ISO 31000:2018
Risk management

A PRACTICAL GUIDE

UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION

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

Contents

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.

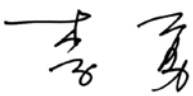
All events, whether large or small, can have a strong effect on organizations, businesses and the markets and economies in which they operate. Given the present uncertainties, it is hardly surprising when organizations struggle to identify and manage their risks. Managing risk effectively is how all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

Every organization faces risks that could impact its objectives. Risk management is the practice of using processes, methods and tools for managing these risks. Therefore, organizations that have identified risks and committed to the effective management of those risks will be better prepared to deal with them.

This handbook has been developed to provide valuable insight on how to implement ISO 31000 *Risk management – Guidelines* and support an organization's effort in creating and protecting value.

United Nations Industrial Development Organization

Vienna International Centre
P.O. Box 300
AT – 1400 Vienna
Austria

International Organization for Standardization

ISO Central Secretariat
Ch. de Blandonnet 8
Case Postale 401
CH – 1214 Vernier, Geneva
Switzerland

iso.org

We care about our planet.
This handbook is printed on recycled paper.

ISBN 978-92-67-11233-6