International Standard

ISO 18128

Information and documentation — Records risks — Risk assessment for records management

First edition
2024-03

Reference number
ISO 18128:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 46, *Information and documentation*, Subcommittee SC 11, *Archives/records 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

Successful organizations identify and manage all their business risks. Identifying and managing the risks to records processes, controls and systems (records risks) is the responsibility of the organization's records professionals.

This document is intended to help records professionals and people who have responsibility for records in their organization to assess records risks.

This is distinct from the task of identifying and assessing the organization's business risks to which creating and keeping adequate records is one strategic response. The decisions to create records or not in response to general business risks are business decisions, which should be informed by the analysis of the organization's records requirements undertaken by records professionals together with business managers. The premise of this document is that the organization has created records of its business activities to meet operational and other purposes and has established at least minimal mechanisms for the systematic management of the records.

The consequence of records risk events can be the loss of, or damage to, records, which are therefore no longer useable, reliable, authentic, complete, or unaltered, and therefore can fail to meet the organization's purposes.

The document provides guidance and examples based on the general risk management process established in ISO 31000 (see Figure 1) to apply to records risks, including information on relevant risk assessment tools and techniques. It covers the risk assessment components:

a) risk identification,

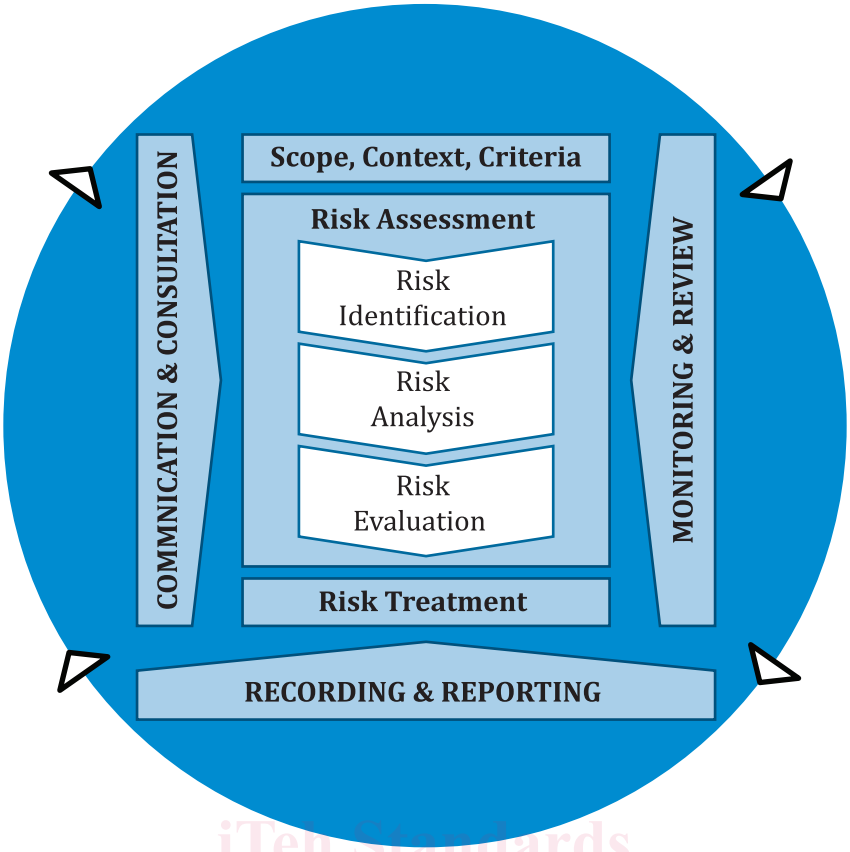
b) risk analysis, and

c) risk evaluation.

This document introduces and explains selected techniques from IEC 31010 that are applicable in a records management environment (see Table A.2 for the list of techniques).

The results of the assessment of records risk should be incorporated into the organization's general risk management framework. Consequently, the organization will have better control of its records and their quality for business purposes.

This document does not deal with risk treatment. Once the assessment of records risks has been completed, the assessed risks are documented and communicated to the organization's risk management section. Response to the assessed risks should be undertaken as part of the organization's overall risk management program. The priority assigned by the records professional to the assessed risks is provided to inform the organization's decisions about managing those risks.



NOTE Source ISO 31000:2018, Figure 4

Figure 1 — Risk management process

Information and documentation — Records risks — Risk assessment for records management

1 Scope

The document:

a) provides methods for identifying and documenting risks related to records, records processes, controls and systems (records risks);

b) provides techniques for analysing records risks;

c) provides guidelines for conducting an evaluation of records risks.

This document intends to assist organizations in assessing records risks so they can ensure records continue to meet identified business needs as long as required.

This document can be used by all organizations regardless of size, nature of their activities, or complexity of their functions and structure.

This document does not directly address the mitigation of risks, as methods for these vary from organization to organization.

It can be used by records professionals or people who have responsibility for records and records processes, controls and/or systems in their organizations, and by auditors or managers who have responsibility for risk management programs in their organizations.

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 30300, *Information and documentation — Records management — Core concepts and vocabulary*

ISO 31000, *Risk management — Guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 30300, ISO 31000 and the following apply.

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

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

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

3.1 Terms specific to risk

3.1.1
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: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 4 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

Note 5 to entry: In the high level structure's core terms and definitions for management systems stated in ISO/IEC Directives, Part 1:2019, Annex L , the definition of risk and the Notes to entry are slightly different.

[SOURCE: ISO 30300:2020, 3.1.26]

3.1.2
risk management
coordinated activities to direct and control an organization with regards to risk

[SOURCE: ISO 31000:2018, 3.2]

3.2 Terms specific to records

3.2.1
authoritative record
record (3.2.2) which possess the characteristics of authenticity, reliability, integrity and useability

[SOURCE: ISO 30300:2020, 3.2.3]

3.2.2
record
information created or received and maintained as evidence and as an asset by an organization, in pursuit of legal obligations or in the course of conducting business

Note 1 to entry: to entry; Records are normally used in plural.

Note 2 to entry: In a management system standard (MSS) implementation, the records created to conduct and direct the management system and to document its implementation are called documented information.

[SOURCE: ISO 30300:2020, 3.2.10]

3.2.3
records control
instrument for helping in the conduct of *records processes* (3.2.5)

EXAMPLE Examples of records controls include metadata schemas for records, business classification schemes, access and permission rules, and disposition authorities.

[SOURCE: ISO 30300:2020, 3.5.6]

3.2.4
records management (preferred term)
recordkeeping (admitted term)
field responsible for the efficient and systematic governance of *records* (3.2.2), using *records processes* (3.2.5), *records controls* (3.2.3) and *records systems* (3.2.7)

[SOURCE: ISO 30300:2020, 3.4.12]

3.2.5
records process
set of activities for managing authoritative records

[SOURCE: ISO 30300:2020, 3.4.13]

3.2.6
records requirements
requirements for evidence of a business function, activity or transaction and for for records processes including how, and how long, records need to be kept

[SOURCE: ISO 30300:2020, 3.3.2]

3.2.7
records risk
risk (3.1.1) related to *records* (3.2.2), *records processes* (3.2.5), *controls* (3.2.3) and *systems* (3.2.8)

Note 1 to entry: Risk management of records is associated with appraisal and records requirements

3.2.8
records system
information system that manages *records* (3.2.2) over time

[SOURCE: ISO 30300:2020, 3.6.4]

4 Core concepts

4.1 Issues and concerns about uncertainty

Uncertainty is a term which embraces many underlying concepts. Commonly recognized forms of uncertainty include decision uncertainty, which has particular relevance to risk management strategies, and which identifies uncertainty associated with value systems, professional judgement, organizational values and societal norms.

Examples of uncertainty include:

— uncertainty as to the truth of assumptions, including presumptions about how people or systems might behave;

— variability in the parameters on which a decision is to be based;

— uncertainty in the validity or accuracy of models which have been established to make predictions about the future;

— events (including changes in circumstances or conditions) whose occurrence, character or consequences are uncertain;

— uncertainty associated with disruptive events;

— the uncertain outcomes of systemic issues, such as shortages of competent staff , that can have wide ranging impacts which cannot be clearly defined;

— lack of knowledge which arises when uncertainty is recognized but not fully understood;

— unpredictability;

— uncertainty arising from the limitations of the human mind, for example in understanding complex data, predicting situations with long-term consequences or making bias-free judgments.

Not all uncertainty is able to be understood and the significance of uncertainty might be hard or impossible to define or influence. However, a recognition that uncertainty exists in a specific context enables early

warning systems to be put in place to detect change in a proactive and timely manner and make arrangements to build resilience to cope with unexpected circumstances.

5 Determining scope, context and criteria

5.1 General

The purpose of establishing the scope, the context and criteria is to customize the risk management process, enabling effective risk assessment and appropriate risk treatment.

In participating in the organization's risk management processes, records professionals can take into account:

a) their roles and responsibilities as technical experts in the field of records management, specifically in assessing records risks;

b) extent and scope of the risk assessment activities, specifically understanding relationships with other areas, such as incident management and information security. These relationships should be made explicit to avoid conflicts and duplication of efforts, and to enable an integrated approach to risk management;

c) methodology and reporting mechanisms, where, if possible, the standard risk assessment methodology and techniques should be applied;

d) risk criteria, where general risk criteria for the organization are established, records risks should be assessed using these criteria.

Assessing records risks should be integrated, where it exists, in the organization's general risk management process. Records professionals should consider the organization's external and internal context, specifically the organization's requirements for authoritative records to support its business needs and objectives.

Where the organization has not established a general risk management process, records professionals need to establish the risk criteria applying to records processes, controls and systems prior to the assessment process.

5.2 Defining the scope

The organization should define the scope of its risk management activities.

The risk management process can be applied at different levels (e.g. strategic, operational, program, project, or other activities). It is important to be clear about the scope under consideration, the relevant records objectives to be considered and their alignment with organizational objectives.

For records risk management, when planning the approach, considerations include:

— records objectives and decisions that need to be made;

— outcomes from the records appraisal process;

— specifics inclusions and exclusions;

— appropriate risk assessment techniques;

— outcomes expected from the steps to be taken in the process;

— resources required, responsibilities and records to be kept;

— relationships with other projects, processes, activities and objectives.

5.3 External and internal context

5.3.1 General

The external and internal context is the environment in which the organization seeks to define and achieve its objectives. Understanding the context is important because:

— risk management takes place in the context of the objectives and activities of the organization;

— organizational factors can be a source of risk;

— the purpose and scope of the risk management process can be interrelated with the objectives of the organization as a whole.

5.3.2 External context

The external context can include factors such as the social and cultural, legal, regulatory, financial, technological, economic, natural and competitive environment. External changes to the organization's context can affect the organization's operations and can directly or consequently impact its records requirements.

5.3.3 Internal context

The internal context can include factors such as:

— governance, organizational structure, roles and responsibilities;

— change of executive leadership such as elected officials or boards;

— political interference;

— information and recordkeeping culture, behaviour and practice;

— recordkeeping capacity and ethics;

— records and information systems, information flows and decision-making processes;

— technologies implemented, including legacy systems and external collaboration systems;

— standards, best practices, policies, guidelines and procedures adopted by the organization.

Internal changes to the organization context can impact the organization's operations and can directly affect records, records processes, controls and systems.

5.4 Definition of records risk criteria

5.4.1 The organization should specify the amount and type of risk that it can or can not take, relative to its objectives. It should also define criteria to evaluate the significance of risk to support decision-making processes. Records risk criteria should be aligned with the general risk criteria and with the risk management framework.

While risk criteria should be established at the beginning of the risk assessment process, they are dynamic and should be continually reviewed and amended, if necessary.

5.4.2 Risk criteria should be based on the organization's business, legal and other requirements, and the views of stakeholders. To set risk criteria, the following should be considered:

a) how consequences (both positive and negative) and likelihood will be defined and measured;

b) time-related factors;