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.

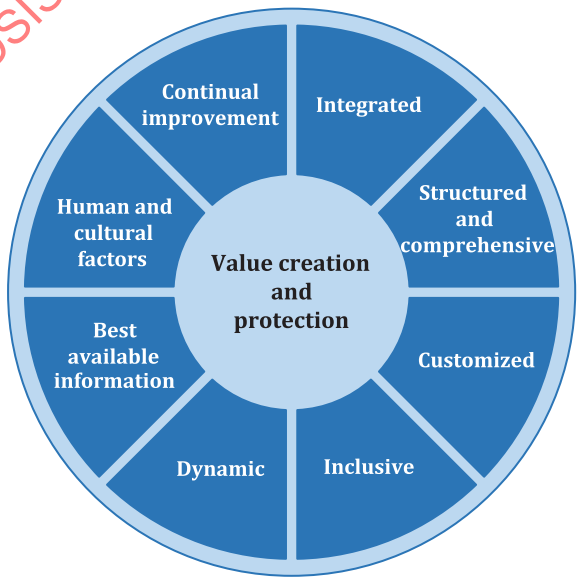

Figure 1 — Principles

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.

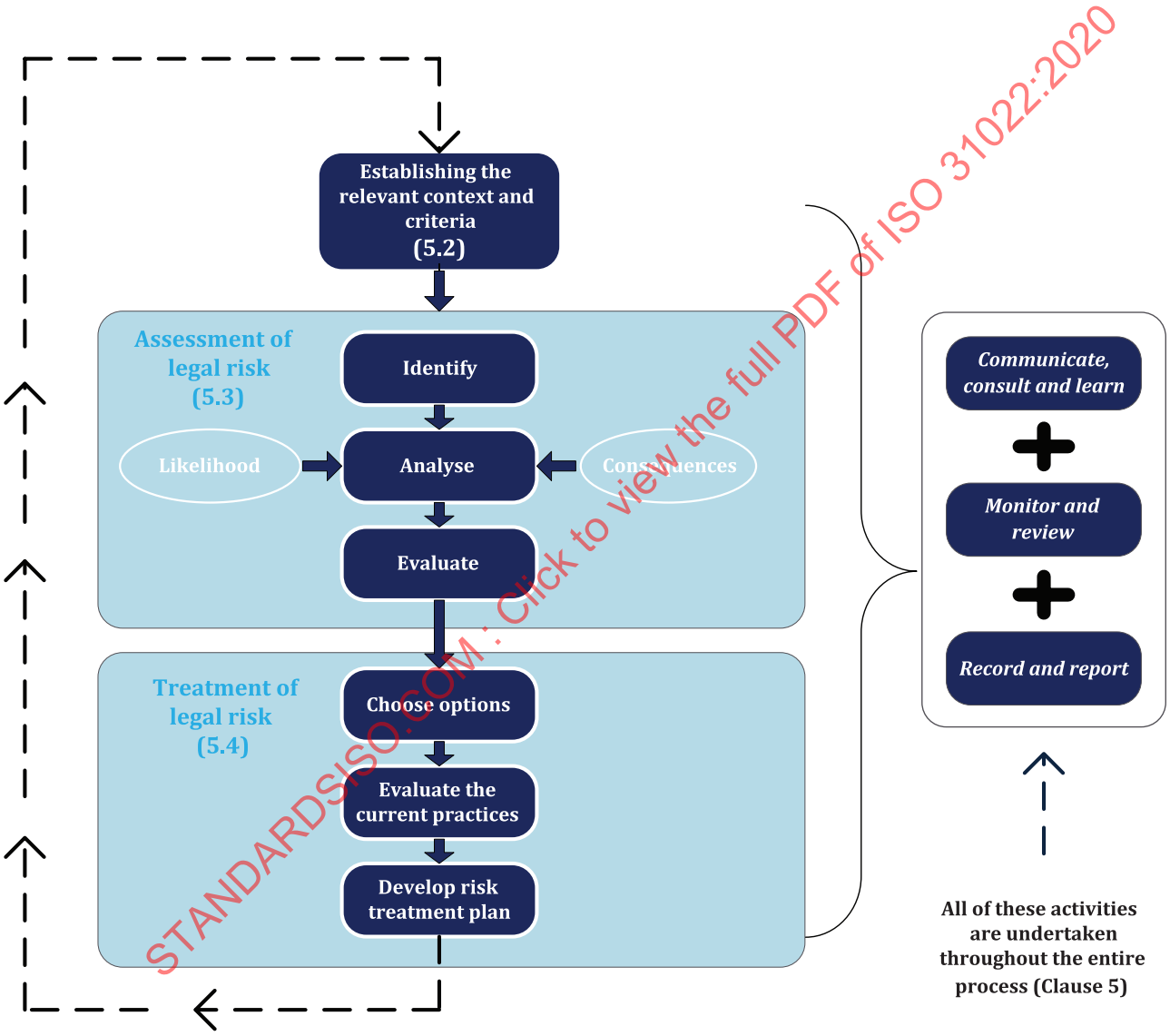

Figure 2 — Process for the management of legal risk

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;

— something related to a policy or contract that the organization is required by law to adopt or a decision only the organization can legally make;

— something relating to a substantial issue of institutional liability or compliance, including investigations by governments, allegations of widespread violations of the law, criminal conduct that could implicate the organization, a major non-compliance, a loss of data that causes data protection and privacy concerns, whistle-blower complaints, matters resulting in reputational loss and any other lawsuits;

— laws relating to disclosure of information, incidents, violations and any other situation;

— lawsuits and settlements "not in the normal course of business" where either the amount involved or the issue presented involves one or more of the other factors listed above.

The definition of the criteria for legal risk is process-driven in requiring that legal risks be characterized and then measured so that they can be quantified and the appropriate risk treatment applied.

A proportionate response will require agreeing the criteria for legal risk, both at management level and throughout the entire organization. Unduly narrow legal risk criteria can have the unintended result of isolating the owners of legal risk from the larger operating risk context. This can create a silo effect that isolates the management of legal risk from other elements of risk management.

Overly restrictive criteria for legal risk that do not fully integrate with the overall risk criteria adopted by the organization can have the unintended consequence of offering an unduly narrow approach to legal risk problems. This could mean that those charged with the legal function become involved only when a crisis escalates, as opposed to at an early stage when earlier engagement would mitigate the legal risk and they are in a better position to offer a treatment for the legal risk.

5.3 Assessment of legal risk

5.3.1 General

The assessment of legal risk is the overall process of the identification of legal risk, analysis of legal risk and evaluation of legal risk.

It is essential to involve a cross-section of relevant individuals from the organization and experts, including legal counsel (internal and external), with a balance of experience and expertise.

5.3.2 Identification of legal risk

5.3.2.1 Overview

The purpose of identifying legal risk is to find, recognize and describe the legal risks that can help or prevent an organization to achieve or from achieving its objectives. To have a comprehensive understanding of legal risk, the organization should identify the sources of legal risk, areas of consequences, events (including changes in circumstances), their causes and their potential consequences.

Through legal risk identification, the characteristics of the various legal risks of the organization should be comprehensively, systematically and accurately described so that the objectives and scope of the legal risk analysis in the next step can be clarified. The relevant and latest information, such as applicable background information and facts (e.g. changes in applicable laws or market practice), needs to be understood when identifying legal risks. In addition to identifying the possible events triggered by legal risk, the possible causes, consequences and impact should be considered carefully.

Other than identifying actual or potential events triggered by legal risk, relevant legal risks should be identified, irrespective of whether the sources of such events are under the control of the organization, or whether their causes are known or not. The organization should select appropriate

legal risk identification tools and techniques applicable to its objectives, resources, capabilities and the environment.

Several techniques for risk identification, which may be applied to the management of legal risk, can be found in IEC 31010:2019, Clause 4.

5.3.2.2 Sources of information useful to the identification of legal risk

The organization should systematically identify its legal risks and the implications for its activities, products, services and reputation. The organization should take these identified legal risks and implications into account when establishing, developing, implementing, evaluating, maintaining, revising and improving the management of legal risk.

The organization should document its legal risks in a manner that is appropriate to its size, complexity, structure and operations.

An organization may identify legal risks related to:

— its organizational objectives and priorities;

— its governance and ethics structures, activities and operations, such as sales, services delivery, production, marketing, procurement, foreign investment, human resources management, financial management, organizational structure, reputation management, information and data management, and information communications technology;

— cyber-attack, social engineering and other cyber threats;

— its interested parties, such as shareholders, regulatory bodies, directors, employees, unions, business associates (including clients, customers, suppliers, vendors and investors), creditors, debtors, communities and government;

— the misapplication or misinterpretation of the legal context, non-compliance with laws, breach of contract, infringement of intellectual property rights, misconduct/intentional wrong-doing and failure to exercise rights;

— responsibilities and accountabilities for the management of legal risk after their occurrence, which can include criminal liabilities, administrative responsibilities, civil liabilities, regulatory fines and/or compensation paid to third parties, etc.;

— the application of specific laws, and also conflict of laws or private international law;

— case law and common law (where applicable).

The organization should develop a process for the identification of legal risk. It may consider the factors mentioned above. "Legal" in this context does not just refer to the laws of the jurisdiction in which the parties are domiciled, incorporated, managed or operated. Risks can arise from international legal obligations, including international and private international law obligations, penalties or other outcomes.

Some of the sources of information that can be useful to the identification of legal risk are given in the following examples.

EXAMPLE 1 Information that can be useful includes an understanding of the relevant:

— laws;

— external context of legal risk;

— internal context of legal risk;

— communication and consultations with internal stakeholders, e.g. internal personnel and external stakeholders;

— existing legal risk criteria;

— legal risk plans;

— record-keeping requirements with respect to legal professional privilege, attorney–client privilege and work product (or their equivalent concepts and terms under the relevant national law);

— data destruction and retention policies in accordance with data protection laws and regulation.

EXAMPLE 2 Compliance obligations that can be relevant to the identification of legal risk include:

— agreements with community groups or non-governmental organizations;

— agreements with public authorities and customers;

— organizational requirements and business ethics, such as policies, processes and procedures;

— voluntary principles or codes of practice;

— voluntary labelling or environmental commitments;

— any obligations arising under a contract;

— relevant organizational, industry and international standards.

To ensure the legal risks are identified comprehensively, systematically and accurately, the organization should establish a legal risk identification methodology to meet its management needs. This methodology is part of the process for the management of legal risk and should provide different approaches to identifying legal risks, as well as enabling all organizational levels to identify and report legal risks from a variety of perspectives.

An organization can then decide how to apply this methodology in the legal risk identification process.

The organization should have processes in place to identify new and changed laws and other legal-risk-related obligations to ensure the ongoing management of legal risk. The organization should have processes to evaluate the consequence of the identified changes and implement any necessary changes in the management of legal risk.

EXAMPLE 3 Approaches to obtain information on changes to laws and changes to compliance obligations can include:

— subscribing to the mailing lists of relevant regulators;

— membership of professional groups;

— subscribing to relevant information services;

— attending industry forums and seminars;

— monitoring the websites of regulators;

— monitor internal and external litigation trends and decisions;

— meeting with regulators;

— seeking advice from legal advisors;

— using law firm publications and their know-how/professional support lawyer teams;

— using independent and objective analysis, insights and advice from internal audits;

— developing and maintaining an internal legal risk knowledge database;

— monitoring the sources of compliance obligations (e.g. regulatory requirements and court decisions).

The organization should build a process for legal risk identification. It may choose one or more of the approaches mentioned above.

An example of a legal risk identification method is given in Annex A. An example of a legal risk register is given in Annex B.

Annex E presents and comments on key clauses to consider when reviewing contracts.

5.3.3 Analysis of legal risk

5.3.3.1 General

The analysis of legal risk includes qualitative or quantitative analysis of the identified legal risks. The outcome of this analysis becomes the input for the evaluation and treatment of the legal risks. The causes of the events triggered by the legal risks and the synergies arising between them, their likelihood of occurrence and their consequences should be taken into consideration when analysing legal risk.

For the analysis of the likelihood and consequences of events triggered by legal risk, historical data simulation, business analytics, artificial intelligence and modelling, as well as expert opinions, can all be used, individually or in combination, see IEC 31010 for additional information on techniques. Divergences between experts' legal advice in relation to the legal risk should also be taken into consideration.

Legal risks and other risks can arise jointly and transform into each other under certain conditions. The organization should analyse the correlation between legal risks and other risks to understand the consequences and relationships between the risk events. The interdependency/correlation among legal risks and other risks needs to be understood in order to formulate an integrated strategy for the management of legal risk and other risks.

5.3.3.2 Likelihood of events related to legal risk

The likelihood of events related to legal risk can involve the following factors:

— the range of laws, along with enforcement practices and conventions by the relevant regulatory authorities;

— the improvement of, and compliance with, the existing framework for the management of legal risk, including strategies, governance, internal rules and policies;

— employees' and contractors' demonstrated compliance with laws, and the rules and policies of the organization;

— the frequency and number of activities related to legal risk occurring within a certain period;

— failure to record, analyse and learn from previous events;

— benchmarking the frequency and number of activities related to legal risk occurring within a certain period against other organizations.

Annex C provides further guidance on estimating the likelihood of events related to legal risk.

5.3.3.3 Consequences of events related to legal risk

The consequences of events related to legal risk can involve the following factors:

— the different types of benefits and losses (financial and non-financial) that can be caused by the events triggered by legal risk;

— adverse media (including social media, as well as traditional media) coverage;

— the amount and scope of benefits and losses (financial and non-financial), and stakeholders' reactions to such consequences.

Annex D provides further guidance on estimating the consequences of events related to legal risk.

5.3.4 Evaluation of legal risk

Legal risk can be evaluated by comparing the results of various risk analyses with its risk criteria and then prioritizing those legal risks. This evaluation should help decision-makers to consider various legal risk treatment options. When possible and appropriate, the organization's decision should take into consideration the following:

— the wider environment of the organization, including the perception of internal and external stakeholders;

— organizational objectives, priorities and the risk management policy;

— organizational and stakeholder values, morals and ethics;

— the attitude to risk and tolerance levels, which have helped to form the strategy;

— the organization's risk profile (including the maturity of the organization in relation to the management of legal risk and its negotiating leverage with a third party).

5.4 Treatment of legal risk

5.4.1 General

The treatment of legal risk refers to the corresponding strategies implemented by an organization to deal with its legal risks.

A risk treatment plan should consider a range of treatment options, which may include legal remedies as well as financial, operational and reputational remedies for each prioritized risk.

Further information is given in ISO 31000:2018, 6.5.

5.4.2 Choosing options for the treatment of legal risk

Risk treatment options are given in ISO 31000:2018, 6.5.2.

A risk evaluation is a prerequisite for developing a risk treatment plan and enables the organization to make informed decisions concerning legal risk treatment options. Once an organization evaluates its legal risks, it becomes critical to demonstrate an appropriate management of such risks otherwise the organization could be exposed to unwanted litigation and losses.

Key risk indicators (KRIs) are data points that give some guidance on whether a particular option for the treatment of risk is proving effective for the management of legal risk. To choose effective KRIs, an organization can identify potential data points generated by its operational processes. KRIs can be reported as single indicators (e.g. "contract value"), but they usually provide better information when they are combined with related data points. Some examples of KRI combinations are as follows.

— Contract liability versus contract value: a running total of liability versus value, when broken down by contract type, third party, etc., should give a good indication of how much risk an organization is taking on to win particular areas of business.

— Volume of written contracts executed versus volume of deals entered into system: this KRI should tell an organization whether it is entering into deals without having a binding written contract in place.

— Product sales by salesperson versus compliance training registers: this KRI should provide an organization with an indication of the possible exposure to conduct-related risks around the duty of care to customers. If an organization's sales teams have not completed their compliance training, or regularly complete it late, they may not be aware of the latest issues in legislative regulatory compliance and are therefore exposing their organization to increased levels of legal risk.

The following factors should be considered when choosing an appropriate option for the treatment of legal risk:

— the organizational risk management policy, strategic objectives, core values and legal responsibility of the organization;

— a cost benefit analysis of responding to legal risk;

— the stakeholders' perception and their values, attitude to risk and tolerance levels, as well as their preferences on certain legal risk treatment strategies;

— the availability and allocation of resources needed to manage the risk;

— a legal review (including scope and depth) of laws, contractual commitments and limiting risk contractually;

— legal opinions;

— the extent to which the legal risk can under law be transferred, delegated or insured against;

— the level of risk awareness and maturity level within the organization.

5.4.3 Evaluation of the current practices for the treatment of legal risk

When the organization chooses an option for the treatment of legal risk, the current practices of the organization for the treatment of legal risk should be evaluated to understand the appropriateness of the option, and also to provide support for developing the treatment plan for legal risk (as referred to in 5.4.4).

It is important to consider the following factors when evaluating the current practices for the treatment of legal risk:

— the allocation of relevant resources (including personnel, assets and funds and, in particular, the internal and external legal counsel and experts);

— the views and opinions of the internal and external legal counsel and experts.

5.4.4 Development and implementation of the risk treatment plan

After selecting and implementing the appropriate treatment for a legal risk, the organization should assess whether it can accept residual risks (which may not necessarily be legal risks but could be other risks). If the residual risks are unacceptable, the organization should adjust or develop a new risk treatment option, and reassess the risk after considering this adjustment and its effects until the residual risk is within an acceptable level.

In implementing a treatment plan for legal risk, an organization should consider ISO 31000:2018, 6.5.3, and the following.

— Policy and processes: developing or improving its policy and processes related to legal risk treatment. For example, having specific requirements for internal stakeholders to notify its internal or external lawyers when a legal dispute arises or is likely to arise.

— Standard operating practices (SOPs): developing SOPs for internal stakeholders to use. For example, having an SOP for when internal stakeholders need to disclose business information to a third party, which could be facilitated through approved non-disclosure or confidentiality agreements to avoid the inadvertent disclosure of confidential information.

— Techniques and technology: using techniques to treat some legal risks. For example, having contract review templates to ensure that the key legal risks of a contract are identified and addressed prior to contract signature, or developing or improving information security to avoid legal risks by the unauthorized access to information systems of the organization.

— Information: providing availability and access to information for the management of legal risk. For example, a notification to the contract owner that a contract will be automatically renewed unless notice is given to the counterparty within a specified time frame, or releasing risk warning information about certain events triggered by legal risk.

— Activities: undertaking activities to treat legal risks. For example, contract reviews and redrafting by legal experts, or selecting a suitable dispute resolution method (litigation, arbitration or mediation), dispute resolution expert and appropriate dispute resolution strategy.

— Training to illustrate examples: providing training on the management of legal risk to key internal stakeholders to improve their skills and awareness of legal risk. For example, training courses outlining relevant laws, the impact of such laws on the individuals' role at work, and the consequences to those individuals of non-compliance.

The management of legal risk is a dynamic and iterative process and the techniques used need to be evaluated and adjusted, based on changes in the internal and external legal risk environment, to ensure their effectiveness.

The organization should track and monitor the effect of the treatment of legal risk and the external context, assess the changing risks and re-formulate the treatment of legal risk when necessary.

5.5 Communication (internal and external), consultation and reporting mechanisms for the management of legal risk

5.5.1 General

The organization should establish:

— internal communication and reporting mechanisms as outlined in ISO 31000:2018, 6.2, to ensure there is appropriate communication about key components of its system for managing legal risk at the appropriate time and level;

— a connection between the mechanism and way of communication and other risk information sources, in order to ensure the appropriate communication flows within the organization and to external stakeholders.

External communication and reporting should ensure that confidentiality, professional legal privilege and attorney–client privilege (or its equivalent form of protection in the relevant jurisdiction) are maintained.

5.5.2 Communication, consultation and learning

The organization should communicate and consult in a timely manner with relevant stakeholders at each stage of the process of the management of legal risk, to ensure that these stakeholders (including those internal personnel who implement the management of legal risk) fully understand the legal risks and their effect on the organization. The relevant stakeholders should also know their roles in the decision-making process for the management of legal risk and should be able to make appropriate decisions based on relevant information. They also should implement these activities effectively and efficiently.

Since the organization's personnel at all levels, as well as external stakeholders, have different values, perspectives and focus, their preferences and expectations regarding the management of legal risk are likely to be different too. This can have an important effect on decision-making and the implementation of the management of legal risk. Therefore, communication and consultation with the relevant stakeholders during the decision-making process and implementation of risk treatments should include having a robust monitoring and review process and keeping records of risk management practices (see 5.5.3 for further details). In order to facilitate effective communication and consultation, the organization should aim to provide the necessary information to everybody with the responsibility, accountability and authority for the management of legal risk and oversight. The management function

should also be able to communicate with relevant stakeholders, including regulatory authorities, legislative and judicial functions, and other external stakeholders.

In order to build a risk management culture throughout the organization, learning should:

— occur at all stages in the management of legal risk;

— be promoted to raise awareness and understanding of the exposure to legal risk;

— be used to provide clarity on governance and leadership, the mandate, goals and objectives, stakeholder involvement, roles and responsibilities, and conformity to policies, processes and procedures.

5.5.3 Monitoring and review

The monitoring and review of the management of legal risk includes the following:

— staying abreast of changes in the environment, such as the introduction of new laws and the enforcement of such laws, in order to adjust the organization's strategy accordingly;

— monitoring events triggered by legal risk, analysing their frequency and patterns, and drawing conclusions from them (including potential correlation with and amplification of other risks);

— considering an early warning system with key stakeholders to identify warning signals for significant legal risks that could arise;

— monitoring and reviewing:

  — outcomes following risk treatment;

  — changes in the environment;

  — the building of integrated risk treatment plans;

  — the designation of the responsible and accountable parties;

— comparing progress with the risk treatment plan, reviewing and updating the risk treatment plan periodically and in a timely manner to seek assurance on its adequacy, suitability and effectiveness in relation to the management of legal risk.

5.5.4 Recording and reporting

An organization should consider the following issues in relation to record-keeping and reporting:

— legal professional privilege, attorney–client privilege and work product (or their equivalent concepts and terms under the relevant national law);

— destruction, retention and privacy policies, in accordance with data protection laws;

— the availability and accessibility of documentation for stakeholders to improve decision-making and for internal or external audit purposes;

— whether the relevant documentation needs to be maintained securely, with a chain of evidence process documenting that no alterations have been made to the documents, information or evidence;

— confidentiality and security measures in relation to documentation of a confidential nature, such as setting up limited and authorized access to such documentation.

An organization should report on the progress of changes in implementing the management of legal risk and adherence to the measures.

6 Implementation of the management of legal risk

6.1 General

The management of legal risk should be embedded within the activities and operations of the organization to ensure that its outcome is part of the organization's decision-making process. The implementation of the management of legal risk should be integrated with the organization's strategy, and the risk management framework, objectives and management systems within the organization. This includes a policy for the management of legal risk and organizational functions, procedures for the integration of the legal process into various processes, the allocation of resources and the communication mechanism, among other management tools.

6.2 Policy for the management of legal risk

In addition to ISO 31000:2018, 5.2 and 5.4.2, the policy should consider any specific matters relevant to the management of legal risk.

6.3 Roles and functions for the management of legal risk

The organization should assign the authority, responsibility and accountability for the management of legal risk. ISO 31000:2018, 5.4.3, and the following should be considered:

— those assigned with the authority and responsibility for the management of legal risk should have the expertise and capabilities appropriate to carry out the tasks;

— allocating the necessary resources to support those with the authority and responsibility for the management of legal risk; for example, an organization could have a contract management team, an internal legal counsel, or an external counsel available for consultation by the risk owners;

— the interplay and interdependencies with the organization's overall risk management function to ensure that objectives and interests are aligned;

— allocating tasks between internal and external resources for the management of legal risk;

— identifying and defining common terms relating to the management of legal risk in collaboration with key stakeholders;

— facilitating and providing advisory services, training and consultation to the risk owners to identify, analyse, evaluate and respond to legal risk;

— recommending risk identification, analysis and evaluation techniques and determining the legal risk criteria and the organization's approach to risk;

— communicating the management of legal risk according to the organization's policy and plan;

— reporting on the management of legal risk performance to top management for review and further improvement;

— coordinating business units to select possible legal or non-legal strategies to respond to the identified legal risks;

— assessing the status of organizational resources currently being used to assess and treat legal risks;

— formulating an implementation plan for the management of legal risk for the organization, and integrating that plan with the implementation plans for the risk management framework, risk treatment and the strategic and operational plans of business units;

— establishing communication channels between internal and external legal resources and law enforcement bodies;

— monitoring the compliance of persons who have been assigned the authority, responsibility and accountability for the management of legal risk;

— identifying industry best practices that set a threshold higher than the minimum standards required by law.

The following activities should be carried out jointly by the business units and those who have been assigned the authority, responsibility and accountability for the management of legal risk:

— periodically review the progress of implementation plans for the management of legal risk and the effectiveness of legal risk treatments;

— develop integrated response management plans to ensure that the significant events triggered by legal risk will be managed properly;

— clarify the responsibilities and accountabilities of members who are responsible and accountable for the enforcement of legal risk treatment measures, maintenance of the legal risk framework and reporting of relevant risk information in accordance with ISO 31000:2018, 5.4.3;

— record and report legal risks in accordance with ISO 31000:2018, 6.7;

— make clear the duties of management and other members of the organization in relation to the management of legal risk in accordance with ISO 31000:2018, 5.4.3.

6.4 Integrating the management of legal risk

The organization should establish a robust supporting framework in line with the objectives of the management of legal risk. The organization should establish, document and communicate the organizational processes to all personnel to ensure they are aware of the legal risks.

To ensure consistency, the overall risk management and the management systems of the organization should be considered in relation to the management of legal risk, so as to integrate the management of legal risk into all organizational activities.

6.5 Resource allocation for the management of legal risk

The organization should allocate appropriate resources for the management of legal risk in accordance with their risk management plan and ISO 31000:2018, 5.4.4.

6.6 Awareness of legal risk

The organization should promote an awareness of legal risk, taking into account the following considerations:

— the attitude, management philosophy and commitment from top management to the management of legal risk;

— a systematic training programme for the management of legal risk, including workshops, classes and training provided by subject matter experts;

— communication lines for the observations of members of the organization as well as from multidisciplinary work teams to improve the management of legal risk.

Annex A
(informative)

An example of a legal risk identification method — Legal risk identification matrix (LRIM)

The management of legal risk calls for a structured approach to assessing legal risks in the context of an organization. Through the adaption of appropriate risk management techniques, an organization can proactively identify legal risks and can then reduce or eliminate risks or reconfigure their processes to minimize their exposure to them.

The legal risk identification matrix (LRIM) is one approach to organizing legal risks identified and collected as events of different types by business areas/units/activities. By considering the various business areas/units/activities concerned, the LRIM connects legal risks of various types with the operations of the organization. In a LRIM, all identified legal risk events are categorized into different types.

These legal risks of different types can occur in different business areas and have different causes and characteristics. The LRIM helps to comprehend systematically all the organization's legal risks. Table A.1 provides an example of a LRIM that categorizes the legal risks into six different types and includes a brief explanation of the different categories.

For the categorization of legal risks to be useful, it is important to recognize that each category may not be mutually exclusive and that a single business activity can generate legal risks that fall into one or more categories. In addition, while the LRIM refers to the legal risks for organization, this can include the actions of agents, employees, contractors, etc. that work for or with the organization.

Within each category of legal risk there can be "red flags" that should be identified. These red flags should be escalated within the organization's governance structure so that they are addressed appropriately. Such red flags can include:

— jurisdictions where there is a lack of a fully functioning rule of law or political instability;

— conditions requiring the supplier to provide a contractual indemnity because of the extreme duty of care required;

— dangerous products or dangerous performance conditions.

Table A.1 — An example of a LRIM

Parameter	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6
Legal risk typologies	Unpredictability	Non-compliance with applicable laws	Breach of contract	Infringement of rights	Omission in exercising rights	Improper choice
Business activity 1						
Business activity 2						
Business activity 3, etc.						

Key

Category 1: Unpredictability in the legal risk context can arise when an organization faces a significant change in law in an environment, market or territory in which the organization has operations, or if the organization decides to enter into a new environment, market or territory where laws are unfamiliar to the organization or where there could be an absence of local law in some respects.

Category 2: Non-compliance occurs when an organization violates an applicable law. For example, an organization fails to make an appropriate disclosure in its financial reporting obligations to regulators.

Category 3: Breach of contract occurs when the organization or the contracting counterparty breaches a contractual obligation through non-performance or improper performance, which gives rise to legal consequences, e.g. a damages claim or a right for the non-defaulting party to terminate the contract for breach. For example, the organization fails to deliver goods on time as per its contractual obligations.

Category 4: An infringement occurs when the organization encroaches on, breaches or violates the legitimate rights or expectations of a third party. For example, it would be an infringement of the intellectual property rights of a third party to use its trademark without permission. An infringement may arise under a contractual obligation by a party to a contract or it may arise where there is no contractual obligation.

Category 5: Omission in exercising rights occurs when there has been conduct that falls below the standards of behaviour established by law for the protection of others against unreasonable risk of harm. An organization can act negligently or be the victim of negligence by others. In addition, an organization can be negligent in the exercise of its own rights, obligations and liabilities resulting in damage to the organization. For example, if an organization fails to timely notify its insurance company of a loss it suffered, this negligence in the exercise of its rights can result in the loss not being covered under the organization's contract with the insurance company.

Category 6: Improper choice occurs when an organization has several courses of action to take in respect of a legal risk issue, all of which can be legal but each one presents different costs, implications and consequences, i.e. an alternative or alternatives are given up when a decision is made. For example, a company can choose to attempt to resolve a dispute with a trading partner through litigation or arbitration. Either approach – litigation or arbitration – could resolve the dispute but each will have different implications in terms of preserving the commercial relationship between the parties, reputation in the industry and community, time commitment involved, and costs incurred.

Annex B
(informative)

An example of a legal risk register

A legal risk register is a compilation of potential legal risk event occurrences with corresponding laws, possible outcomes and consequences. It helps the user to identify legal risks with respect to the relevant laws. An example is given in Table B.1.

Table B.1 — Example of a legal risk register

Operational activities	Legal risk category	Legal risk event identified (dates, occurrences)	Applicable relevant laws	Legal consequences	Past cases	Opinion of internal/in-house legal teams	Opinion of external legal advisor	Recommend-ed solution/ action plan

It is important that an organization compiling a legal risk register does so with guidance and supervision from its internal legal department and/or external legal advisors, ensuring that the legal risk register remains protected by the applicable legal professional privilege in each respective jurisdiction covered by the information it contains. An example is given in Table B.2.

If the legal risk register is not regularly maintained in coordination with appropriate legal professionals, a company could find that, in certain jurisdictions, for example, the legal risk register could be subject to disclosure in subsequent litigation, resulting in a loss of protection of the work product doctrine (or the equivalent protection applicable by local law).

In some common law jurisdictions, it can be possible to benefit from legal professional privilege by incorporating, as part of legal risk management, a process where incidents or claims are notified by the risk owner (if possible or even practicable) direct to external legal advisors who themselves retain, compile and complete a claims register. Local legal advice should be sought.

Table B.2 — Legal advice received, quantitative/qualitative analysis and decision

Legal risk event identified (dates, occurrences)	Opinion of internal/in-house legal team	Opinion of external legal advisors	Quantitative analysis of the legal risk problem	Qualitative analysis of the legal risk problem	Recommended treatment plan given to the board of the organization or to the responsi-ble team	Decision of the board or the responsible team

An organization should aim to review its legal risk register regularly. As part of this review a set of structured interview questions (see Table B.3) can be developed to seek input from the heads of business and operational teams, and to review both the exposure and the effectiveness of the control environment. The questions should align to the last review and should incorporate changes in the organization over the last period since review. The interviews are a useful method to reflect on previous periods and to explore new ways to partner with the business and operational teams to support them manage their legal risk. Certain legal risks will not always be escalated to the board of an organization but instead will be considered by the responsible team [i.e. the person(s) in the organization with the requisite authority] to make a decision in relation to the recommended treatment plan.

Table B.3 — Sample questions for structured interviews

Interview question	Purpose of question
How do risk controls influence decision-making on the management of legal risk?	How robust the senior manager considers the process for the management of legal risk. How well it is communicated and what information they use to monitor it.
How many of your contracts have an auto-renewal clause that will become effective?	Whether interviewees have a good view of their existing contracts, and actively manage them.
How many contracts does your organization enter into in a specified period?	Whether there is a contract management process in place.
How many transactions did your organization negotiate last year? What deviations to standard terms and conditions did it sign up to?	What level of governance is in place for negotiations.
What is the biggest cause of disputes against the organization?	Any potential problem areas and whether there is a general awareness of litigation issues.

Annex C
(informative)

An example for estimating the likelihood of events related to legal risk

Estimating the likelihood of events related to legal risk occurring is a two-step process.

First, it is determined whether a risk event could occur with a certain degree of likelihood. Second, it is determined if such a risk event has legal consequences or not and, hence, qualifies as a legal risk.

Once this second determination has been made, the legal risk is rated on a scale ranging from a minor legal risk with little or no likely regulatory or monetary consequences involved to a legal risk with significant regulatory or monetary consequences.

Table C.1 gives a non-exclusive list of some of the potential factors to consider, along with an appropriate rating.

A higher score indicates a higher likelihood of corresponding legal risks.

Different practical methodologies, e.g. using a weighted average formula, can be used to assess the likelihood of legal risks through the combination of scores of several factors from Table C.1.

Table C.1 — Assessing the likelihood of a legal risk event

Parameter	1	2	3	4	5
Effectiveness of risk and governance policies and procedures as set through internal controls	Policies and procedures for internal controls are well designed.	Policies and procedures for internal controls are complete.	Policies and procedures for internal controls are more likely than not complete.	Policies and procedures for internal controls are incomplete.	Policies and procedures for internal controls are non-existent.
	Policies and procedures for internal controls are fully implemented and reviewed regularly to ensure that they remain robust and appropriate to the changing needs of the organization.	Policies and procedures for internal controls are implemented.	Policies and procedures for internal controls are more likely than not implemented.	Policies and procedures for internal controls are insufficiently implemented.	Policies and procedures for internal controls are not implemented.

Table C.1 *(continued)*

Parameter	1	2	3	4	5
Adequacy of training for legal risk implications	Employees are fully aware of the legal risk implications applicable to the work they undertake for the organization and fully incorporate these principles into their day-to-day functions, setting best practice standards for the organization.	Employees are aware of the legal risk implications applicable to the work they undertake for the organization and incorporate these principles into their day-to-day functions.	Employees are aware of the legal risk implications applicable to the work they undertake for the organization and are more likely than not to incorporate these principles into their day-to-day functions.	Employees are aware of the legal risk implications applicable to the work they undertake for the organization but do not incorporate these principles into their day-to-day functions.	Employees are not aware of the legal risk implications applicable to the work they undertake for the organization.
Counterparty risk	The ability of the counterparty to comply with its contractual obligations is excellent and the probability of breach of contract or default on their part is not likely.	The ability of the counterparty to comply with its contractual obligations is very good and the probability of breach of contract or default on their part is less likely than not.	The ability of the counterparty to comply with its contractual obligations is good and the probability of breach of contract or default on their part is more likely than not.	The ability of the counterparty to comply with its contractual obligations is weak and the probability of breach of contract or default on their part is strong.	The ability of the counterparty to comply with its contractual obligations is extremely weak and the probability of breach of contract or default on their part is very strong.
Enforceability of laws	Very clear rules on enforceability. Very clear expectation that courts in the applicable jurisdiction will enforce the laws or judgments based on such laws.	Clear rules on enforceability. There is sound expectation that courts in the applicable jurisdiction will enforce the laws or judgments based on such laws.	Some clear rules on enforceability. Some reasonable expectation that courts in the applicable jurisdiction will enforce the laws or judgments based on such laws.	No clear rules on enforceability. Some reasonable expectation that courts in the applicable jurisdiction will enforce the laws or judgments based on such laws.	No clear rules on enforceability. No reasonable expectation that courts in the applicable jurisdiction will enforce the laws or judgments based on such laws.
Business activity	The related activities occur once a year.	The related activities occur once every quarter.	The related activities occur once a month.	The related activities occur once a week.	The related activities occur once a day.

Annex D
(informative)

An example for estimating the consequences of events related to legal risk

Events related to legal risk will result in financial, regulatory, reputational, geographical and intra-organizational consequences for the organization.

Quantitative analysis of legal risk consequences can be performed by subdividing each of the categories listed in Table C.1 along a spectrum that ranges from no consequence to severe consequence, depending upon the specific effects that the legal risk has upon the organization. Thus, each of the five categories listed in Table C.1 can be further divided along a spectrum of five grades from 1 to 5, with 1 indicating no legal risk consequence and 5 indicating a severe legal risk consequence. An example is given in Table D.1.

The weighting given for each of the five categories will vary depending on the organization involved and the complexity of the legal risk issues involved. An organization should develop its own weighting system to assess the consequence of a legal risk by evaluating the specific consequence of the five categories in line with similar organizations, the country or countries it operates in and the specific industry operations which are the subject of its focus. For example, a financial institution operating in a highly regulated industry on a global basis could give regulatory and reputational risk a greater weight than the other categories listed.

In customizing its management of legal risk, each organization may remove and/or add the categories used to evaluate the consequences of legal risk. The list of categories contained should not be an exclusive list.

Table D.1 — Example of an analysis of the consequence of legal risks

Parameter	1	2	3	4	5
Monetary consequence[a]	0 to 100 000	100 001 to 1 000 000	1 000 001 to 5 000 000	5 000 001 to 10 000 000	10 000 001+
Non-monetary consequence	Minor loss of reputation, corporate image or intellectual property.	Small loss of reputation, corporate image or intellectual property.	Loss of reputation, corporate image or intellectual property.	Substantial loss of reputation, corporate image or intellectual property.	Significant loss of reputation, corporate image or intellectual property.
Geographical consequence	The consequence is limited entirely to one country or the same region, the consequence of which on the overall organization's operations is minimal.	The consequence is limited to one or more countries (but not all countries where the organization operates) other than the jurisdiction in which the organization (or the holding organization owning or controlling the same) is incorporated or is "essentially at home" and the consequence on the overall organization's operations is moderate.	The consequence is limited to only the jurisdiction in which the organization (or the holding organization owning or controlling the same) is incorporated or is "essentially at home" and the consequence on the overall organization's operations is significant.	The consequence is limited to one or more countries (but not all countries where the organization operates) as well as the jurisdiction(s) in which the organization (or the holding organization owning or controlling the same) is incorporated or is "essentially at home" and the consequence on the overall organization's operations is significant.	The consequence is to all countries in which the organization operates, and the consequence is so pervasive as to be threatening to the entire organization.
Intra-organizational consequence	The consequence is limited entirely to one discrete area of the organization or one of its subsidiaries or operating divisions with a minimal overall consequence on the organization.	The consequence is limited entirely to one or more discrete areas of the organization or one of its subsidiaries or operating divisions with a moderate overall consequence on the organization.	The consequence is limited to only the organization or one of its subsidiaries or operating divisions and the consequence on overall operations is significant.	The consequence is limited to the organization and one or more of its subsidiaries or operating divisions and the consequence on overall operations is significant.	The consequence is to the entire organization and its subsidiaries and operating divisions and the consequence is so pervasive as to be threatening to the entire organization.

[a] The monetary impact thresholds will vary according to the size, nature of the organization, country in which the organization operates, and the currency values and fluctuations when operating in jurisdictions with differing currencies.