



ISO 31000:2018

Risk management

A PRACTICAL GUIDE



UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION



Documents

Document Sharing Hub

Copyright protected document

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

© ISO 2021

ISO copyright office

CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org
Published in Switzerland

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

Contents

Foreword	5
Preface	7
Introduction	9
ISO 31000 Guidance Handbook	11
1. Using the ISO 31000 risk management principles	11
2. Leadership, commitment and responsibilities	13
3. Risk management framework	25
4. Risk management process	39
5. Effectiveness of the risk management program	57
6. Continual improvement	61
Annex A	66
Example of gap analysis	66
Annex B	68
Example of risk categories	68
Bibliography	71
ISO documents	71

Foreword

If risk is the combination of opportunities, threats and future uncertainty, then risk management is an essential discipline for informed decision-making within all organizations. Moreover, past years have borne witness to all forms and scale of risk, across the spectrum of sizes and potential impacts; these range from the challenges and opportunities seen in day-to-day management, through to major events, such as logistic disruptions, political unrest, large-scale data breaches, and unprecedented lockdowns triggered by global pandemics. Each of these has resulted in an increased recognition and appreciation of the absolute value of risk management.

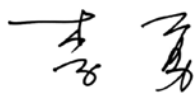
All events, whether large or small, can have a strong effect on organizations, businesses and the markets and economies in which they operate. Given the present uncertainties, it is hardly surprising when organizations struggle to identify and manage their risks. Managing risk effectively is how all organizations bring greater certainty into their planning and activities.

To serve this highly relevant need, ISO 31000:2018, *Risk management – Guidelines*, has been designed to assist organizations by providing guidance and direction on how to integrate an effective decision-making framework into their governance, leadership and culture. Organizations that manage risk well not only survive but thrive.

As a foundation standard on risk management, ISO 31000 explains the fundamental concepts and principles of risk management, describes a framework, and outlines the processes of risk identification and management. ISO 31000 is supplemented by IEC 31010:2019, *Risk management – Risk assessment techniques* and ISO 31073, *Risk management – Vocabulary*; these two ISO standards contain valuable information and guidance on risk management techniques, as well as the terms and definitions. To further assist organizations in implementing risk management, we have now added *ISO 31000:2018 – Risk management – A practical guide*, to the family of standards.

This handbook was written at the request of the ISO Technical Committee, ISO/TC 262, *Risk management*, to provide an implementation guide to the International Standard on risk management, ISO 31000. The aim of this handbook is to assist organizations seeking guidance on how to integrate risk management into their activities. The handbook therefore includes information on risk management principles, the framework, roles and responsibilities, planning, processes, communication, monitoring and review, and continual improvement. This handbook was written by experts from Working Group 6 under the ISO/TC262, *Risk management*, for those who are either starting their risk management journey or require additional guidance on how to improve their current, risk management programme.

We hope this handbook, jointly published by the International Organization for Standardization (ISO) and United Nations Industrial Development Organization (UNIDO), will support your organization's effort in creating and protecting value to assist in realizing the multiple benefits offered by ISO 31000.



Li Yong

Director General

UNIDO



Sergio Mujica

Secretary-General

ISO

Preface

This handbook aligns with ISO 31000:2018, *Risk management – Guidelines*. It is intended to guide organizations to implement and practice risk management. For brevity, this handbook will refer to this International Standard as ISO 31000. This handbook is consistent with the contents of ISO 31000; however, it does not replicate the ISO 31000 structure. It is intended to guide organizations to implement and practice risk management.

Any feedback or questions regarding this document should be directed to the user's national standards organization.

Introduction

Implementing effective risk management supports quality and success, and potentially the good of society.

ISO 31000 defines risk as the effect of uncertainty on objectives. This can include the organization's purpose, vision, and values as well as the goals and targets articulated at different levels in the organization. They can also include the factors that are important to a particular decision.

The International Standard provides a common approach to managing any risk and is not industry or sector specific. It provides guidance to assist organizations in integrating an effective risk management program into all their activities and functions.

This handbook expands and provides context to the clauses in ISO 31000. It provides advice regarding introducing and implementing risk management, including how to create and protect value for stakeholders. The handbook demonstrates how to:

- ▶ Use the principles of effective and efficient risk management in the way risk is managed;
- ▶ Develop a plan for integrating risk into an organization's existing arrangements;
- ▶ Understand how organizational culture influences the design and implementation of risk management;

- ▶ Confirm that the need for effective risk management is considered when changes affect the organization;
- ▶ Apply the risk management process to identify, analyse, evaluate, and where required, to treat risk;
- ▶ Communicate and consult with stakeholders;
- ▶ Monitor and review the risk management plan and process; and
- ▶ Continually improve based on context and lessons learned.

As with ISO 31000, this handbook can be used to manage risk in all types of organizations. It applies to an organization, and to its activities. It applies to organizations that are considering implementing ISO 31000 or seeking improvement of existing risk management.

ISO 31000

Guidance Handbook

1. Using the ISO 31000 risk management principles

The risk management principles link the framework and practice of risk management to the organization's strategic goals and objectives.

The core principle and purpose of risk management is that it creates and protects value. The principles are foundational in all aspects of risk management and have been incorporated within the sections of this handbook.

Risk management is integrated: Risk should be considered during normal business activities and decision-making throughout the organization and integrated within the organization's overall management system.

Risk management arrangements should be structured and comprehensive: A structured framework assists organizational understanding of roles and responsibilities and provides consistent procedures. These include procedures to identify, understand and treat risk and communicate information.

Risk management is customized: This principle encourages organizations to customize risk management to their organization's objectives and needs.

Risk management is inclusive: Timely and appropriate engagement of stakeholders enables a wide range of views to be considered as part of risk management, resulting in better-informed decisions.

Risk management is dynamic: As an organization's context and circumstances change over time, so will its risks. This principle reinforces that risks are to be periodically reviewed to ensure that they are addressing organizational objectives.

Best available information: Informed decision-making requires relevant and accurate information from the organization as well as from other sources. Risk management should reflect and consider the input of internal and external stakeholders.

Human and cultural factors: Risk management involves collaboration and the engagement of stakeholders. This can result in understanding the human and cultural factors most important to organizational success. This principle also refers to taking unique circumstances and human needs into account when integrating risk management into the organization and developing appropriate risk management processes.

Continual improvement: This principle encourages an organization to continually monitor, review and improve risk management processes to ensure their relevance, efficiency, and effectiveness in support of the organization's overall performance.

2. Leadership, commitment and responsibilities

2.1 Overview

Managing risk adds and protects value by enabling organizations to achieve their objectives more effectively and efficiently, and with greater long-term certainty. Organizations that continue to succeed are those with the ability to forecast and prepare for risk.

Implementing and enhancing risk management supports an organization's objectives and creates and protects value for the organization. Implementation begins with understanding what value means to the organization. The value of risk management is expressed in many terms such as market share, profit, service management, project delivery or social services. No single risk management model achieves these goals. Each organization is responsible for identifying value, which depends directly on the mission, vision, strategic objectives, and the primary activities of the organization.

The value of risk management is sponsored by the organization's oversight body, put into effect by top management and risk owners and applied across the organization through a common framework. This framework can vary widely among organizations but typically involves leadership and commitment, resources, defined accountabilities, communication, plans, actions, and processes.

2.2 Role of risk management in decision making

2.2.1 General

The key to effectively managing an organization and creating value is informed, logical, structured, and consistent decision making. To weigh different options in the pursuit of its objectives and desired outcomes, decision makers select from choices based on experience, reason, and best available information. The risk management process provides a basis for informed decision-making to determine one course or courses of action. Risk management is a decision-making discipline that is to be integrated into all aspects of an organization. The method selected to assess risk can assist the decision maker to make an informed decision. Decision making is a fundamental part of strategic and operational management and controls of a well-run organization.

Good decision making is based on a clear understanding of the context and underlying uncertainties in achieving objectives. Organizations will face multiple risks, some with compounding or cascading effects. Both the nature of individual risks and the interaction between risks can be identified and understood to support informed decision-making, and better recognize potential unintended consequences of decisions. Developing and evaluating alternative scenarios reduces uncertainty in decision making and illuminates unknowns that can occur. Timeframes and the extent of impact on the organization determine the criticality of decision-making processes.

EXAMPLE – Case study

To get its products to market safely and profitably, a petroleum refinery company needs to understand risks related to physical design, operations, safety, the environment, quality, reputation, regulation, supply chain, and economics and the interactions between them.

To be effective, risk management needs to be understood within the context of the governance, compliance, processes, and operating procedures of an organization. For organizations to achieve their strategic and operational objectives, risk management is to be aligned with the governance structures, mission, values, and culture of the organization.

For an organization to thrive and be sustainable, managing the uncertainty in achieving the organization's strategic and operational objectives is an integral part of all the organization's activities, functions, and processes. It is a top-down and bottom-up approach. Therefore, decision making can be clearly understood and leveraged when establishing the risk management framework.

2.2.2 Integrating risk into decision making

A decision can be considered to have three stages: a pre-decision stage, an active decision stage and a post-decision stage. Risk management can be integrated into all three stages. For example, risk may be assessed prior to deciding whether to proceed with an initiative. During the active decision stage, risk is considered in the context of setting expectations regarding the acceptance of loss and maximizing gain. After the decision has been made, risks that arise from the implementation of strategy can be assessed and treated.

At times, decisions simply and directly flow from available and reliable evidence where possible outcomes are predictable and probable. At other times, decisions are made under uncertain conditions, where the current state of information is such that:

- ▶ The order or nature of things is unknown;
- ▶ The consequences, extent, or magnitude of circumstances, conditions, or events is unpredictable;
- ▶ Credible probabilities to possible outcomes are imprecise at best;
- ▶ Rapidly changing and dynamic situations affect assumptions; and
- ▶ Available information may be ambiguous or incomplete.

Integrating considerations of uncertainty into decision making can lead to better decisions and better outcomes. To integrate risk into decision making, it is necessary to understand:

- ▶ Who the individual decision makers are;
- ▶ Who is accountable for implementing the decisions;
- ▶ The risk-taking attitudes of the people concerned;
- ▶ The importance and relevance of the decision;
- ▶ The implication of the decision for various parts of the organization; and
- ▶ The available resources to fulfil the decision.

Other key considerations are the importance and relevance of the decision, and the implications of the decision on various parts of the organization.

2.3 Benefits of risk management

Effective risk management enables an organization to achieve its objectives by continually assessing risks to reduce surprises and improve performance. Risk management also provides relevant stakeholders with continuous, consistent, and reliable information. Additional benefits from implementing and integrating processes to manage risk across an organization include:

- ▶ A more efficient use and allocation of capital and other resources;
- ▶ The ability to recognize and capture opportunities and threats quickly, and to respond to them;
- ▶ A reduction in the likelihood and impact of loss;
- ▶ Clearer, better-informed decisions;
- ▶ Lower compliance/auditing costs;
- ▶ Cost savings from using risk information to streamline and improve processes;
- ▶ Better management of human and cultural aspects that affect performance; and
- ▶ A greater understanding of potential events and the ability to influence their outcomes.

2.4 Integrating risk management with organizational strategy

2.4.1 Overview

All decisions and activities of an organization involve risk, starting with strategy. Integrating risk and strategy enables management to select the best strategies and manage relevant risks. The following subclauses illustrate the steps to integrate risk management into strategy development.

2.4.2 Communication and consultation

Consultation with stakeholders is important when developing a strategy to provide input for identifying risks and to gain support for the resulting plans. Dialogues and discussions about strategy are an opportunity to reach a consensus view of the risks faced by the organization.

Communicating and consulting with appropriate stakeholders occurs at the start and throughout strategic planning where additional input would improve the understanding of risks or confidence in the resulting actions.

2.4.3 Establish the strategic context

In developing strategy, top management may consider the current internal and external context, past performance, and the vision for the near, medium, and long term (see *subclause 3.4.1 Understand and use organizational context*). Integrating risk management into strategic planning requires a deep understanding of the key business drivers, the needs and objectives of the organization, and how they may change over time.

2.4.4 Identify risks associated with strategy

As organizations develop strategies, they consider opportunities and threats, and the associated risks.

When determining strategic risks, the organization may consider elements such as long- and short-term risks, as well as current and emerging risks.

with strategy span multiple elements of an organization and its ability to achieve objectives.

EXAMPLE

The climate crisis is contributing to an increase in extreme weather events, which may impact the durability of structures, the reliability of production, disrupt travel, etc. These impacts may affect asset life-cycle management, and the projection of operational costs and returns.

2.4.5 Assess the risks of the strategy

Assessing the risks associated with the strategy is an iterative process. Risks are assessed during strategy selection as well as afterwards, to identify and analyse risks in more detail. Assessments involve collecting and analysing information, consulting stakeholders and experts and using techniques such as those identified in IEC 31010:2019, *Risk management - Risk assessment techniques*. Interviews with top management and oversight bodies enable discussions and consideration of risks to potential strategy including emerging risks.

2.4.6 Finalize the plan, including the risk treatment actions for the risks identified

The implementation plan for the strategy is to incorporate the treatment of the risks identified. The strategy needs to be integrated into and communicated to all levels of the organization.

2.4.7 Monitor and review risks and strategic objectives

Risks, strategic objectives and key risk performance-measures (see *Clause 6 Continuous improvement*) are to be monitored as part of regular reviews.

2.5 Assigning roles and responsibilities

2.5.1 Overview

To be successful, risk management requires full support from top management (defined as members of senior executive teams) and from oversight bodies (most commonly the board). Top management is ultimately responsible for an organization's management of risk and its successes and failures. Accountability for managing risk is an important aspect of governance within the organization. A risk governance structure includes a clear understanding of roles, responsibilities, accountabilities, and oversight. Clearly articulating accountabilities for risk management at all levels supports a full understanding of roles and responsibilities. The following subclauses (*see 2.5.2 to 2.5.6*) outline roles in managing risk in an organization.

2.5.2 Oversight bodies

Boards or oversight bodies have a vital role on behalf of stakeholders to ensure that the organization is managing the risks it faces appropriately. The oversight body's responsibilities regarding risk include:

- ▶ Overseeing the culture that supports risk management within the organization and how incentives drive that support;
- ▶ Defining the amount and types of risk that an organization can take, in conjunction with top management;
- ▶ Maintaining oversight of risks and controls that can impact the organization's objectives;
- ▶ Taking steps to ensure that the language used to communicate about risk and its management is clear and understood across the organization;
- ▶ Ensuring risk management is embedded in processes that support important decisions; and
- ▶ Determining an appropriate structure for risk management assurance, including the role of audit and risk committees.

EXAMPLE – Case study

In the example of a small family-owned organization, in some cases the board is comprised of the owners and top management such as the finance and operations managers.

In the case of a not-for-profit start-up, initially the board may include professional colleagues, partners, and volunteers. As the not-for-profit gains a greater understanding of its context, strategic objectives and risk, requirements for new board skills and experience in legal, marketing and fundraising may arise.

2.5.3 Top management

Whether as a formal or informal process, all organizations manage risk.

Top management need to demonstrate a commitment to managing risk that emphasizes its importance, integration, and effectiveness throughout the organization. Top management's responsibilities are to:

- ▶ Understand the dynamic risk environment in which the organization operates;
- ▶ Have an overview understanding of risk within the organization;
- ▶ Establish and communicate a policy regarding risk management internally and to stakeholders as appropriate;
- ▶ Ensure that risk management aligns with the strategy and objectives of the organization;
- ▶ Set an example and actively model how to consider risk in decision making, following the same processes expected of the rest of the organization;
- ▶ Establish the amount of risk that the organization is willing to take in pursuit of objectives;
- ▶ Allocate resources to implement, monitor and improve risk management throughout the organization;
- ▶ Ensure implementation of a risk management framework and processes;
- ▶ Encourage people to view risk identification, analysis, and treatment positively; and
- ▶ Manage the risks they own.

2.5.4 Stakeholders

A stakeholder is a person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity (see ISO 31000). Stakeholders may have the opportunity to provide their perspective, and have it considered, even though it may not align with that of the organization.

External stakeholders can include:

- ▶ Shareholders who expect a return on their investment and ongoing performance of results;
- ▶ Customers who are affected by the quality of products and services;
- ▶ Suppliers and partners who expect an enduring and reliable relationship;
- ▶ Government (national and local levels), unions, non-governmental organizations; and
- ▶ The public, who depend on the organization's economic and environmental performance, its reputation and compliance with legal and regulatory obligations.

Internal stakeholders include employees, all levels of management, and others involved in the effective management of risk. Specific responsibilities include:

- ▶ Being aware of and fulfilling their responsibilities as defined by the risk management framework;
- ▶ Providing input into risk management activities;
- ▶ Participating in risk management procedures and processes to identify and analyse risk;
- ▶ Ensuring treatments for risks are effective within their area of accountability;
- ▶ Reporting risks; and
- ▶ Following policies and procedures to ensure compliance.

At times there can be an overlap between external and internal stakeholders, for example shareholders.

2.5.5 Risk owners

A risk owner is a person or an entity with the accountability and authority to manage risk. The organization's culture and structure play a key part in determining the best model for assigning risk owners.

Risk owners are to have the appropriate level of decision-making authority to manage their assigned risks.

Risk ownership can be delegated through several levels of the organization. This assists in reducing the workload on top management as well as cultivating the thinking, behaviours and actions regarding risk and risk management throughout the organization.

EXAMPLE

A risk owner can be at any level of the organization, for example the project manager in charge of a specific project or a process manager in charge of the budget and resources for a production line in a factory.

Risk owners require:

- A good knowledge and an understanding of their area of risk;
- The appropriate level of decision-making authority within the organization;
- Access to resources such as people and/or funding;
- Suitable training in risk management; and
- Knowledge and understanding of key stakeholders.

2.5.6 Risk leaders

Risk leaders are responsible for ensuring the implementation and integration of the risk management framework and process into the organization's management system and processes.

At times they are referred to as risk champions or coordinators. They have knowledge and understanding of risk and provide the capacity to facilitate the risk process. In some organizations this can involve designing and customizing the framework and developing appropriate tools and guidance to assist others in their risk management responsibilities.