INTERNATIONAL STANDARD

**ISO 31022**

First edition
2020-05

# Risk management — Guidelines for the management of legal risk

*Management du risque — Lignes directrices relatives au management du risque juridique*

This document is a preview generated by EVS

Reference number
ISO 31022:2020(E)

© ISO 2020

This document is a preview generated by EVS

**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2020

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 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

 © ISO 2020 – All rights reserved

# Contents

Page



This document is a preview generated by EVS

© ISO 2020 – All rights reserved

# Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 262, *Risk management*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

This document is a preview generated by EVS

 © ISO 2020 – All rights reserved

# Introduction

Organizations operate in a complex environment with a variety of legal risks. Not only are organizations required to comply with the laws of all the countries within which they operate, legal and regulatory requirements can vary between different countries, strengthening the need for organizations to understand and have confidence in their processes. Organizations need to keep pace with legal and regulatory environment changes and review their needs as new activities and operations are developed. Organizations face considerable uncertainty when making decisions and taking actions that can have significant legal consequences. The management of legal risk helps organizations to protect and increase value.

This document provides guidance on activities that support organizations to manage legal risk efficiently and cost effectively to meet the expectations of a wide range of stakeholders. By developing an improved understanding of the external and internal legal context, organizations may be able to develop new opportunities or improve operational performance. However, failure to meet the requirements and expectations of stakeholders can have considerable and immediate negative consequences that could affect an organization's performance and reputation and might lead to criminal prosecution of top management.

ISO 31000 provides a generic framework for the management of all types of risks, including legal risk. This document is aligned with ISO 31000 and provides more specific guidelines applicable to the management of legal risk. The purpose of this document is to develop an improved understanding of the management of legal risk faced by an organization applying the principles of ISO 31000. These guidelines are intended to help organizations and their top management to:

— achieve the strategic outcomes and objectives of the organization;

— encourage a more systematic and consistent approach to the management of legal risk, and to identify and analyse a comprehensive range of issues so that legal risks are proactively treated with the appropriate resources and supported by top management and by the right level of expertise;

— better understand and assess the extent and consequence of legal issues and risk, and to exercise proper due diligence;

— identify, analyse and evaluate legal risks, and to provide a systematic way to make informed decisions;

— enhance and encourage the identification of opportunities for continual improvement.

It should be noted that legal risk within this document is broadly defined and is not limited to, for example, risk related to compliance or contractual matters. It includes these, but legal risk is deliberately defined to also include risks from or to third parties where there is not necessarily a contractual relationship with such third parties but where there is a possibility of litigation or other action depending on the third parties' contractual obligations with their stakeholders.

This document:

— provides guidance for the management of legal risk so it aligns with compliance activities and provides the assurance needed to meet the obligations and objectives of the organization;

— can be used by organizations of all types and sizes to deliver a more structured and consistent approach to the management of legal risk for the benefit of the organization and its stakeholders across all processes;

— offers an integrated management approach to the identification, anticipation and management of legal risk;

— supports and complements existing approaches, enhancing them by providing better information and insight on potential issues that the organization could face;

This document is a preview generated by EVS

© ISO 2020 – All rights reserved

— supports any process of compliance that organizations could have in place, such as a compliance or other management system;

— supports the compliance function by more broadly identifying the organization's legal and contract rights and obligations.

It is intended that organizations using this document will benefit from improved commercial and operational results, such as an enhanced reputation, better staff retention, improved stakeholder relationships and greater synergies between resources and capabilities.

While this document is intended for use as part of the ISO 31000 framework, it should be noted that the ISO 31000 framework may be used either on a standalone basis or with other management systems.

This document is not intended to:

— be a substitute for risk owners seeking expert legal advice (external or internal);

— apply to the process of law making or lobbying for new laws or changes to existing laws.

All references to the word "include" and "including" in this document should be interpreted as meaning the wording "including, without limitation".

This document is a preview generated by EVS

 © ISO 2020 – All rights reserved

# Risk management — Guidelines for the management of legal risk

This document is a preview generated by EVS

## 1 Scope

This document gives guidelines for managing the specific challenges of legal risk faced by organizations, as a complementary document to ISO 31000. The application of these guidelines can be customized to any organization and its context.

This document provides a common approach to the management of legal risk and is not industry or sector specific.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 31000, *Risk management — Guidelines*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 31000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

**3.1**
**risk**
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

[SOURCE: ISO 31000:2018, 3.1, modified — Note 3 to entry has been deleted.]

**3.2**
**legal risk**
*risk* (3.1) related to legal, regulatory and contractual matters, and from non-contractual rights and obligations

Note 1 to entry: Legal matters can have their origin in political decisions, national or international *law* (3.3), including statute law, case law or common law, administrative acts, regulatory orders, codified law, judgments and awards, procedural rules, memoranda of understanding or contracts.

Note 2 to entry: Contractual matters relate to situations where an *organization* (3.4) fails to meet its contractual obligations or to enforce its contractual rights, or enters into contracts with terms and conditions that are onerous, inadequate, unfair and/or unenforceable.

© ISO 2020 – All rights reserved