fails to perform at any time then the commitment to, and benefits derived from, risk management will be diminished or lost.

Clause 4.5 of the standard deals specifically with monitoring and review of the risk management framework and states that the organization should:

- measure risk management performance against indicators, which are periodically reviewed for appropriateness,
- periodically measure progress against, and deviation from, the risk management plan,
- periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal contexts,
- report on risk, progress with the risk management plan and how well the risk management policy is being followed, and
- review the effectiveness of the risk management framework.

It is important to evaluate the alignment of risk management activities with the governance and business planning cycle and also whether risk considerations have been included in major decisions. It is equally as important to ensure that the risk management activities give effect to the 11 principles of risk management, described earlier.

Section [2.3](#) deals specifically with the development of performance measures of risk management. There are three types of performance measures:

- overall success,
- process indicators, and
- outcome indicators.

The measure of overall success (e.g. the achievement of organizational objectives) is done at the organizational level and should integrate the success of the other measures. It is, however, a lagging indicator and it will not provide an early warning if the risk management processes are not functioning as planned.

Ongoing monitoring of the organization's context is where leading indicators can be found, changes in the context will change your risk levels before changes in performance are detected. A major change in the internal or external context of the organization should trigger a review of the risk management framework to determine what changes may be required in order to accommodate the changed context.

As an example of a change to the internal context, if the senior management of the organization modifies the objectives of the organization or their objectives for risk management, the risk management framework will need to be evaluated to determine if changes are required in order to maintain effective risk management.

Major changes in the external context could be changes to the regulatory environment, environmental or safety incidents in your organization or one like it, or a change in the ownership of the organization or the addition of a new and different product or service offering. These are examples of the kinds of major changes to the context that should trigger a review of the risk management framework.

5.2 Monitoring and review of the risk management process

Have you developed effective and comprehensive approaches to monitoring and reviewing the risk management process?

☐ **Yes** ➡ Go to next question

☐ **No** ➡ See guidance below

The purpose of monitoring and review as identified in Clause 5.6 of the standard includes:

- ensuring that controls are effective and efficient in both design and operation,
- obtaining further information to improve risk assessment,
- analysing and learning lessons from events (including near-hits), changes, trends, successes and failures,
- detecting changes in the external and internal contexts, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities, and
- identifying emerging risks.

Monitoring is an ongoing and comprehensive process that can identify when and where action is required. Monitoring may detect changes in the context (e.g. new laws, changes in interest rates, new competitors) or where change in

the risk management process itself is required (e.g. it is too complex or is not integrated into organizational processes).

The accountability for monitoring the risk management process should be clear, and these responsibilities should be identified in job descriptions. Performance assessments of staff with risk management responsibilities should measure how effectively they have delivered their responsibilities and provide recognition of success and assistance where performance has been inadequate.

Some organizations have identified indicators that provide information on the level of a risk or group of risks, and are called Key Risk Indicators (KRIs). These are most appropriate for large complex organizations where managers may not have direct information on the relationship with clients. Having and monitoring KRIs can act as an “early warning system” for changes to risks that are important to the organization.

KRIs are measures that relate to the internal or external context, or to specific risks or risk sources, or drivers. Usually, KRIs have acceptable values or ranges of value and when a KRI is outside the acceptable range of values, management is advised. While some organizations have performance indicators, performance is usually a “lagging indicator”, that is change in the risk is already diminishing performance. Ideally, KRIs are leading indicators that have predictive value and enable intervention before a risk becomes uncontrolled. No single KRI can assess an entire organization. KRIs are a tool to support monitoring and to provide managers with information that the organization’s context or risks may have changed enough to warrant further investigation.

Table 6 — Example key risk indicators

Activity	Possible key risk indicators		
Human Resources	Absenteeism	Days lost to sick leave	Grievances, formal complaints
Finances	Profits or losses misaligned with projections	Accounts receivable unpaid beyond established norms	Financial rating of organization falls, higher interest rates on debt
Compliance	Accidents, injuries on-site increased	Auditors report control weaknesses	Warnings or legal action by regulator
Information Technology	Network reliability and availability diminishes	Calls to technical support for assistance increase	Reporting from automated systems is delayed or unreliable
Risk Management	Risk information absent from decision documentation	Management overrides or ignores controls	Frequency of customer complaints
Customer Service	Increases in returned products or declined services	Number of calls to customer service function	Contact from important clients seeking redress or refunds

As risk management follows a “Plan-Do-Check-Act” cycle, monitoring the organization, monitoring is the **check** step, provides information on how to **act** to improve risk management for the next planning cycle.

6 Continuous improvement of the framework

6.1 Determining the effectiveness of risk management

Have you developed a reliable approach to assess the effectiveness of the risk management framework?

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

The results of monitoring and review activities discussed in Chapter 5 of this guide are the primary input into the assessment of the effectiveness of the risk management framework. While monitoring and review are essential elements of ISO 31000:2009, they are also included in the attributes of enhanced risk management in Annex A of the standard. Enhanced risk management is defined as risk management that has a high level of performance, and it should be seen as the goal that all implementations of risk management strive to achieve. There are two outcomes in Annex A that characterize high-performing risk management. These outcomes are:

- The organization has a current, correct and comprehensive understanding of its risks.
- The organization's risks are within its risk criteria.

Confirming that the organization has a current, correct and comprehensive understanding of its risks

Confirmation that there have been no material changes in the context since the risks were initially assessed is an indication that the inventory of risks is accurate and complete. If there have been major shifts in the context, for example new products, new markets, changes in the price of inputs to your product or service, then risk identification and risk assessment should be repeated to determine how the risks have changed in response to the changed context.

Evaluating whether there is a comprehensive understanding of the risks is more complex. Records of decisions or management meetings can be checked to determine whether the risk information that they are being provided with is useful to them and supports the consideration of risk information in decision-making.

Risks faced by the organization are modified by risk treatments so that resulting risk level or magnitude is within the risk criteria. Where risks are beyond or outside the organization's risk criteria and cannot be effectively treated, the organization can make decisions to accept the risks or to stop the activity that is associated with the intolerable risk.

Example — Responding to a change in context

In some parts of the world, cigarettes are very heavily taxed and comprehensively regulated. Smoking is prohibited in all public buildings, and on all modes of transportation, including private cars when children are present. A cigarette manufacturer may decide to treat the risks that this regulatory framework presents by avoiding that market. An alternative strategy could be to develop a new but related product where these regulations do not apply. Some manufacturers have developed “e-cigarettes”, small electronic devices that deliver nicotine gas on a demand basis. Whether a decision was taken to abandon the regulated market or to develop a new product, the organization has treated the risk of stringent regulations in a way that reduces the risk to the organization.

Confirming that the organization's risks are within its risk criteria

The outcome that risks are within the organization's risk criteria is another way of saying that all of the organization's risks, when risk treatments have been taken into account are tolerable. These risks still require ongoing treatment and monitoring as the organization wants to maintain its performance and its achievement of objectives. Having risks within the risk criteria only means that, with treatment, every risk that the company faces is tolerable and can be accepted.

Risks that are tolerable are still subject to treatment. Where these risks are reducing the achievement of objectives, organizations will continue to implement risk treatments to reduce the severity of the risk so that its severity or magnitude after risk treatment is tolerable.

The review and monitoring of risk management is done to ensure that when the magnitude of risks changes, that this will be identified and action will be taken to treat the risks that have changed. Monitoring risk levels to ensure that they remain within the organization's risk criteria is a measure of the performance of risk management.

6.2 Continual improvement of the framework

Have you developed a reliable approach for the continual improvement of the risk management framework?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

The final step in the risk management framework of ISO 31000:2009 is “continual improvement”. The organization should always be striving to improve its risk management as noted in Annex A of the standard.

Risk management, when implemented effectively, is an important tool for an organization to improve the achievement of its objectives. In any organization, regardless of its size and complexity, the internal and external contexts are always changing. Risk management cannot “stand still” and continue to be effective. This step seeking continual improvement is in place to specifically

recommend that action be taken on the results of the monitoring and review. Chapter 5 contains examples of the kinds of changes in context that would require risk identification to be repeated. As an example, material changes in the size and scope of your organization (e.g. operating at a second location or in a different country) will result in changes to both internal and external context. When the context changes, risk identification should be repeated so that an assessment can be made to determine if changes to the risk management framework are required.

A critical element to the “plan-do-check-act” cycle is determining whether the implementation of a planned action, like aligning your risk management with ISO 31000:2009 is having the desired effect. There will be “quick wins” where a particular process or concept aligns well with the culture of your organization and is quickly adopted and implemented effectively. Conversely there will be components that do not function as planned, that may not be well understood, or that may not be aligned with the culture of your organization.

The information provided here is to assist you in finding the areas of risk management that are working well and can be considered best practices and also to identify areas where improvements should be implemented for the next period or planning cycle.

Search for your own best practices by identifying those elements of your risk management framework that are working well and evaluate the reasons for this success, to determine whether these practices can be implemented in other areas of your organization. A best practice could be the effective tailoring of the risk management framework so that employees view it as simple and straightforward. It is important to have a mechanism that ensures best practices are identified and that their implementation is recognized and rewarded.

When you find areas of risk management that are not functioning as planned and are not ‘creating and protecting value’ these areas represent areas that require attention. The incomplete or inadequate implementation of risk management can quickly become an important source of risk.

Continual improvement of risk management includes working towards achieving enhanced risk management as described in Annex A of the standard.

There are five attributes of enhanced risk management that can be evaluated that are listed below.

1. Continual improvement

Continual improvement in risk management is achieved by setting performance goals and by conducting a review of risk management processes, systems, resources, capability and skills. Where these are found to require improvement, the appropriate steps should be taken.

2. Full accountability for risks

Enhanced risk management includes clear accountability for risks, controls and treatment. This accountability is comprehensive and clearly defined. Accountable individuals need to have the authority, appropriate skills and the resources to:

- check controls,
- monitor risks.
- improve controls, and
- communicate effectively to external and internal stakeholders.

The organization supports those with risk management accountability by providing them with the authority to manage risk and the time, resources training, and skills to manage risks effectively.

3. Application of risk management in all decision-making

All decision-making within the organization, at all levels of importance and significance, explicitly considers risks and includes the application of risk management.

4. Continual communications

Enhanced risk management includes continual communications with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance.

5. Full integration into the organization's governance structure

When enhanced risk management has been achieved, it is seen as central to the organization's management processes. The governance structure and

management processes are based on the management of risk. Managers consider risk management to be an essential part of every decision in order for organization to achieve its objectives.

By evaluating your risk management against these five attributes you can determine whether you have achieved enhanced risk management. If you have not, then develop a plan to improve the risk management framework based on the information you have gathered.

6.3 Continual improvement of the implementation of the process

Have you developed a reliable approach for the continual improvement of the risk management process?

☐ **Yes** → Go to next question

☐ **No** → See guidance below

There are two steps to achieving continuous improvement of the risk management process. The first is to ensure that the existing process is performing as planned and the second is to identify areas where improvements to the process are possible and are cost effective to implement.

In Section [5.2](#), information was provided on evaluating the implementation of the risk management process. In the implementation of any process there will be strengths and weaknesses, successes and failures. In order for risk management to be an effective tool for the organization, the successes need to be noted and the failures or weaknesses need to be understood and addressed.

To determine if the existing risk management process is working effectively, review the performance of the organization as well as any key risk indicators you have identified. These are described in Section [5.2](#) and examples are provided in [Table 6](#). The risk management process should be well understood and valued by managers as a useful source of information for decision-making. Surveys (see Annex B.3) of managers and staff can provide information on whether the risk management process is working as planned and becoming a fully integrated business practice.

A very common weakness that emerges in implementing risk management is an incomplete understanding of the organization's commitment to risk management or of senior management's support for it.

If risk management becomes only a process that must be done, it will quickly degrade into a “tick box” for managers. A “tick box” is a process or step that is seen as having no inherent value and which is completed out of obligation. The consequences of such a perception will be that risk management information will become less accurate and less useful.

Training and capacity building are tools that can support the effective implementation of the risk management process. The individuals who are involved in risk assessment (i.e. risk identification, risk analysis and risk evaluation) should be trained and the effectiveness of this training should be monitored. In some organizations, the individuals accountable for risk assessment work together to form a “community of practice”. Successes are shared and challenges are solved with the collective wisdom and experience of others who have similar responsibilities with regard to risk.

Risk management information should be available to managers at a time and in a form where it is considered to be a valuable input to planning and decision-making. If monitoring and review is detecting that this is not occurring, it is important to take action to correct this.

Identifying and implementing steps that will improve the risk management process is the second step in improving the risk management process. One approach to this can be conducting a “strengths, weaknesses, opportunities and threats” (also called SWOT) analysis of the risk management process. This can be done using a survey or by reviewing the information developed from the monitoring of the risk management process (see Section [5.2](#)).

In looking for opportunities to improve risk management, pay particular attention to how changes in context are identified and responded to. Principle J notes that risk management states, “Risk management is dynamic, iterative and responsive to change”. In order to improve risk management, pay particular attention to the activities that monitor the context of the organization. These activities should provide a way for employees to identify when and how changes are affecting the organization and when the risk management process

needs to be used to reassess the risks that may be affected by these changes. If there is a tradition of using the same risks with the same risk information year after year, introducing a step where the context statements are contrasted with the current internal and external contexts can be a simple way of improving the risk management process.

Another important and effective mechanism to improve the risk management process is to have the management team identify changes that would make the risk management information they receive more valuable and easier to use. In some organizations, the risk management process has focused on producing graphs (including “heat maps”) and complex risk registers rather than providing information on risks that managers can use and which will lead to better decisions.

Improving the risk management process should always be focused on improving the achievement of objectives, and helping embed risk management into the decision-making and culture in all parts of the organization.

Annex A — Risk management techniques for SMEs

A.1 Qualitative approaches to assessing consequence and likelihood

Risk management at the organizational level may not have reliable and accurate quantitative information on risks, their potential consequences and the likelihood of these consequences. For most SMEs, a qualitative approach to assessing risks will be the most practical approach. Qualitative approaches “rely on descriptive or comparative characterization of consequence, likelihood and the level of risk”¹⁹).

Defining the scale that will be used in the organization may be prescribed by statute, regulation or policy. In general, the consequence scale covers the full span of potential consequences from “no real consequence” to a consequence whose outcome can be described as extreme, and which could potentially result in permanent harm to the organization. There are several approaches that are commonly used, some divide this universe into three divisions (sometimes referred to as low, medium and high”) while other approaches divide this range into as many as 10 or more categories. There is considerable research into this area and several valuable papers have been published by the Australian Centre of Excellence for Biosecurity Risk Analysis (CEBRA) at the University of

19) As noted in SA/SNZ HB 436:2013 Clause C2.

Melbourne²⁰⁾. Many practitioners are of the view that the number of categories for both consequence and likelihood should be an even number, so as to avoid a common strategy of “choosing the middle”.

Consequence

Consequence scales are more relevant to those being asked to make the assessment if the descriptors have numbers and high-level terms (like “extreme”). A best practice is to develop a table of consequence levels that includes categories describing the area of impact. These categories for consequence often include: financial impact; impact on operational capacity; impact on reputation; impact on legal and regulatory obligations; and impact on outputs or deliverables. [Table A.1](#) below, has been provided as an example of this approach.

It is critical to understand that such tables do not result in a linear relationship among the severity levels and therefore mathematical operations (e.g. adding, multiplying) are not valid and should be avoided.

Likelihood

It is critical to note that the likelihood that is assessed is the likelihood of the consequence that has been identified. The risk assessment process is to assess consequence, and then the likelihood of the consequence, taking into account current controls, current staff, and current budgets.

The period of time for which the likelihood is assessed should be decided by the organization in the light of the context, as many organizations have an annual planning cycle the likelihood is often assessed for one year. [Table A.2](#) has been provided as an example of a Likelihood scale, as with other examples, the likelihood scale provided here should be considered, reviewed and tailored for your organization. Where there are risks which have a very long period or low frequency (like climate change, desertification, severe floods) a different approach entirely, often Scenario Analysis²¹⁾, is used to assess these risks.

20) Assessment of strategies for evaluating extreme risks, Linguistic uncertainty in qualitative risk assessment and how to minimize it, Uses and misuses of Multi-Criteria Decision Analysis in Environmental Decision-Making, and others.

21) An excellent overview of this approach can be found in the book, The Scenario Planning Handbook, Ralston and Wilson, Thomson Southwestern, 2006, 258 pp.

Table A.1 — Example consequence scale

Level	General	Legal	Environmental	Operational	Financial	Reputational
6	Extreme	A non-compliance that results in the organization ceasing operations for over one year.	An impact on a natural system, species or area that results in extinction, irreparable biological harm or irretrievable loss.	The organization cannot operate at one or more locations for more than one year.	Greater than \$10m or 100 % of the organization's net worth.	Sustained negative media attention at national or international level lasting for more than 3 days.
5	Very Severe	A non-compliance that results in the organization ceasing operations for six months to one year.	An impact on a natural system, species or area that results in a species being identified as endangered, biological harm or loss that takes more than 2 years to recover from.	The organization cannot operate at one or more locations for six months to one year.	Greater than \$5m or 50 % of the organization's net worth.	Sustained negative media attention at national or international level lasting for more than 3 days.
4	Severe	A non-compliance that results in the organization ceasing operations for one to six months.	An impact on a natural system, species or area that results in a species being identified as threatened, biological harm or loss that takes 6 months to 1 year to recover from.	The organization cannot operate at one locations for six months to one year.	Greater than \$2m or 30 % of the organization's net worth.	Sustained negative media attention at national or international level lasting for 1 day.

Table A.1 (continued)

Level	General	Legal	Environmental	Operational	Financial	Reputational
3	Moderate	A non-compliance that results in the organization paying a fine of \$1M or 10 % of the organization's net worth.	An impact on a natural system, species or area that results in a species abundance at historic lows, biological harm or loss that takes less than 6 months to recover from.	The organization's operations are reduced by 80 % or more for 30 days.	Greater than \$1m or 10 % of the organization's net worth.	Sustained negative media attention at a regional level lasting for 1 day.
2	Low	A non-compliance that results in the organization paying a fine of less than 1\$M or 10 % of the organization's net worth.	An impact on a natural system, species or area that results in a depression of species abundance within the normal range, biological harm or loss that takes less than 2 months to recover from.	The organization's operations are reduced by up to 80 % or more for 10 days.	Less than \$1m or 10 % of the organization's net worth.	Negative media attention at local level lasting for 1 day.
1	Insignificant	Compliance with all applicable statutory instruments.	No significant negative impacts on the environment.	The organization's operations are not affected.	Impacts can be absorbed with no budgetary adjustments.	Complaints are received by the organization but not sustained.

Table A.2 — Example likelihood scale

Level	Narrative	Likelihood in one year
6	Almost certain	> 95 %
5	Very Likely	80 % to 95 %
4	Likely	50 % to 80 %
3	Possible	20 % to 50 %
2	Unlikely	6 % to 20 %
1	Rare	< 5 %

There are biases in using qualitative assessments and it is a methodology that does not permit the use of arithmetic combination (e.g. adding, multiplying or any other mathematical process). It is possible to assign overall risk level or severity using a table such as [Table A.3](#) below.

Table A.3 — Example severity matrix

C O N S E Q U E N C E	5 (highest)	Very High	Extreme	Extreme	Extreme	Extreme
	4	High	Very High	Very High	Extreme	Extreme
	3	Moderate	High	High	Very High	Very High
	2	Low	Low	Moderate	Moderate	Moderate
	1 (lowest)	Low	Low	Low	Low	Low
		1 (lowest)	2	3	4	5 (highest)
Likelihood						

This severity matrix is not bilaterally symmetrical and hence in its current form it is “skewed” to focus attention on high consequence risks. It also notes that the lowest impact risk, remains at a low severity regardless of how likely the occurrence. Some tables make the mistake of assuming that an insignificant risk that is highly likely somehow becomes more severe.

Qualitative analyses are necessarily subjective and imperfect. When individuals who have a good understanding of both the risk and the organization make these determinations, a reasonable approximation of the consequence and likelihood is derived. This is especially true when each individual

provides their assessment independently, which can easily be accomplished by the use of electronic voting methodologies. Another valuable step is to draw on the entire internal context of the organization when forming a group to make these assessments. Having managers and employees from one area of the organization may introduce a bias that a broader sample can avoid. Every organization should develop a severity matrix that aligns with the risk attitude of the organization and that has the support of the senior management team.

There are other methodologies, including prediction markets ²²⁾ (which can only predict likelihood) that can be quite accurate, but which are more complex to establish and are likely of little practical value to an SME.

A.2 Identify advocates for and experts in risk management

In some very large organizations, there are employees who are designated as “risk champions”, it is a curious title as they have not won anything, the title flows from the use of the term champion when it means advocate. Webster includes this definition: “someone who fights or speaks publicly in support of a person, belief, cause, etc.”

Advocates for risk management are not salespersons, but rather individuals who are convinced of the benefits that risk management can provide, and are anxious for others to understand how risk management can result in the operations of the organization moving more smoothly and effectively and where solutions, actually risk treatments, significantly improve the results that are achieved.

Advocates for risk management can be identified, but are rarely created. The passion for risk management as a tool to improve results comes from experiencing the benefits of effective risk management. Some employees may have such experience from previous employment experiences or from using risk management in their personal lives. Employees without this prior experience

22) B. Cowgill, J. Wolfers, and E. Zitwewitz. Using Prediction Markets to Track Information Flows: Evidence from Google. 2008.

of success will need to have it in your organization. This will come, and when you can identify individuals who are seen by others as knowledgeable and enthusiastic advocates for the use of risk management, it may be valuable to provide them with an opportunity to interact with others in your organization who have risk management responsibilities.

Training is essential to effective implementation of the risk management process. Incomplete or “half-hearted” implementation will cause the effectiveness of risk management to degrade with very negative consequences. Training can be done through such practices as “job-shadowing” or mentoring, where experienced individuals are accompanied by employees who can acquire skills by studying the work and approaches of people with more experience or training.

Sending employees to formal training should be done cautiously, especially since the current interest in risk management has resulted in “certificate mills” where entrepreneurs present themselves as experts in risk management and offer colourful certificates but transfer little or no useful information. The credentials of any organization offering training should include references for those who are teaching. These references should be for delivering risk management, not simply for training. As implied by the saying “the proof of the pudding is in the eating”, the value of any risk management training should be determined by what the individual taking the course has learned and can apply upon their return to the organization.

A.3 Choosing a risk assessment methodology for risk identification

Risk identification is one of the most critical elements of risk management. It is also an element that is often incomplete or inadequate.

Risk identification is carried out to develop a full understanding of uncertainties that can enhance or limit the organization’s ability to achieve its objectives. Risks can be related to economic or environmental conditions, community, stakeholder or employee relations, confusion over objectives or roles and responsibilities, or any other condition that can impact on the achievement of objectives.

Risk identification will always include documenting, validating and testing the information that is collected. The identification process will use information found in programme evaluations, internal or external audits, “lessons learned” reports where failures or accidents have occurred in the organization or a similar one. Information used in risk identification should be checked for bias, as an important source of risk can be “wilful blindness”, which is where there is a culture or tradition of not exploring risk in certain areas (such as illegal or questionable activities by managers or valued employees). There may not be a willingness to look for risks associated with powerful individuals, even though this can be a very important source of risk. All potential sources of risk should be included in the risk identification process. It may well be that risks associated with important or powerful individuals are “accepted” rather than treated, but this should be an explicit risk management decision taken by the organization’s management team.

Individuals who do risk identification should be trained or accredited because risks that are not identified are omitted from the risk management process and are not analysed, evaluated or treated. As noted in the standard, appropriate tools and techniques should be used and a person who is trained and experienced in risk management will be in a position to recommend and implement the appropriate tools and techniques. The risk identification process should be comprehensive and systematic but should result in a list of risks that can significantly influence the achievement of objectives. IEC 31010:2009 has a list of techniques. These are described below.

The following example is provided to assist you in understanding how to choose a risk identification methodology that is fit for your organization.

Options for risk identification

Once the context for risk management has been identified, the identification of risks is the next critical step. It is important to choose an approach that you understand and which fits the size and nature of your organization.

Below is a list of the risk assessment techniques identified as “strongly applicable” for risk identification in both IEC 31010:2009 and SA SNZ/HB 89:2013 Risk Management — Guidelines on Risk Assessment Techniques.

The risk assessment techniques are:

- Brainstorming.
- Cause and Consequence or Cause Effect Analysis.
- Checklists.
- Consequence/likelihood matrix.
- Failure Mode Effect Analysis (FMEA).
- Hazard Analysis and Critical Control Points (HACCP).
- Hazard and Operability Studies (HAZOP).
- Human Reliability Analysis (HRA).
- Primary or Preliminary Hazard Analysis (PHA).
- Scenario Analysis (SA).
- Sneak Circuit Analysis (SCA).
- Structured or Semi-Structured interviews.
- Structured What-If Techniques (SWIFT).

As this guide is intended as a bridge to the more comprehensive and detailed information provided by standards organizations, only four techniques will be described in detail. The purchase of one or both of the documents listed above is recommended.

While 13 techniques are listed above, only four risk identification techniques are presented in detail. These have been chosen because of their simplicity and ease of use. They are:

- Brainstorming.
- Checklists.
- Interviews — Structured or semi-structured.
- Structured What-if Techniques (also known as SWIFT).

Brainstorming

This process is a meeting of individuals who are well informed about your organization and the products and services it offers, as well as those knowledgeable of the internal and external contexts of your organization (laws, regulations, customer preferences, labour market, the organization's physical and intellectual assets, employees and managers). A critical success factor is the presence of an experienced facilitator and someone who records thoughts, suggestions, comments and recommendations so that they can be analysed further.

The objective of the session, risk identification for the organization, must be clearly communicated to all participants. The method that would be used to prepare a list of relevant risks and current controls should be fully described for all participants. The method should capture all inputs, and align information on each risk separately for use in the subsequent steps of risk assessment, namely risk analysis and risk evaluation.

Brainstorming about risk is a facilitated discussion, where every member of the group is considered to have information of value. There is a clear objective and there are certain rules, such as only one person speaking at a time. The subject of the brainstorming is established by the facilitator and is focused on risks or uncertainties that the organization may face or be affected by. In general this is a process that is an idea generator, and specific risks may not be completely clarified or discussed at length. Virtually every idea that is raised is captured without analysis or debate.

Its strengths include its simplicity and ease of use. Its weaknesses include that some people may be reluctant to speak freely about risks in front of colleagues and managers. Another weakness is that the product is often a broad spectrum of thoughts, ideas and concepts and considerable work by a trained risk professional is required to extract the risk information from meeting notes that can be unstructured and chaotic.

A limitation of brainstorming is the size of the group involved. In order for brainstorming to benefit from the experience and knowledge of participants, the size of the group must be manageable, usually less than 30, often less than 10.

Checklists

This process relies on participation of individuals who have the qualities identified for brainstorming. Checklists can be the next step for a risk list developed by brainstorming or a list developed based on risk events that have occurred, or were “near hits” for the organization. The checklists themselves are usually a list of known control weaknesses or failures for your organization or ones that are similar.

Checklists are a formal way for the organization to focus on each risk and carefully review its relevance to the organization and determine if it should proceed to the subsequent steps of risk assessment, risk analysis and risk evaluation.

The process can be done in a meeting setting where each item on the checklist is described and discussed. This discussion will explore the relevance of the risk to the organization, current controls and potential controls that can modify the risk but which are not currently in use. By providing a comprehensive checklist it is possible to ensure that all known or expected risks are evaluated and discussed. In this way checklists are more comprehensive than brainstorming, which can overlook or exclude risks.

Checklists can be weak at identifying and analysing “blind spots”²³⁾, which are risks that are often overlooked or ignored as unimportant. They can become ritualistic and “tick box” exercises if not implemented carefully. It should be clear to all participants that the objective is to get their personal input on causes of the risk, consequences and controls, both those that are in place and those that are not present but which could be effective.

Checklists can be used in every step of risk management from risk identification to risk treatment. Checklists can be formalized (see Annex B.5 of this guide on documentation) and retained by the organization. It is important that these lists are regularly evaluated to determine their ongoing relevance to the organization as its internal and external contexts evolve. In some organizations there are checklists of business critical risks, this list is often referred to as Key Risk Indicators or KRIs.

Interviews — Structured or semi-structured

This process relies on participation of individuals who have the qualities identified for brainstorming. In this risk identification process, the knowledgeable individuals are interviewed, usually on a “one-on-one” basis.

Once again the person conducting the interviews should have a good understanding of risk, as well as interviewing experience. As the name suggests, structured interviews are conducted through the use of a series of prompts or

23) Van Hecke, M.L. 2007. 256 pages Blind Spots, Why Smart People do Dumb Things. Prometheus Press ISBN: 1-59102-509-5.

questions that have been predefined and often explore the same aspects of an organization from different perspectives. Semi-structured interviews are more free-flowing and allow the interviewee to focus on specific areas of uncertainty that they may be well informed about, or have concerns over.

A major difference between interviews and brainstorming or checklists is that interviews are not held in a group setting. In many cases more details are available as interviews are conducted individually and risk information that may be critical of fellow employees or managers may be discussed where in a group setting employees may not wish to present information that could be seen as critical of co-workers or managers.

Interviews should be based on questions that are “open ended”, for example “Tell me what risks we could face that are related to inventory?” rather than closed ended “Do you conduct regular physical counts of every item in the warehouse?” where the answer can be a simple yes or no.

Interviews are also useful where there are reasons, like ensuring corporate confidentiality, or personal privacy, that make group discussions inappropriate. Interviews can also be used to gain insights from external stakeholders, for example customers or bankers, who may have excellent perspectives on risks that are external to the organization.

Transforming the interview notes into risk information is best accomplished through the use of a risk professional who has the experience and knowledge to aggregate often complex narratives into specific information on risks, their causes, consequences and current controls.

A limitation of this technique is the time required and the need for extensive preliminary work to ensure that the scope of the interviews is comprehensive. Time is also required for a skilled risk management practitioner to analyse the interview notes.

Structured What-If Techniques (also called SWIFT)

This process relies on participation of individuals who have the qualities identified for brainstorming. As with brainstorming, it is conducted in a group setting. Similar to a structured interview there are specific conditions or prompts that are presented to the group to focus the discussion and to gather quite

specific information on conditions or changes that could occur. As the title suggests, the prompts to initiate a discussion can take the form of a question that begins with “What if...?”.

Examples of questions include “What if there was a failure of the electricity supply for an extended period?” or “What if a large international organization began to offer the same products or services that we do, only at a lower price?”. These types of questions are developed before the workshop and often explore known risks or situations that have affected similar organizations in the past. There are other structures to these questions that can include “Has something ever happened that you felt could limit our success as an organization?” or “If our company had a major problem, please describe what you think the problem might be and what would have caused it?”

The discussion in these “what-if” sessions is often more detailed in regard to risk treatment measures. Participants respond by identifying relevant controls that are in place and the ability of these controls to modify the risk that was the subject of the question.

A strength of this approach is that it can assess risks at all levels, ranging from individual actions or processes to holistic assessments of entire processes. This approach can be directed to risks in an office environment or to a manufacturing environment where you may wish to also seek information on safety hazards as well as risks.

The notes from a SWIFT session can be used to develop a comprehensive list of risks and also form the basis for a risk treatment plan.

A.4 The Bowtie methodology, a simple and comprehensive tool

This chapter presents the Bowtie methodology as a tool to assist SMEs in obtaining a better understanding of their risks, current controls and potential consequences. It is an extremely powerful technique that is described in more detail in IEC 31010:2009 and SA SNZ/HB 89:2013.

While its origins date back to the 1970s, the Bowtie methodology has become a valuable tool for government and business to capture a comprehensive picture of risk sources, relevant controls, risk events and potential consequences. Unlike many ways of recording risk information the Bowtie methodology clearly differentiates between controls that operate before a risk event from those that operate after a risk event has occurred. An example would be that for a risk related to the loss of control of a car, a source of risk could be icy conditions on the road; pre-event controls would include special tires for ice and snow, as well as instruction for driving in winter conditions. The risk event (in Bowtie methodology it is called the “top event”) is the loss of control over the car. The post event controls (also called recovery controls) include seat belts and airbags, to prevent injury to passengers, and barriers down the middle of the road to prevent the car from entering the path of oncoming cars.

The Bowtie methodology builds on two proven analytical approaches to understanding risk. It includes ideas and structures found in a Fault Tree analysis such as the example shown in [Figure A.1](#). The example shown in [Figure A.2](#) is where there is a fault, in this case “no flow into barrel E”. The graphic shows a series of conditions that can cause this result. There are two high-level causes, no flow from pipe B or no flow from pipe C, the box “and” indicates that both of these conditions must be true in order for the specified failure to occur. The next level of the analysis shows conditions that could result in no flow from each pipe. In each case, there are a series of events or conditions, either one of which could lead to the “no flow” condition. Where either source could lead to the result are connected with an “or” connector.

A fault tree analysis starts with the undesirable condition or fault at the top. All sources that could give rise to this fault are shown in a “tree” of potential sources. The graphic is therefore called a fault tree analysis as it shows all the branches or sources that can produce a specific fault.

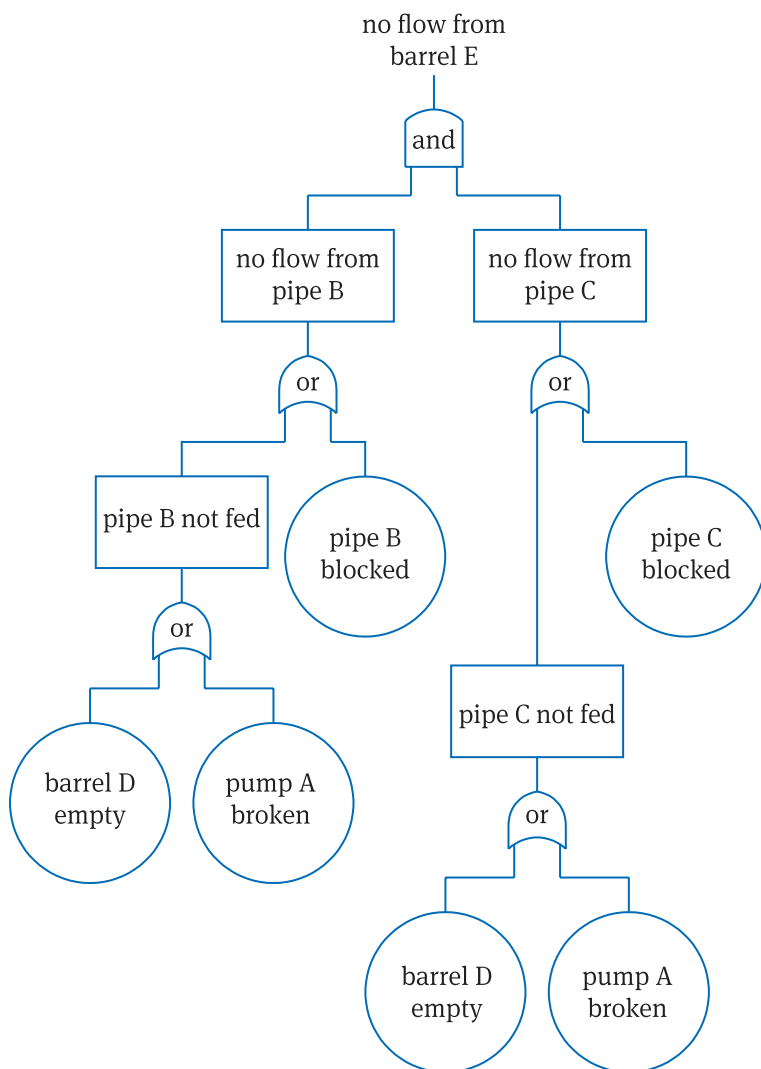


Figure A.1 — Fault Tree analysis ²⁴⁾
 (Reproduced with permission from CGERisk Inc.)

24) Graphic provided by CGERisk Inc. Leidschendam, Netherlands.

The second element of a Bowtie analysis is based on an Event Tree which is used to model outcomes, or consequences of a specific event. [Figure A.2](#) describes the potential consequences of a release of a flammable liquid which can result in an explosion, fire or spill, depending on the conditions which exist after the release.

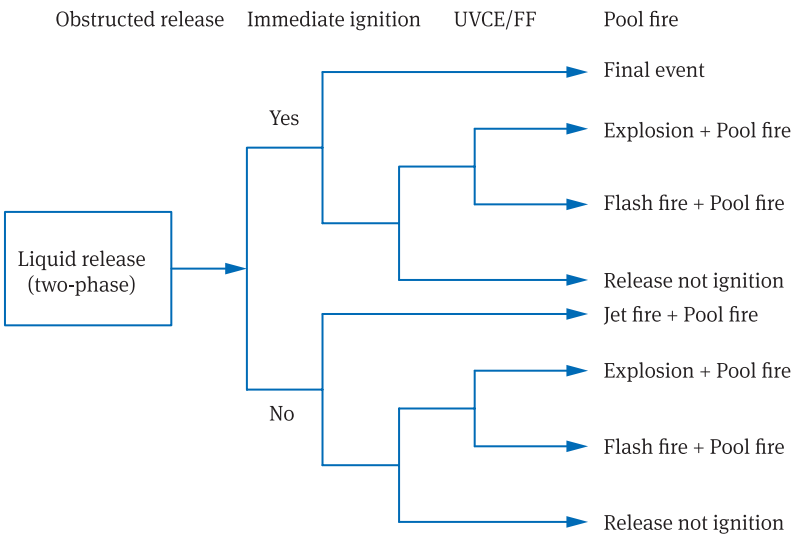


Figure A.2 — Event Tree analysis ²⁵⁾
(Reproduced with permission from CGERisk Inc.)

The Bowtie methodology connects these two tools at the “top event” and creates a shape that is similar to a man’s bowtie as shown in [Figure A.3](#).

²⁵⁾ Graphic provided by CGERisk Inc. Leidschendam, Netherlands.

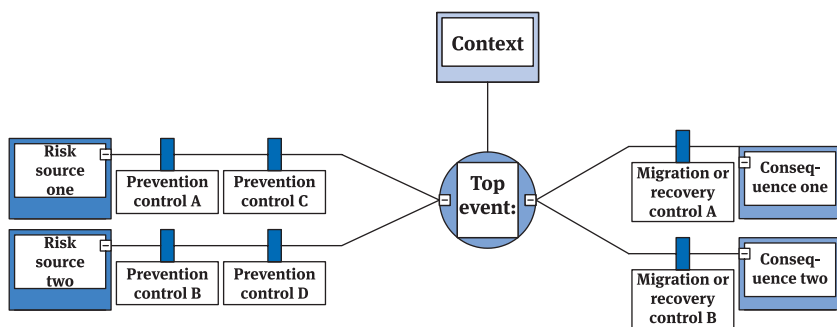


Figure A.3 — Bowtie diagram

On the left hand-side is a list of potential sources of risk, which can create a particular risk event (or top event). This is a fault tree analysis. Lines are drawn from the source of risk to the risk event. Controls or risk treatments (also called prevention controls or barriers) are added to the drawing between the risk source and the risk event. It is possible to characterize the nature of the risk treatment (a physical barrier, a law or regulation, a policy or guideline) and the person or entity responsible for implementing, maintaining or enforcing the barrier.

On the right hand side of the drawing are the potential consequences of a risk event. This is the event tree portion of the analysis. The visual structure of a bowtie diagram helps organizations to better understand that a risk event, such as a spill of flammable liquid, does not inevitably result in a specific consequence, like explosion or fire. It highlights the nature and effectiveness of controls that act to limit or prevent consequences even after the event has taken place. Controls that take effect after a risk event are described as mitigation or recovery controls.

This methodology can be used to enhance a brainstorming session or to collect information on risks and controls that are relevant to your organization. It will be most effective when you involve your employees and managers in identifying and describing the nature of the risks and the effectiveness and ownership of the controls. If, for example, you have a control where you verify the signature of authorized employees, the individual who checks the signed document against a signature card is the responsible individual, and as this is

a financial transaction, the person in charge of your organizations financials, a treasurer or chief financial officer, is the control owner.

The Bowtie methodology is very easy to implement. It brings a clear focus to discussions about risk and completed bowties can be retained for easy communication of risks and controls to stakeholders. Since this approach maps all controls and their mode of action (e.g. preventative barrier), it facilitates decision-making regarding the need to add, remove or modify the array of relevant controls when the risks change in response to changes in the context.

While it is possible to develop bowties using flip charts and whiteboards, and even word processing or presentation software, there are sophisticated and elegant software implementations which are reliable and widely used. If you decide to use the bowtie approach in your organization, the acquisition of such software can simplify and enhance your implementation of risk management.

Annex B — Specific guidance for SMEs

B.1 Guidance on implementing the principles of risk management

For risk management to help you to achieve your objectives, it is important to align your implementation of risk management with the 11 principles set out in the standard.

For all principles

Alignment with all of these principles is required for your risk management to be effective, reliable and sustainable. Implementation of a few of the principles will not have the same positive result. Some of the principles are linked to one another, which should facilitate effective implementation.

Ensure that you understand the intent of the principle, and the specific terms that are used.

For each principle, determine how it can apply, how it can be achieved, measured and tracked. The organization will also need to set out in its risk management framework how this assessment will be done, how frequently it will be done and who will do it.

Risk management training in your organization should include a focus on these 11 principles, how your organization has aligned with them and how performance against each principle is measured. In many cases there will be business related indicators, which will indicate whether the principle is being applied effectively.

Principle A: Risk management creates and protects value

This principle has two aspects or elements.

The first aspect is that it explains the reason for managing risk. Value is created through more effective achievement of objectives and is preserved and protected by ensuring that the process used to manage risks is sensitive to changes in the organization and its internal and external contexts. Risk is managed to achieve objectives including the objective of creating and protecting value and is never implemented as an end in itself or to “tick a box”. The term “ticking a box” refers to limited completion of an activity or step for the purpose of saying that step has been completed, regardless of whether the step was completed effectively in a way that the step will provide the intended benefits.

The second aspect of this principle is that it sets out a measure that can be used to design your risk management framework and process and to measure its effectiveness. Committing to creating value is a reminder that the costs of implementing risk management must be less than the benefits (in terms of improved achievement of objectives) that it provides. The value created can be less severe consequences from risk events that limit or constrain the achievement of objectives, or a decision to open a new business line or services because of the positive uncertainty that the business uncertainty (risk) provides. This principle should guide choices made on risk treatment. This principle could be included in a policy statement to clarify the reason for making a commitment to implement risk management.

Alignment with this principle should be assessed by the system or process that is established to monitor and review risk management. Potential measures of risk management’s performance include more consistent performance, and increases in: business value; profitability; credit ratings; or share price.

Principle B: Risk management is an integral part of organizational processes

The standard describes this principle by noting that risk management is not a stand-alone activity, rather it is a responsibility of both management and employees.

This principle describes a core condition that should arise from the implementation of risk management. Organizational process include everything from the procurement of supplies and services, to planning for the coming period (year, month etc.) to making decisions on activities that will be changed, either expanded, reduced or eliminated. Organizational processes also include training and instruction or guidance manuals.

The term “integrated” indicates that risk management should be built into processes not added on or seen as a separate activity. Risk should be explicitly considered in the normal course of all decision-making. It is essential that the organization’s risk criteria are clear, easily understood and available to all employees. When the risk criteria are clearly understood, integrating risk management into organizational processes can be done in such a way that it becomes an essential, or expected part of every decision.

A measure of the degree to which risk is integrated into organizational processes is the presence of explicit analysis of risks in operational plans and in the minutes of management meetings.

Principle C: Risk management is part of decision-making

The standard clearly states “*risk management helps decision-makers make informed choices, prioritize actions and distinguish among courses of action.*” This principle is contained in Principle B as organizational processes always include decision-making. Since decisions give rise to uncertainty, it is essential that decisions are implemented in a way that reduces uncertainty. Decisions need to be aligned with the risk management framework and the risk management process that the organization has developed, approved and implemented. The performance measure described for Principle B above can be applied to this principle as well.

Principle D: Risk management addresses uncertainty

Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed is the standard’s description of this principle. As risk is the “effect of uncertainty on objectives” risk management has to address that uncertainty by understanding it and by understanding how to respond to that uncertainty in planning, decision-making and priority setting.

Uncertainty has been extensively studied, in particular with respect to philosophy, economics, physics and sociology. Some studies ²⁶⁾ suggest that there are two general types of uncertainty, the first is described as “essential randomness”, (e.g. like the result of a roll of dice) and the second is the result of insufficient, incomplete or missing information.

As decision-makers consider the uncertainties relevant to a plan or a decision, they need to fully understand the uncertainty, its consequences related to objectives and how any risk treatment decision may cause changes in the uncertainty. An example would be an organization where inputs are imported and are from a jurisdiction with a different currency.

The organization may wish to reduce uncertainty related to the volatility of currency exchange rates by purchasing amounts of a foreign currency that are sufficient for a fixed period (e.g. one year) so that they stabilize the price of their product or service. Other uncertainties could relate to whether or not employees will comply with a company rule or guideline. This principle indicates that important uncertainties need to be addressed in order to manage risks effectively.

Principle E: Risk management is systematic, structured and timely

This principle will assist organizations by ensuring that risk information is of consistent quality as time passes, has been developed in a structured way and is provided to decision-makers at a time when the information can be taken into account. As noted in the standard, this will contribute to efficiency and to reliable results.

Alignment with this principle can be accomplished by ensuring that the risk management framework and process are both well documented. They should be consistently aligned with the governance and decision-making framework in the organization. Risk information should be available in advance of decisions where the risk information is relevant. An example of timeliness would be that the risks related to the organization’s financial position are analysed and available prior to the organization making an important decision on spending.

26) The Emergence of Probability, 246 pages, Hacking, I. 1975, Cambridge University Press, ISBN-13: 978-0521685573.

Principle F: Risk management is based on the best available information

The standard notes that decision-makers should be aware of and take account of limitations related to the information that is used to support risk management. Decision-makers should seek out the most complete and accurate information that is available relevant to risks. Sources of information vary. Information from physical measurements (like size and mass) may be less subject to bias than information obtained by surveys, sampling, estimation or modelling.

Alignment with this principle can be achieved by always evaluating the inputs to risk management to ensure that the information is accurate, and that any errors, biases or other uncertainties are understood and accounted for when the information is used. When risk assessments are repeated annually, it is important to verify that the information on the risk, including information on the internal and external contexts, is updated before reassessing the risk. It is a best practice to document considerations that have been made regarding the accuracy, completeness and reliability of information so as to determine if it can be used or should be disregarded and new, more accurate information be acquired.

Principle G: Risk management is tailored

While the standard notes that risk management should be aligned with the internal and external contexts, this principle goes much farther. The risk management framework and process should be developed so that all their aspects are fully aligned with the size and complexity of the organization, its culture and capabilities and also the nature of the risks that can exert an effect on the achievement of objectives.

Tailoring can be achieved by the manner in which the risk management framework and process are developed and implemented. Tailoring does not refer to deletion of elements, rather it relates to how risk management is conducted and adapted to the organization. In SMEs, the implementation of risk management will need to align with the governance and decision-making of the organization, this may include few formal policies, a flexible governance structure and managers with responsibility at multiple levels and in multiple areas.

Like a well-made garment, a tailored implementation of risk management should fit the organization, its culture and needs and be both familiar and comfortable. When risk management is tailored to the organization, it will be fully integrated (Principle B) and part of all decision-making (Principle C).

Principle H: Risk management takes human and cultural factors into account

The standard indicates that risk management recognizes the capabilities, perceptions and intentions of people who can influence the achievement of an organizations objective. Human and cultural factors influence how risks are perceived and how risk treatments will be implemented. An organization's culture is often influenced by "tone at the top", how managers and organizational leaders approach and resolve problems, decide on which risks to pursue or avoid and set the risk attitude of the organization. An example is an organization that is an aggressive new business that operates with high levels of uncertainty. In order to be successful such organizations need to be very explicit about their risk appetite and risk tolerance and to communicate these to decision-makers. The culture of such an aggressive organization is one where limiting controls are regarded as an impediment to achieving objectives. If this is the cultural and human dimension of the organization, then where there are mission critical controls like compliance with legal requirements, risk management will need to be tailored (Principle G) so that it is dynamic, iterative and responsive to change (Principle J).

Risk management, in accounting for human and cultural factors, should include monitoring and review at every stage to ensure that the risk treatments that are decided upon are implemented effectively and that they result in the desired change in risk magnitude.

Principle I: Risk management is transparent and inclusive

In this principle, transparency can be achieved through effective communication of the risk criteria, the risk management framework and the risk management process. For this to be inclusive, the internal and external stakeholders should be included in both communication and consultation. Transparency and inclusiveness depends on ethical behaviour and the communication of accurate and complete information with integrity and clarity.

There are certain aspects of risk management that may be exempted from this requirement for transparency and inclusiveness. Risks associated with new products or services, profit margins, debt and the expansion or contraction of the organization may be confidential and it may be impossible to share them or include external stakeholders in any discussion of the risks and their magnitude.

Transparency and inclusiveness can be assessed through consultations with internal and external stakeholders.

Principle J: Risk management is dynamic, iterative and responsive to change

This principle is linked to Principle F, using the best available information, and Principle D, addressing uncertainty. To be effective, risk management must respond to changes in the internal and external contexts. Changes may include new competitors, changes in prices of inputs to your product or service, or changes to taxes and tariffs. There may also be changes in cultural and human values (Principle H) that affect the internal stakeholders in a way that changes a risk. Effective Risk management needs to be able to detect and respond to changes that lead to changes in risks.

If you developed a comprehensive context statement when you developed the risk information for your organization, one test of your alignment with this principle would be to periodically compare this initial context with the current context and determine whether your risk management process, framework and risk information responded to the changes in context you have detected.

Principle K: Risk management facilitates continual improvement of the organization

This principle indicates that risk management enables an organization to continually improve its performance. Organizations improve by responding to changes in context (internal and external) so that they can continue to achieve their objectives when circumstances change, or improve their achievement of objectives when changes in context provide enhanced opportunities. Risk management also facilitates improvement by providing a mechanism to assess whether changes in the organization will enhance or degrade the

achievement of objectives. Risk assessment methodologies such as those described in IEC 31010:2009, include tools to assess the organization's resilience to changes. It is possible, using scenario analysis for example, to determine how the organization can improve performance if input or operating costs are lowered.

Continuous improvement of the organization includes the review and improvement of the risk management framework and risk management process. As the organization becomes familiar with risk management, the process and framework will evolve and mature so that it can become more fully integrated into the organization. Monitoring of the objectives, for example those related to profit, quality, sales growth and cash flow will provide managers with a measure of the effectiveness of risk management. The risk information should be evaluated to determine how the risk treatments could evolve to improve results. This is how risk management facilitates the improvement of the organization.

B.2 Guidance on transitioning to align with ISO 31000:2009

B.2.1 Clarify your objectives for the transition

Your reasons for making a transition from your existing approaches to risk management to an implementation that is aligned with ISO 31000:2009 should be clear. These objectives may include:

- Increased consistency so you can compare risk magnitude from year to year and in all parts of the organization.
- Increase the achievement of objectives, such as net profit, market share, time between failures, quality of the organization's products or services.
- Consistency with global approaches to demonstrate to clients, governments, investors and insurers that your risk management is aligned with the global standard.
- Increased clarity and accountability for using risk information to inform decision-making.
- Fuller integration of risk management with business processes.

The objectives for the transformation need to be developed by the senior management of the organization, evaluated, approved and then provided to managers and decision-makers.

B.2.2 Analyse your current risk management activities

All organizations manage risk, it is how they come into existence and how they continue to operate. The early or immature forms of risk management include “fire-fighting”, a term used to describe responding when an apparent threat to the organization is clear and when risk treatment is essential in order for the organization to survive. Risk management may also include narrowly focused risk management where risks, like credit risk or market share risk, are managed by a team, but there is no effort to identify and manage all risks that can affect the achievement of objectives in positive or negative ways.

When analysing your current risk management, identify written policies and procedures relating to risk, audits, reports or other studies about how the organization identifies threats and opportunities and responds to them. If there are unwritten practices or policies, for example to always ask the owner before making a large purchase with the organization’s funds, these too should be collected and evaluated. Once you have a comprehensive picture of all the risk management activities in your organization, then you can proceed to the next step, which is to look for gaps between the risk management that you have and an implementation of risk management that is aligned with ISO 31000:2009.

B.2.3 Conduct a gap analysis with ISO 31000:2009

Using the information on your current risk management practices compare what you have and what ISO 31000:2009 recommends. Examples to look for include clear, explicit, formally approved commitments to:

- Use risk management as an input to decision-making.
- Provide resource (people and money) to enable the risk management function.

- Provide training in risk management as required.
- Include risk management responsibilities in position descriptions.
- Create and implement a risk management framework.
- Create and implement a single risk management process for the organization that includes the relationship among the elements of the process and also shows the flow of the analysis, from start to finish for each cycle (annual, monthly etc., as appropriate for the context).
- Review risks periodically (often annually) and to implement changes that can improve the risk management capability of the organization.
- Create a risk treatment plan that is monitored and which has a clear process if treatment is not implemented as planned, or to seek alternatives when treatment has not had the intended effect on the achievement of objectives.
- Seek explicit risk information on every significant decision at all levels of the organization.
- Align your risk management with the 11 principles in ISO 31000:2009.
- Monitor the context of the organization and as the context changes, review the risks and remove risks when they are no longer relevant and add new risks as they become relevant.

Determine where there are gaps, and analyse what changes are appropriate to tailor ISO 31000:2009 to your organization. Note however that the principle on tailoring risk management does not imply choosing to implement only parts of the standard, it suggests rather that all of ISO 31000:2009 is implemented in every case, from a one to two day risk analysis of a small project to a large scale annual risk management program for a medium-sized organization. Tailoring applies to the complexity, cost and level of detail of the risk management programme. In order to implement effective risk management that is aligned with ISO 31000:2009 you will need to ensure that all elements of the standard, including principles, process and framework are in place for your organization.

B.2.4 Develop a plan for the transition

Developing a plan to transition to risk management that aligns with ISO 31000:2009 follows the same process as any well-formed plan. This plan should be developed in the light of the guidance in Clauses 4.3.4 regarding

the need for integrating risk management into organizational processes) and 4.4.2, implement the risk management process in a way that aligns with the risk management process described in Clause 5 of the standard. An effective transition plan includes the following elements:

- a clearly stated objective for the transition,
- a budget with a contingency,
- a time line with milestones and review stages where the plan can be changed to respond to new information or changes in context,
- clear accountability for all involved,
- a mechanism to test whether the completed plan has achieved the stated objective,
- describe in detail, each step of the transition plan,
- develop measures that can track the completion of each step in the plan,
- recognize or reward the individuals involved when the plan is implemented successfully.

The plan should fit with the size, complexity and culture of your organization and be written in a way that the team responsible for the transition is familiar with and can follow.

B.2.5 Implement the transition plan, monitor progress and make adjustments when required

Once again implementing the risk management transition plan should be done in the way that any well-formed plan is implemented. The objective of the plan is paramount and when the implementation is not aligning with the delivery of the stated objective, then the plan needs to be reviewed. There should be clear criteria that trigger a review or realignment of the plan. Such triggers can be a delay of more than a set time or percentage of the plan or an increase in costs of either a specific amount or a percentage of the overall costs of implementing the plan.

B.2.6 Monitor the implementation of the new risk management process and framework

The transition from the risk management that the organization had in place initially to risk management aligned with ISO 31000:2009 was done to accomplish specific objectives established by the organization's management. As noted elsewhere in this guide, the implementation of risk management, including the process and the framework, should be monitored and reviewed, and where the results of this monitoring indicate that changes are required in order to achieve the objectives for implementing risk management, these adjustments should be made and tested.

B.3 Guidance on communication and consultation

There is a clear difference between communication and consultation. Although the terms are often used together they are quite different. Communication is imparting or sharing of information by any means (e.g. written, spoken, electronic) and can be bilateral, such as a discussion, letter or telephone call or multilateral, which includes meetings, published documents or articles in magazines and newspapers, or mass email communications or information sharing on social media.

Consultation is a specific form or type of communication. It is a bilateral process, and is generally conducted by an individual or organization (for our purposes called the first party) to gain information from a stakeholder or interested person, community or group (which we will call the second party or parties) regarding a decision or proposal that the first party is considering. Consultation is done as an input to decision-making, however it is not shared decision-making. Consultation is where the second party communicates with the intent to influence the first party to take a particular decision or to choose a particular outcome or path forward.

Channels of communication

In any communication, the organization that opens the communication is obliged to ensure that the communication is in a form that is convenient, familiar and effective for the other parties. The parties who are the primary audience for communication are often referred to as the “target audience”. This starts with using language that is familiar to this audience but also includes the use of channels that they are familiar with and value. The communication may be public or private meetings, letters (paper or electronic), newspapers, magazines, web sites, flyers or notices that are delivered directly to the other parties or are delivered to areas and using methods that can reasonably be expected to reach the target audience.

While social media (Facebook, Twitter, Instagram, Pinterest) has emerged as a major channel for communicating with some demographic groups, the characteristics of the target audience should be assessed before using social media as a means of communicating with relevant stakeholders. Some large organizations have internal social networks just for employees, however, enabling this can be costly and is not well suited to SMEs.

It is essential that the message arrives as intended. Use clear and simple language and focus on the core message to be communicated. In places where multiple languages are used, ensure that the translation of your message has been done accurately and that the sense of the message has been included, not just a mechanical, word-for-word translation. Metaphors, slogans, phrases or “nicknames” may have very different and unintended meanings when translated. In face-to-face communications, ensure that your message is being communicated clearly and enunciated correctly. Use of jargon or slang should be avoided.

Verifying the effectiveness of communication

In any communication it is possible that the message can be garbled or misinterpreted. To avoid this, a process to assess the effectiveness of the communication is required. This can be a survey or an interview with members of the target audience. Principle H, which says risk management should take human and cultural values into account, is especially important here.

Complex and sensitive subjects

When communicating complex information (e.g. likelihoods of an event, potential for inter-related or consequential events) use the simplest terms possible. If graphics or charts are used, be sure that these are in a form that is familiar to the target audience. If you are communicating potentially negative consequences, you should use an expert and test your messages with a small group from the target audience before launching a broad communications initiative. The remotest possibility of illness, injury or incapacitation, however unlikely, needs to be communicated extremely carefully so that the likelihood of the event is as apparent to the target audience as the consequence that is being communicated.

Clarifying the nature of consultation

A common failing of a consultative approach is when the target audience (the second party) believes that they are providing direction or instructions to the first party. Confusion of this sort can destroy the value of the consultation. The scope and nature of the consultation should be clear at the outset, if the consultation is about the timing or location of an activity, like construction, it should be made clear that the construction will proceed in any event and that the purpose of the consultation is simply to assess the impact of timing and location.

The use of surveys

The use of surveys is emerging as a way to obtain the views of stakeholders. This form of consultation has limitations that need to be carefully considered before choosing this approach. The most effective, and most expensive, are telephone surveys where you are able to confirm that the person providing the information is in the target audience you wish to reach. While it is possible to decline to participate in a telephone survey, the company or organization conducting the survey can continue to make calls until they have a result that is a statistically valid reflection of the input from the target audience or audiences. When surveys are mailed (paper or electronic) and participation is by “opting in”, there may be a bias in the results and this bias needs to be assessed and considered when the results of the consultation are compiled by the organization.

Non-governmental organizations and public interest groups have traditionally been consulted in large public meetings. Stakeholder groups more accustomed to large public meetings may not see using surveys to consult with stakeholders as transparent or credible. You will need to determine the consultative approach that can work effectively to consult those stakeholders who are key to a risk management engagement.

Tone

Consultation in public meetings can be an ineffective mechanism if any party behaves rudely or is intemperate. When choosing to consult, the organization needs to consider this aspect of public meetings when choosing how to go about the consultation. A meeting where there is anger and incivility will not function effectively as a means for the organization to effectively consult stakeholders. It is important that any public meeting open by stating the rules for the meeting and for having an option, like adjournment, should the consultation become unruly or unproductive.

Be clear on disposition of inputs

Many individuals and groups interpret consultation as an opportunity to direct an organization and approve or disapprove of the matter being consulted on (e.g. new manufacturing facility, increases in traffic to and from a location, increased water use or waste discharge). The context of the consultation must be clear to all participants and the organization needs to be prudent in any statements made to avoid confusion on what has been agreed to and how the input from the stakeholders has been considered. Casual remarks or observations made by representatives of the organization should be avoided as any statement made by a representative of an organization may be taken as a formal commitment or policy of the organization. Similarly a consultation will not be effective if the organization makes statements that can be misinterpreted by stakeholders and creates an expectation that change has been agreed to, when it has not.

B.4 Guidance on risk treatment

Overview

As noted in the standard, risk treatment involves selecting and implementing one or more options for modifying a risk, by providing a new control, or by modifying an existing control. Effective risk treatment begins by assessing the option being considered and determining if it will modify the risk and result in a risk level that is tolerable.

Risk treatment can take any of the following forms:

- Avoiding the risk by ending, or not starting the activity which is associated with the risk (e.g. not producing products that require storage, handling or disposal of hazardous materials).
- Increasing the risk to pursue an opportunity (e.g. opening a new location, developing a new product or service).
- Removing the risk source (e.g. moving your organization to a jurisdiction with a different tax regime).
- Changing the likelihood (e.g. introducing an additional safety control for an activity).
- Changing the consequences (e.g. moving to automated manufacturing where the risk to human health and safety is too great and machines or robots can produce the product and ensure that employees are protected from injuries associated with the manufacturing process).
- Sharing the risk with another party (e.g. purchasing insurance or using contractors or financing partners).
- Retaining the risk by informed choice (e.g. a criteria based determination that the current risk level is acceptable).

Selecting risk treatment options

When risk evaluation has determined that a risk requires modification, a risk treatment is selected. As identified in the Bowtie analysis (see Annex A.4), controls can act before a “loss of control” condition occurs, or after. Risk treatments that act in advance of a loss of control event are designed to reduce the likelihood of the event or its consequences should it arise. Please review [Figure A.1](#), which provides a comprehensive overview of the risk treatment process.

Example

As an example of pre and post event risk treatments, consider that the “loss of control” or risk event is that a vehicle loses traction and skids while travelling at high speed. Risk treatments that act before the loss of control occurs includes speed limits, signs warning when skids are more likely after a rain storm or snowfall, to programmes that reduce the likelihood that a driver is impaired by alcohol or drugs. All of these act to reduce the likelihood, consequences or both of a vehicle skidding out of control. The post event controls are in place to prevent certain potential consequences. Guardrails at the side of the road can prevent a skidding vehicle from falling over a cliff or ravine. These cannot prevent the skid from occurring and are only of value after a vehicle and driver has lost control. Similarly seat belts and air bags can act to reduce injury from a collision but do not treat the risk that the vehicle itself will be damaged. These are specific risk treatments to prevent injury or loss of life after the skid has commenced. There are other post event risk treatments including ambulances, emergency hospital treatment for reconstruction or physiotherapy. All of these are post event treatments after the loss of control event and a specific consequence, in this case injury, has occurred. These post consequence risk treatments are remedial and act in the same way as clean-up operations after a spill of hazardous or noxious materials.

Selecting risk treatments will be informed by the maturity of the implementation of risk management. The first assessment that needs to be made is whether risk treatment will be preventative or remedial, that is, proactive or reactive interventions. It is important to record and understand the current controls that are in place regarding this risk and whether they are preventative or remedial. Several of the principles of risk management set down in the standard (and explained in Annex A.4) are relevant to risk treatment. The principle that risk management creates and protects value is a critical one to consider here. The risk treatments that may be used should be evaluated in the light of their cost and the value of the change in risk that they can deliver. An existing risk treatment or control can be adjusted so that the risk level becomes tolerable.

All aspects of a risk treatment need to be considered, here Principle H, taking human and cultural factors into account is important. Determine not only the cost and benefit of the control, but also the training and monitoring costs

that may be required in order for the control to operate effectively. The person responsible for implementing the control should have the authority to ensure that the control is implemented, as well as the knowledge, skill or training to implement the control effectively.

Preparing risk treatment plans

When risk treatment has been identified, the next step is to develop and execute a plan to ensure that the specific risk treatment is implemented and that the risk treatment has had the intended effect on the magnitude of the risk. One approach to creating a risk treatment plan is to develop a table. [Table B.1](#) is an example of a table that could be included in a risk treatment plan.

Table B.1 — Example of risk treatment table

Unique ID (number)		
Risk category		
Description of potential impact		
Current status of treatment (functioning effectively, ineffective, not implemented)		
Action required to have treatment operate effectively		
Initial impact and likelihood assess- ment		
Desired or target impact and like- lihood assessment to be achieved after treatment		
Detailed description of risk treat- ment		
Person accountable for implement- ing the treatment		
Date or frequency of implementation of risk treatment		

Table B.1 *(continued)*

Describe performance measure that assesses whether treatment is in place and operating (evidence or other measure)		
Rationale, notes or comments		

B.5 Guidance on risk management documentation

B.5.1 Overview

Clause 5.7 of ISO 31000:2009 describes the importance of, and a process for, recording the risk management process. Record-keeping throughout the risk management process is essential. Records kept for risk management fall into several key categories:

- The Risk Management Framework and accompanying documents (policy, objectives, resourcing). Documents setting out accountability and authority, or procedures and guidelines.
- Policy documents and registers of regulatory instruments.
- The external and internal contexts summary/statement.
- A checklist of alignment with 11 principles.
- A risk register including information on risk levels, dates when the information was created or verified, risk owners, risk sponsors and information on the consistency and scope of the information.
- A controls register, including the status of controls, control owners and control effectiveness.
- Risk treatment plans including accountability, and monitoring information on progress and effectiveness.

B.5.2 Risk management framework, policy and supporting documentation

Chapter 3 provides very detailed guidance on the risk management framework. The notes here can be used as a checklist to identify key aspects of what should be recorded and retained.

- Risk management policy
 - a comprehensive list of senior management's objectives for implementing risk management,
 - a clear commitment to provide specific resources (staff and money) to support the implementation and execution of risk management,
 - a clear summary of the results that are expected and the performance measures for these results (e.g. profitability, losses, organizational value, share price, market retention or growth, etc.), and
 - a clear commitment to align with ISO 31000:2009 and its 11 principles.
- Risk management procedures tools and training
 - a comprehensive summary of tools including a record or register of risks, a register of controls, a risk treatment plan, guidelines and handbooks that will support the ongoing implementation of risk management,
 - a description of the annual risk management cycle, including who will complete each stage of the risk management process as set out in the standard and at what time the in the annual planning cycle the work will be completed,
 - an inventory of training that is available to risk management practitioners and also to decision-makers and other staff. This may include online training courses or internal training that will be made available, and
 - a clear description of the methodology to be used for each element of the risk management process including details on timing, reporting and accountability for entering information into the risk register.
- Context statements
 - this is a clear and complete description of the internal and external contexts for each risk management engagement. This statement may be in point form but should be comprehensive and include not only

statements of fact like company size, market competitors and tax treatment, but also inferences and assumptions.

B.5.3 Checklist of eleven principles

This is an inventory or table that provides evidence of the documents, controls, actions, initiatives and programmes that give effect to the principles. This list should be dated and should be monitored as a part of the overall programme of monitoring and review.

B.5.4 Risk register or inventory of risk information

This is usually a table of risk information, usually an electronic document or spreadsheet. There are some characteristics that any inventory of risk information should include

- A history of amendments and updates that shows the date and the person who made the updates.
- For each risk
 - The category or group the risk is found in (e.g. financial, market, regulatory).
 - The name of the risk.
 - A description of the risk or risk event.
 - An inventory of the risk causes or risk drivers.
 - An inventory of potential consequences of the risk.
 - The name of the risk owner or risk sponsor, the person responsible for tracking the risk within the organization and for ensuring that the risk information is current and relevant.
 - An inventory of the controls that act on each risk and the control owner.
 - The current risk magnitude (likelihood and impact).
 - The desired, preferred or “target” risk magnitude.
 - What action is required in regard to each risk, who is accountable for completing and verifying this action (these two functions must be segregated) and on what date is it required.

B.5.5 Controls register or inventory of controls

This is usually a table of controls, those things that modify risk.

The controls should be grouped by their category (e.g. financial controls, performance controls, security controls, etc.).

The inventory of controls should identify for each control:

- The “Five Ws”
 - What is the control – a description.
 - Where does the responsibility for the control lie.
 - Who is responsible for executing the control (control owner).
 - When is the control performed (e.g. every purchase, daily, weekly, when refinancing is planned etc.).
 - What risks does the control modify.
- Identify if the control is preventative or detective.
- Identify if the control is automated or manual.
- What are the compensating controls that detect if a control has failed and identify the actions that will be taken when a control fails.
- The person or mechanism that monitors the control.
- Performance measures or outcomes that can assess and track the effectiveness of the control.
- The path for reporting control weaknesses or control failures and the criteria for escalating a weakness or failure to management for action.
- The span of the control (e.g. entity level, high level or transaction level).

B.5.6 Risk treatment plans

This is a comprehensive plan that identifies actions that will be continued or undertaken to treat the organization’s risks. The risk treatment plan can be a simple table as shown [Table B.1](#). More details on what they should include and how they work is found in Annex [B.4](#).

B.5.7 Records — Essential considerations

Records can take many forms, from paper-based file systems with complex access and control systems to a series of electronic records maintained on an individual computer, or a network server or a service on the internet (commonly called “cloud storage”). No matter how an organization creates, manages, protects and accesses its records there are a series of attributes that all records systems should have. The key attributes of effective record-keeping are described below.

B.5.7.1 Accountability and governance

Any record management system has to have a mechanism (a control, person or group) that is responsible for creating, protecting, maintaining and controlling access to the records. If a paper-based system is chosen there can be a physical “file room” with filing cabinets, controls (like keys or passwords) and security (including fire suppression, prevention of access by unauthorized individuals, and logs of access use.) If electronic records are maintained, there is still a need for accountability and governance, but this can be implemented on the computer system itself.

B.5.7.2 Control over access

No matter whether a paper-based or electronic records system is used, control over access and information security is essential.

Specific criteria need to be developed that identify who can create records and when and how this will be done. Criteria can also be developed on how it is logged into the system and how access and changes are logged. There needs to be adequate controls to ensure that only those who are approved to do so, can create and update records. Many systems provide “read-only” access to some records and in support of the transparency principle, risk management records should be accessible to internal stakeholders provided that records with personal information and records that are confidential to the organization are adequately secured.

There should be an access and change log for the files, for paper-based systems this was simply a paper form, computer systems can be set up to limit the ability to make changes to members of an approved group and can log the names and dates when records are modified.

Electronic records can be accessed remotely via internal or external networks. This access should be implemented in accordance with the security and access protocols.

B.5.7.3 Security and integrity

Risk management records should be secured against unauthorized access and also be secured against harm. There are various ways of backing up or copying electronic records to a second computer in a secure location. The records should be secured against disaster (fire, flood, explosion) either by directly securing the location or by having an up-to-date complete copy of the records in a different but also secured location. Contingencies should be provided for where uninterrupted access is critical to the organization.

B.5.7.4 Search capability

It must be possible to search the records quickly and in a way that provides a user with the record or subset of records that meet certain criteria that the searcher has established. The Internet's success as a store of information is wholly dependent on the availability of "search engines" (e.g. Google) that can scan millions of records for specific pieces of information or images that meet certain search criteria. Paper-based systems can also be designed for easy searching (e.g. searching for purchase records of a certain range of dollar values between two dates). The Dewey Decimal system or the Library of Congress System are both used by libraries around the world to categorize the storage of books in a way that makes finding the information a user is looking for easily and reliably.

Whatever system is used to make the records searchable it should be easy to use, reliable and stable.

The search capability should be developed so that it can be used both by those who need access to investigate and update the information and those who will only have access to read or review the information.

B.5.7.5 Reliability

The records need to be created, maintained and made available in a manner that ensures that the information is reliable. The controls over governance, access, security and integrity set out above should provide for this. The records, whether paper or electronic need to accurately reflect the risk information about the organization. Those responsible for the records need to ensure that unauthorized changes are prevented.

B.5.7.6 Compliance

In many jurisdictions there are statutory or regulated requirements regarding the creation, retention and management of risk-related information. Records must always be managed so that these requirements are met, and that this compliance can be verified.

B.5.7.7 Specialized software

There are several companies that sell software that has been designed for keeping records of risk management information. The process of reviewing and acquiring software should only proceed after the needs of the organization in all the areas set out above have been defined and approved by the organization's management team. The organization should ensure that it acquires the software service that it requires and that configuration of the software so that it meets the organization's needs is included. Modifying complex software after purchase can increase the price significantly.

B.5.7.8 Retention, disposition and destruction

The governance framework for the records system should set out the process regarding the retention, disposition and destruction of records. There should be a systematic process that specifies when records should be removed from the active records system. Records that have been removed from active systems may have to be archived or retained in accordance with statutory or regulatory requirements. Records that are no longer required for any purpose should be disposed of. Disposal of records should be formally authorized and the governance system for records should provide the organization with adequate assurance that records that are disposed of or destroyed are no longer required for the organization. Where the information in the records is proprietary or contains personal information these records should be destroyed in a manner that ensures that the records cannot be recovered. There are systems that provide for the complete destruction of both paper and electronic records and these should be utilized when appropriate. Records that are destroyed should include all copies of the record wherever they are held in the organization, including in electronic backup systems.

Annex C — Guides, handbooks and references for SMEs

C.1 Guides and handbooks for ISO 31000:2009

ISO

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

Australia and New Zealand

SA/SNZ/HB 436:2013, Risk Management Guidelines — Companion to AS/NZS ISO 31000:2009

SA SNZ/HB 89:2013, Risk Management — Guidelines on Risk Assessment Techniques

AS/NZS 5050:2010, Business Continuity — Managing Disruption Related Risk

SA/SNZ/HB 141:2011, Risk Financing Guidelines

SA/SNZ/HB 158:2010, Delivering Assurance based on ISO 31000 Risk Management — Principles and Guidelines

SA/NZS/HB 203:2012, Managing Environment-Related Risk

SA/SNZ/HB 246:2010, Guidelines for Managing Risk In Sport And Recreation

SA/SNZ/HB 266:2010, Guide for Managing Risk in Not-For-Profit Organizations

SA/SNZ/HB 327:2010, Communicating and Consulting About Risk

Canada

CAN/CSA 31001:2011, Implementation Guide to CAN/CSA ISO 31000:2010 Risk Management — Principles and Guidelines

UK

BSI 31100:2011, Risk management. Code of practice and guidance for the implementation of BS ISO 31000

Ireland

NSAI NWA 31000:2010, National Guidance on Implementing I. S. ISO 31000:2009 Risk Management — Principles and Guidelines

Austria — Available in German and in English

ONR 49001:2014, Risk management for Organizations and Systems - Risk Management - Implementation of ISO 31000

C.2 Valuable reference books on risk management

Fraser, J. and Simkins, B.J. 577 pages. 2009. Enterprise Risk Management: An Introduction and Overview, in Enterprise Risk Management, John Wiley and Sons, Inc., Hoboken, NJ, USA. ISBN: 978-0-470-49908-5

Fraser, J., Simkins, B.J. and Narvaez, K., 688 pages. 2014. Implementing Enterprise Risk Management: Case Studies and Best Practices. John Wiley and Sons, Inc., Hoboken, NJ, USA. ISBN: 978-1-118-69196-0

Bernstein, P. 586 pages. 1998. Against the Gods, The Remarkable Story of Risk, John Wiley and Sons, Inc., Hoboken, NJ, USA. John Wiley and Sons, Inc., Hoboken, NJ, USA. ISBN 978-0-470-49908-5

Jachia, L and Nikonov, V. 118 pages. 2013. Risk Management in Regulatory Frameworks: Towards a Better Management of Risks. United Nations, NY ISBN-10: 9211170680

C.3 Books about risk

Duffey, R., and Saull, J. 526 pages. 2008 Managing Risk, The Human Element. John Wiley and Sons, Inc., Hoboken, NJ, USA ISBN: 978-0-470-69976-8

Gardner, D. 407 pages. 2008. Risk. Why We Fear The Things We Shouldn't. McClelland and Stewart. Toronto, ISBN 978-0-7710-3259-2

Ralston, B, and Wilson, I. 258 pages, 2006. The Scenario Planning Handbook, Ralston and Wilson, Thomson Southwestern, Indiana ISBN 978-0-324-31285-0

Talbot, J. and Jakeman, M, 471 pages. 2008. The Security Risk Management Body of Knowledge. Risk Management Institution of Australasia, Carlton South, VIC. ISBN 978-0-9804777-0-2

Taleb, N. 316 pages, 2005. Fooled by Randomness, The Hidden Role of Chance in Life and Markets. Random House, New York, ISBN 0-8129-7521-9

Slovic, P. 473 pages. 2000 The perception of risk. Risk, society, and policy series. Earthscan Publications London, England. ISBN-13: 978-1849711487

Van Hecke, M.L. 2007. 256 pages. Blind Spots, Why Smart People do Dumb Things. Prometheus Press ISBN: 1-59102-509-5

With empirical evidence showing that around half of SMEs close down before completing their fifth year, it is clear that operating a business can be a risky endeavour.

ISO 31000 : Risk management – a practical guide for SMEs describes the requirements of ISO 31000, and provides guidance to identify and implement risk management strategies.

**International Organization
for Standardization**

Ch. de Blandonnet 8, CP 401
CH-1214 Vernier, Geneva, Switzerland

International Trade Centre

Palais des Nations,
CH-1211 Geneva 10, Switzerland

**United Nations Industrial
Development Organization**

Vienna International Centre, P.O. Box 300,
AT-1400 Vienna, Austria

iso.org

© ISO, 2015
All rights reserved

ISBN 978-92-67-10645-8

