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

Reference number
ISO 31022:2020(E)

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

Page

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.

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;

— 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".

Risk management — Guidelines for the management of legal risk

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.

Note 3 to entry: Risk from non-contractual rights is the risk that an organization fails to assert its non-contractual rights. For example, the failure of an organization to enforce its intellectual property rights, such as its rights related to copyright, trademarks, patents, trade secrets and confidential information against a third party.

Note 4 to entry: Risk from non-contractual obligations is the risk that an organization's behaviour and decision-making can result in illegal behaviour or a failure in non-legislative duty-of-care (or civil duty) to third parties. For example, an organization's infringement of third-party intellectual property rights, failure to meet the requisite standards of care due to customers (such as mis-selling), or inappropriate use or management of social media resulting in a third-party claim of defamation or libel and tortious duty generally.

3.3
law
system of rules, principles and practices, which a region, country or community recognizes as regulating the actions of *organizations* (3.4)

Note 1 to entry: Laws may include any:

— statute, regulation, codified law, by-law, ordinance or subordinate legislation;

— common or case law;

— binding court order, judgment or decree;

— applicable industry code or policy enforceable by law.

3.4
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO 19600:2014, 3.2.1, modified — Note 1 to entry has been modified.]

4 Principles

The effective management of legal risk requires the values and principles introduced in ISO 31000, as shown in Figure 1.

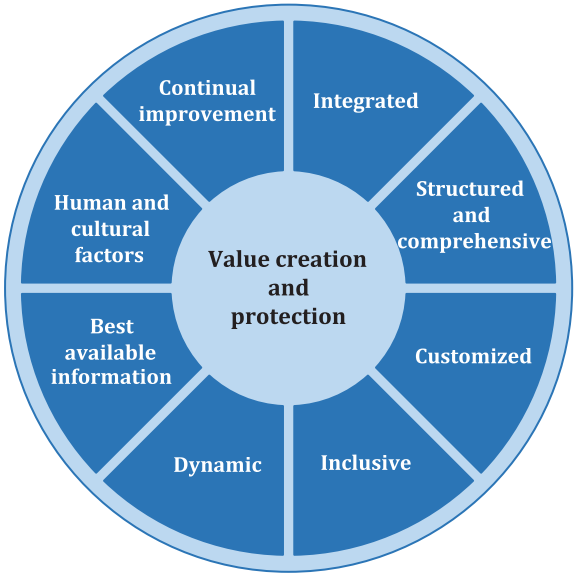

Figure 1 — Principles

These eight elements are described below in a) to h) in the context of the management of legal risk. In addition, for the management of legal risk, the principle of "equity", see i), should also be considered.

a) Integrated: The management of legal risk is integral to the overall governance and management of the organization. The activities of the legal risk management process should be embedded into the strategic planning, business decision-making and management processes of the organization. For the integration of the management of legal risk into organizational processes and activities, proper roles and responsibilities should be established within the organization. The management of legal risk should be integrated with other management systems, such as compliance, safety, quality and with internal controls. While assessing legal risks and considering treatment options, legal subject matter experts should be consulted together with other experts or specialists.

b) Structured and comprehensive: While following the generic risk management process, it is important to assess the organization's legal risks within an appropriate context so that a comprehensive and consistent approach to the management of legal risk can be adopted.

c) Customized: The management of legal risk in an organization should be customized to reflect the differences of its external context, including the legal and regulatory environment and sector characteristics, as well as its internal context, including the nature of the legal entity, organizational objectives and values.

   The organization should have a detailed understanding of the applicability, impact and consequences of failure to comply with relevant laws, and processes to ensure that applicable new or updated laws are adequately identified, assessed for impact and interpreted.

   The organization should minimize the complexity and cost of legal proceedings. It should attempt to minimize and manage the negative consequences of legal risk. The organization can actively seek opportunities to avoid disputes or litigation by taking action to treat legal risks before an adverse event occurs, or is likely to occur, or attempt to reach settlement in a way that balances costs, commercial objectives, reputation and time invested by the organization.

d) Inclusive: By involving all stakeholders in the management of legal risk, an organization can mitigate adverse events, including regulatory enforcement. The organization should take care to ensure legal privilege (or its equivalent form of protection in the relevant jurisdiction) is maintained as far as practicable and confidentiality is maintained, but in both instances such protections need to be assessed against the benefits of inclusiveness.

e) Dynamic: An organization should monitor and adapt to changes in laws, public policy and the context within which it operates, and establish appropriate early warning indicators.

f) Best available information: For the effective management of legal risk, in addition to the experience of in-house legal counsel, if it exists, business intelligence, business analytics, legal databases and systems (including case management), electronic file management tools and services should be used. If necessary, know-how provided by external law firms, service providers or advisors can be used.

g) Human and cultural factors: Given that stakeholders can have different knowledge, expectations and views regarding legal risk and, given that such views could be emotionally, socially, culturally and politically constructed and perceived, the organization should develop formal and informal mechanisms to help ensure that human and cultural factors do not adversely result in legal risks. The organization should also seek to encourage the realization, benefits and opportunities of the management of such risks. Every member in the organization should be aware of how each action or non-action affects legal risk.

h) Continual improvement: An organization should take into consideration, and act on lessons learned, post transaction reviews, best practices, professional advice from internal and external counsel, and internal audit, and consider applicable changes in law.

i) Equity: For decision-makers, establishing the principles of equity guides the management of legal risk and includes managing conflicts of interest and provides an unbiased, independent voice in decisions and support due diligence and fairness for the best interests of an organization.

NOTE There is no one common agreed definition of equity, rather, "equity" incorporates different ideas and concepts, including justice, fairness and equality.

5 Legal risk management process

5.1 General

The management of legal risk is iterative and should be integrated in all activities and operations of the organization. The risk management process as applied to the management of legal risk is described in 5.2 to 5.5 and is illustrated in Figure 2. This diagram complements ISO 31000:2018, Figure 4.

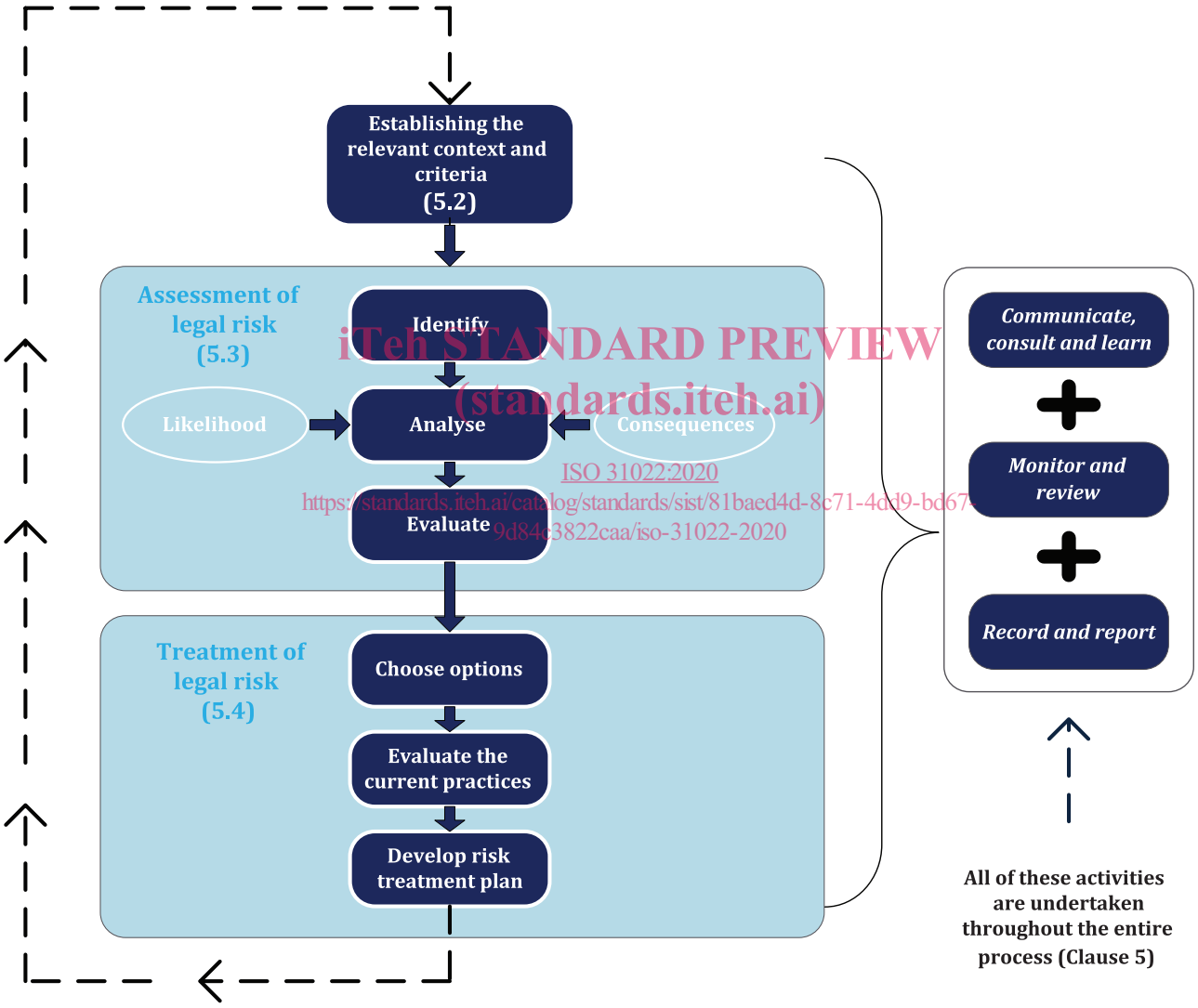

Figure 2 — Process for the management of legal risk

Monitoring and reviewing, reporting, communication and consultation should be ongoing throughout the entire process of the management of legal risk across the organization. Further details are given in 5.5.

5.2 Establishing the relevant context and criteria

5.2.1 General

In addition to ISO 31000:2018, 6.3, the organization should consider the external and internal context given in 5.2.2 and 5.2.3, respectively.

5.2.2 External context of legal risk

The external context of legal risk refers to factors that are outside the organization but related to the management of legal risk. It includes:

— relevant local and international laws and changes in relevant local and international laws;

— trade unions and employer organizations;

— external service providers and advisors supporting the management of legal risk, such as law firms, external auditors, and service providers of information management and analytics;

— external stakeholders, such as businesses, civil society organizations, regulatory bodies, local governments, the public, communities of interest, press and media, and special interest groups, and their expectations regarding the management of legal risk;

— any acts or omissions of third parties, such as fraudulent and deceitful conduct by such third parties;

— applicable international agreements and memoranda of understanding;

— applicable market conditions related to the organization;

— third-party actions or claims;

— laws of the countries where the products/services provided are delivered or supplied.

When examining and understanding the external context of legal risk for organizations operating in multiple jurisdictions, the environmental and cultural differences among different jurisdictions should be considered. The extraterritorial application of national laws, which jurisdiction's law applies in a certain situation (i.e. conflict of laws and the mutual recognition of laws) and the identification of the applicable jurisdiction may also require consideration.

5.2.3 Internal context of legal risk

The internal context of legal risk is substantially in the control of, or subject to the authority of, an organization through its governing and management systems. It includes:

— the nature of the legal entity;

— the financial health of the organization and its business model;

— the internal legal structure of the organization and its governing processes and functions;

— the governance of the organization and its value structures for promoting integrity, such as a code of conduct and other compliance guidelines;

— the current state of the organization's legal matters and its approach to the management of legal risk;

— awareness campaigns on the orientation and continual improvement of performance in matters of legal risk for stakeholders, and systems and arrangements to improve stakeholder behaviour concerning laws and to deter fraudulent and deceitful conduct, such as compliance management systems;

— past experiences and the history of legal disputes or events triggered by legal risk in the organization;

— assets that the organization owns, such as intellectual property and other legal rights for tangible and intangible assets used for processes and activities;

— the effect of rights and obligations under contracts;

— the obligations arising from a duty of care;

— the cross-triggering effects of indemnities, warranties and non-reliance clauses in contracts;

— liabilities arising from labour, environmental, tax and other issues from mergers, acquisitions and disposals;

— the internal policy regarding the management of legal risk;

— other information and resources related to legal risk and its management.

5.2.4 Defining the legal risk criteria

In addition to ISO 31000:2018, 6.3.4, the organization should consider the following.

Legal risk criteria:

— as a term, is a subset of organizational risk criteria;

— are measures that are identified and defined to evaluate a significant and acceptable level of a legal risk or a group of legal risks;

— should reflect the objectives, values, resources, preferences and tolerance of overall risk management in relation to legal risk;

— should be reviewed on a regular basis and at the beginning of any major project to update the criteria and process for managing legal risk;

— can arise from, or be derived from, the application of laws or contractual obligations or liabilities;

— are dynamic and, once defined, belong to the function responsible for the management of legal risk;

— should be aligned with the organization's overall approach to the management of legal risk and/or policy. An organization should develop and adjust its legal risk criteria according to real-life situations.

When determining the criteria for legal risk, factors to consider include:

— the organizational objectives and priorities;

— governance, including the hierarchical level of authorities and the allocation of accountabilities, roles and responsibilities for the management of legal risk in the organization;

— relationships with third parties;

— the scope and objectives of the management of legal risk and the categories of legal risks;

— the principles adopted to determine the level of legal risks;

— the status of policies, protocols, frameworks, processes and methodologies for the management of legal risk;

— stakeholders' acceptance of legal risks or tolerance of the risk level;

— the measurements for the classification of risk levels.

The following situations can require the application of legal risk criteria:

— something that the organization is required by law to undertake, follow or approve;

