International Standard

ISO 18128

First edition
2024-03

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



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,

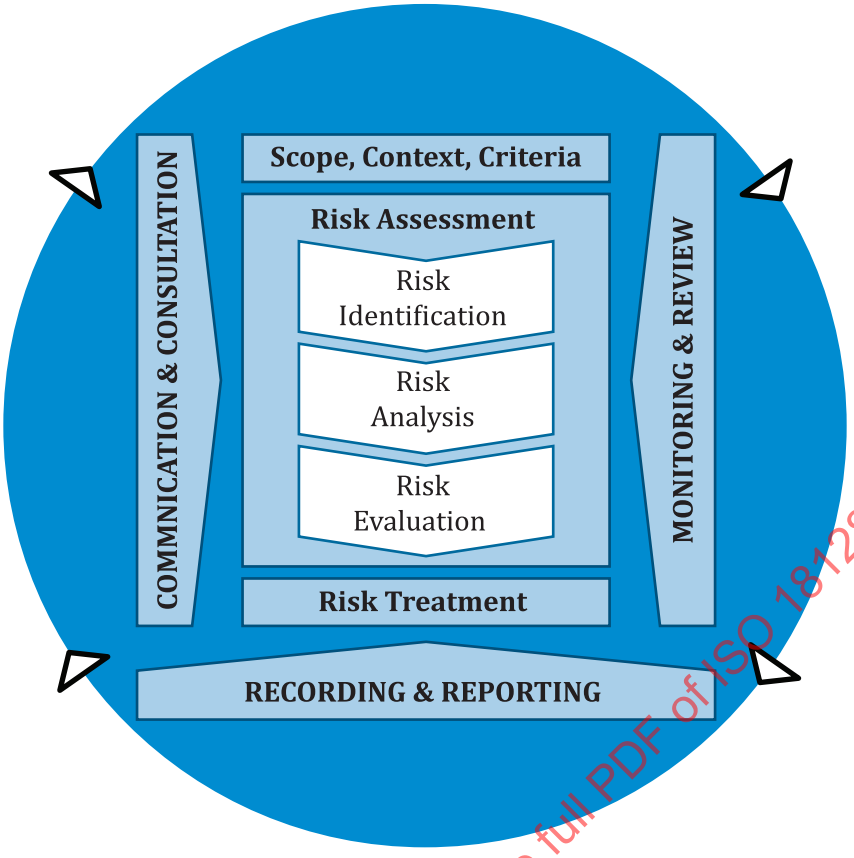
b) risk analysis, and

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;

c) consistency in the use of measurements;

d) how the level of risk is to be determined;

e) how combinations and sequences of multiple risks will be taken into account;

f) the organization's capacity;

g) how to decide when a risk is acceptable and/or tolerable;

h) how to decide when a risk needs treatment or escalation.

**5.4.3** To set records risk criteria, the following should be considered:

a) the nature and type of uncertainties that can affect records objectives and outcomes;

b) criticality or value of the records processes, controls and systems to the business operations;

c) value of the records created and the functions, activities or transactions it supports;

d) level of losses or impact on the authenticity, reliability, integrity and usability of the records;

e) size and scope of the records systems in the organization;

f) the reliability, security, procedure compliance, comprehensiveness, systematization and availability of records systems;

g) records system' integration with other business systems;

h) impacts of the risk to users and stakeholders;

i) risk events and the outcomes that needs to be avoided or seen as an opportunity;

j) amount and effectiveness of existing or possible practicable controls over the risk;

k) any benefits or opportunities presented by the risk to records or records management.

## 5.5 Risk description

Identified risks are generally described and communicated in the form of risk statements. Well-defined risk statements present useful and relevant information which enable organizations to utilize risk information to support decision making across the organization.

Risk statements should be clear, concise and relevant to the organization's business and its objectives. A well-defined risk statement can contain components such as:

— records, process or systems at risk;

— sources of risk or areas of uncertainty;

— event;

— consequences of the source of risk and event.

An example of a risk statement is shown in Figure 2:

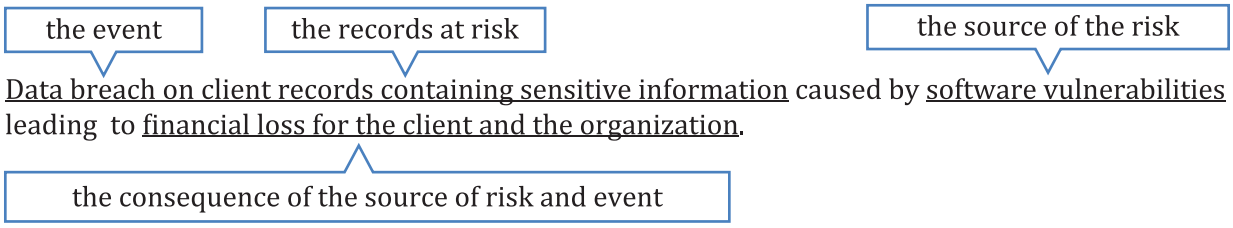



**Figure 2 — Example of a risk statement**

Clear, specific records risk statements should be developed to:

— raise awareness and understanding of records risks relevant to the organization;

— help plan and improve responses to risks;

— help improve records processes, controls and systems.

## 6 Uses of risk assessment techniques

The techniques described in this document provide a means to improve understanding of the risk assessment process and its implications for decision making.

ISO 31000 describes principles for managing risk and the foundations and organizational arrangements that enable risk to be managed. It specifies a process that enables risk to be recognized, understood and modified as necessary, according to criteria that are established as part of the process.

IEC 31010 describes multiple risk assessment techniques which are used:

— where further understanding is required about what risks exist or about a particular risk;

— within a risk management process leading to actions to treat risk;

— within a decision where a range of options each involving risk needs to be compared or optimized.

The way in which risk is assessed depends on the situation's complexity and novelty, and the level of relevant knowledge and understanding.

The techniques included and explained in this International Standard are applicable in a records management environment.

## 7 Risk identification

### 7.1 General

The purpose of records risk identification is to find, recognize and describe risks that can positively or negatively affect the ability of records to support the needs of the organization. The risk identification process includes identifying the causes and sources of the risk, events, situations, or circumstances which can have an impact upon the organization's objectives. Positive records risks, often referred to as opportunities, should also be considered. These can include risks that would strengthen an organization's records management capacity.

Specifically, records risks are identified based on their potential to:

— compromise or preserve the authenticity, reliability, integrity and useability of records;

— weaken or strengthen records processes, controls and systems;

— threaten or safeguard the reliability, security, procedure compliance, comprehensiveness and systematization of records systems.

Records professionals should identify all records risks, whether or not their sources are under their control or the organization's control. Consideration should be given that there can be more than one type of outcome, which can result in a variety of tangible or intangible consequences.

To identify records risks, records professionals should:

— understand the organization and its context (both external and internal), including any issues relevant to its objectives and that could affect its ability to achieve its business outcomes;

— identify business critical areas;

— identify records needs and requirements;

— document how, where and why records are created, captured, managed, and disposed of;

— assess the value and criticality of the records created and managed by the organization;

— consider the recordkeeping and information culture and behaviours and how these could affect records processes, controls and systems;

— be aware and have an understanding of the records systems and other business systems used to support the organization's activities;

— compile a list of possible sources of risks, including records system vulnerabilities and existing systems controls.

## 7.2 Techniques for identifying risks

### 7.2.1 General

There are numerous techniques for risk identification. To ensure that records support the business needs of the organization, records professionals should obtain inputs from various stakeholders such as subject matter experts, users and business owners. Risks can be identified through the formal risk management activities and through other normal organizational activities such as:

— assessment against standards;

— records of incidents or complaints;

— quality assurance and quality control activities;

— appraisal for records (more information can be found in ISO/TR 21946);

— audit activities;

— routine team meetings.

Records professionals can use different tools and techniques such as:

— brainstorming, to help identify new risks and innovative solutions;

— checklist analysis, where checklists relevant to the categories and particular event can be developed and assessed. Previous risk registers can be used as a starting point in risk identification;

— interviews, to get in-depth information and to allow exploration of issues on an individual basis;

— root cause analysis, to identify potential sources and causes of risks based on a similar event that has happened in the past.

Identified risks should be documented through the appropriate mechanisms in the organization.

### 7.2.2 Checklist analysis for risk identification

Checklists are used during risk assessment in various ways such as to assist in understanding the context, in identifying risk and in grouping risks for various purposes during analysis. They are also used when managing risk, for example to classify controls and treatments, to define accountabilities and responsibilities, or to report and communicate risk. This is one of the techniques one we can use in identifying records risks but there are other techniques.

A checklist can be based on experience of past failures and successes but more formally risk typologies and taxonomies can be developed to categorize or classify risks based on common attributes. Examples of commonly used checklists, classifications or taxonomies used at a strategic level to identify factors in the internal and external context include strengths, weaknesses, opportunities and threats (SWOT), and political, economic, social, technological, environmental, legal, ethical and demographic (PESTLE or STEEPLED). At an operational level, hazard checklists are used to identify hazards by source of risk or by consequence. See Table 1 for a checklist example.

**Table 1 — Checklist with examples of sources of records risks**

| Category | Possible source of risks |
|---|---|
| Records | Inadequate records creation processes<br>Inadequate records capture processes<br>Incorrect format when creating records<br>Incomplete metadada when capturing records |
| Records processes | System functionality to capture and manage records and metadata was not designed.<br>Lack or inadequate documentation for the processes.<br>Missing, incomplete, and/or inconsistent data captured.<br>Skill level of system administrators and their understanding of the records processes requirements for managing records in systems.<br>Technology and format obsolescence. |
| Records controls | Inadequate records controls in capturing records in the system.<br>Inadequate access rules, permissions and security policies.<br>User accidentally compromises sensitive data or information. |
| Records systems | Inadequate planning and control mechanisms within the business process and its system implementation.<br>Infeasibility of technology deployed against existing technology.<br>Lack of expertise and/or lack of resources to implement, maintain and keep the systems up to date.<br>Changes in business and operating systems affecting records systems.<br>Lack of support and maintenance.<br>Inadequate system performance in terms of productivity, efficiency, consistency, or other measures. |

In general, the more specific the checklist, the more restricted its use to the particular context in which it is developed. ISO 30301:2019, Annex A can serve as a basis to develop a checklist related to records processes, controls and systems.

NOTE Annex B is an example of a checklist of areas of uncertainty that can assist with determining records risks in an organisation.

## 8 Risk analysis

### 8.1 General

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources,

consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.

Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. The results provide insight for decisions, where choices are being made, and the options involve different types and levels of risk.

## 8.2 Techniques for analysing risks

### 8.2.1 General

Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available. Risk analysis should consider factors such as:

— the likelihood of events and consequences;

— the nature and magnitude of consequences;

— complexity and connectivity;

— time-related factors and volatility;

— sensitivity and confidence levels.

Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use. In the following clauses some techniques for the analysis of records risks are explained, but there are other techniques one can use for this purpose.

### 8.2.2 Business impact analysis (BIA)

This technique analyses how incidents and events can affect records and records management in the organization, and identifies and quantifies the capabilities that would be needed to manage it. Specifically, a BIA provides an agreed understanding of:

— the criticality of key records processes, systems and controls, associated resources and the key interdependencies that exist for an organization;

— how disruptive events will affect the capacity and capability of achieving critical records objectives;

— the capacity and capability needed to manage the impact of a disruption and recover to agreed levels of records management operation.

BIA can be used to determine the criticality and recovery time frames of records processes and associated resources (e.g. people, information technology, systems) to enable appropriate planning for disruptive events. BIA also assists in determining interdependencies and interrelationships between records processes, and internal and external parties.

BIA can be undertaken using questionnaires, interviews, structured workshops or a combination of all three. It provides information that helps the organization determine and select appropriate records continuity strategies to enable effective response and recovery from a disruptive incident.

The inputs to conduct effective BIA to analyse records risks can include:

— information concerning the objectives, strategic direction, environment, assets, and interdependencies of the organization;

— overview of the organization's business products and services and their relationship to records processes and systems;

— an assessment of priorities from previous management review;

— details of the activities and functions of the organization, including processes, resources, relationships with other organizations, supply chains, outsourced processes and functions, and stakeholders;

— information to enable assessment of financial, legal and operational consequences of loss of vital records;

— a list of people from relevant areas of the organization and/or stakeholders that will be contacted.

The outputs include:

— a prioritized list of the organization's products and services;

— a prioritized list of critical processes and associate interdependencies;

— documented impacts from a loss of records and its impact in the critical business processes, including financial, legal, environmental and operational impacts;

— information on records needed to re-establish critical processes.

### 8.2.3 Human reliability analysis (HRA)

This technique refers to a group of techniques that aim to evaluate a person's contribution to the system reliability and safety by identifying and analysing the potential for an incorrect action. HRA is applied at a tactical level to particular tasks where correct performance is critical.

The technique can be used during the design, implementation and modification stages of records management so that they are designed and maintained to minimize errors. For example, HRA can be used:

— during design so that records systems are designed to minimize the probability of error by workers;

— to improve procedures so as to reduce errors.

A hierarchical task analysis is first carried out to identify steps and sub-steps within activities in the records processes and systems.

Potential error mechanisms are identified for each sub-step often using a set of keyword prompts (such as too early, too late, wrong object, wrong action, right object).

Sources of these errors (such as distraction, lack of available time, misfiling, etc.) can be identified and the information can be used to reduce the likelihood of error within the task.

Factors within the individuals themselves, the organization or the environment that influence the probability of error [such as performance shaping factors (PSFs)] are also identified.

The probability of an incorrect action can be estimated by various methods including using a data-base of similar tasks or expert judgement, such as processing guidelines. Typically, a nominal error rate for a task type is defined and then a multiplier is applied to represent behavioural or environmental factors that increase or decrease the probability of failure.

Outputs of this technique include:

— a list of errors or extraordinary performance that can occur and methods by which they can be enhanced through redesign of the records system;

— human performance modes, types, causes and consequences;

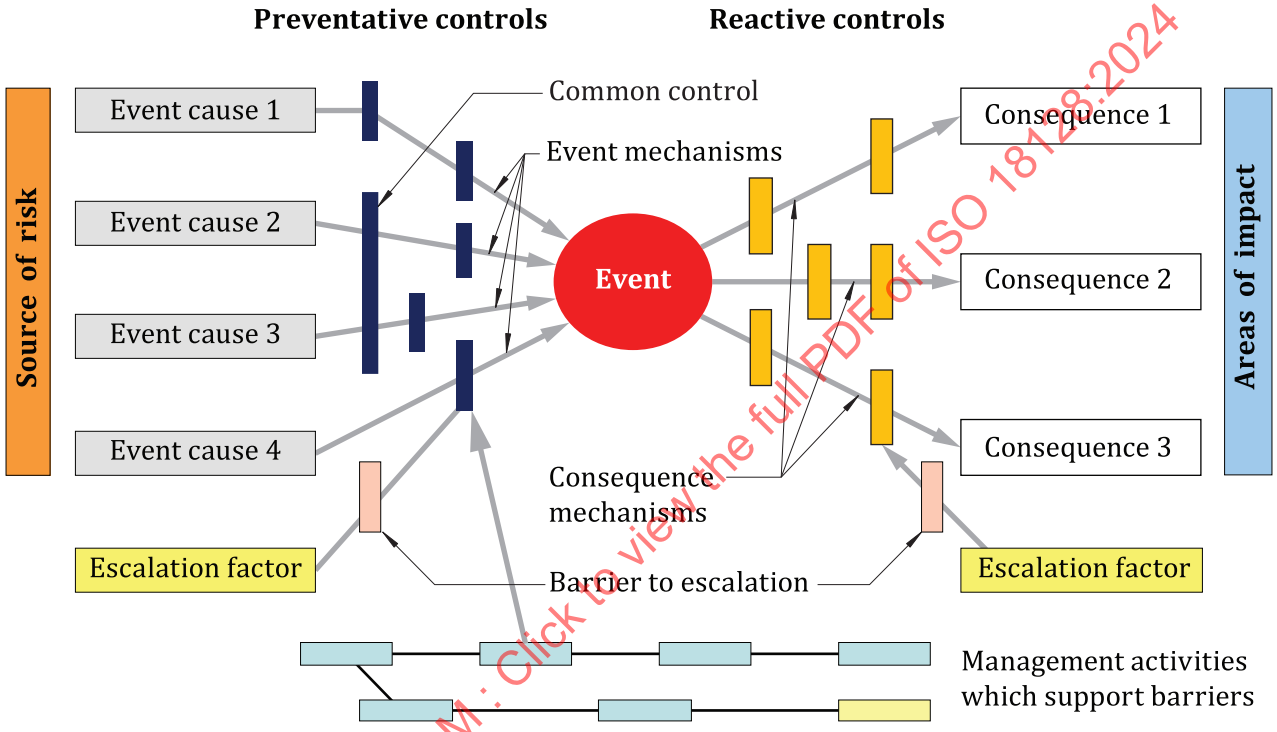
— a qualitative or quantitative assessment of the risk posed by differences in performance.

Various methods have been developed to apply these basic steps. Early methods placed a strong emphasis on estimating the likelihood of failure. More recent qualitative methods focus on cognitive causes of variations in human performance with greater analysis of the way performance is modified by external factors and less on attempting to calculate a failure probability.

### 8.2.4 Bow tie analysis

A bow tie is a graphical depiction of pathways from the causes of an event to its consequences. It shows the controls that modify the likelihood of the event and those that modify the consequences if the event occurs. Bow tie diagrams can be constructed starting from fault and event trees, but are more often drawn directly by a team in a workshop scenario.

This technique is used to display and communicate information about risks in situations where an event has a range of possible causes and consequences. A bow tie is used when assessing controls to check that each pathway from cause to event and event to consequence has effective controls, and that factors that could cause controls to fail (including management systems failures) are recognized. It can be used as the basis of a means to record information about a risk that does not fit the simple linear representation of a risk register.




NOTE IEC 31010:2019, Figure B.2.

**Figure 3 — Example of bow tie analysis**

The bow tie is drawn as follows.

— The event of interest is represented by the central knot of the bow tie, see Figure 3.

— Sources of risk (or hazards/threats in a safety context) are listed on the left hand side of the knot and joined to the knot by lines representing the different mechanisms by which sources of risk can lead to the event.

— Barriers or controls for each mechanism are shown as vertical bars across the lines.

— On the right-hand side of the knot lines are drawn to radiate out from the event to each potential consequence.

— After the event, vertical bars represent reactive controls or barriers that modify consequences.

— Factors that might cause the controls to fail (escalation factors) are added, together with controls for the escalation factors.

— Management functions which support controls (such as training and inspection) can be shown under the bow tie and linked to the respective control.

Some level of quantification for a bow tie diagram can be possible where pathways are independent, the probability of a particular consequence or outcome is known, and the probability that a control will fail can be estimated. However, in many situations, pathways and barriers are not independent, and controls can be procedural and their effectiveness uncertain.

The output is a simple diagram showing main risk pathways, the controls in place, and the factors that might lead to control failure. It also shows potential consequences and the measures that can be taken after the event has occurred to modify them.

# 9 Risk evaluation

## 9.1 General

Risk evaluation is the third and last component of the risk assessment process. The purpose of risk evaluation is to support decisions about which risks need treatment and the priority for treatment implementation. It involves comparing the results of the risk analysis with the established criteria to determine where additional action is required. This can lead to a decision to:

— do nothing further;

— consider risk treatment options;

— undertake further analysis to better understand the risk;

— maintain existing controls;

— reconsider objectives.

The outcome of risk evaluation should be recorded, communicated and validated at appropriate levels of the organization.

In the following clauses some techniques for the evaluation of records risks are explained, but there are other techniques one can use for this purpose.

## 9.2 Techniques for evaluating risk

### 9.2.1 As low as reasonably practicable (ALARP)

This technique can be used to decide whether a particular risk is tolerable or acceptable and generally requires that the level of risk is reduced to as low as reasonably practicable.

The ALARP model can be used to evaluate the analysed records risks, based on an organization's risk appetite, and to decide, for example, whether a particular risk is:

— intolerable, where the risk cannot be justified except in extraordinary circumstances;

— tolerable, where risk should be further reduced if it is reasonably practicable;

— broadly acceptable (the ALARP region, between intolerable and tolerable), where the risk is so low that further risk reduction need not be considered.

The output is a decision about whether treatment is required and the treatment to be applied.

Table 2 shows an example of risk classification using ALARP model, based on the organization's size and nature of its activities, and its risk appetite.

**Table 2 — Example of classification of risks using ALARP model**

| Minor | Moderate | Major | Severe |
|---|---|---|---|
| Anomalous breach of access restriction to records[a] | Unauthorised access to records[b] | Unauthorised access to records — shall be reported[b] | Widespread loss, unauthorised access and damage to records[c] |
| Damage to small quantity of records in one area of operations[a] | Damage to significant quantity of records in one area of operations[b] | Damage to operational records spreading to several areas[b] | Damage to vital records in a majority of areas of operations[c] |
| Limited loss of records/data[b] | Loss of data/damage to the reliability of records[b] | Loss of data/damage to the reliability of records; damage to reputation[b] | Loss of data/loss of reliability/loss of public trust[c] |
| Recoverable loss of records[b] | Operations not disrupted; records recoverable with effort[b] | Loss admitted; disruption to more than one area of operations; recovery effort costly or not possible[c] | Operations shut down; recovery effort costly and time-consuming; records not recoverable[c] |
| [a] Broadly acceptable, can be reduced ALARP. | | | |
| [b] Tolerable, and should be reduced ALARP. | | | |
| [c] Intolerable. | | | |

NOTE Core records are records which are central for an organization operations but not vital.

ALARP technique is not only used as a risk classification tool but also used to consider the risk mitigation strategy, as it requires the organization to reduce the risk to a level that is as low as reasonably practicable.

### 9.2.2 Reliability-centred maintenance (RCM)

**9.2.2.1** This technique is a risk-based assessment technique to optimize the maintenance of records and the performance of records processes, controls and systems. RCM technique operates on the belief that to uphold the authenticity, integrity, reliability, and useability of records and records processes, controls and systems one shall:

a) proactively identify hidden risks or failures;

b) apply preventative maintenance tasks or proactive corrective actions.

It determines what must be done on the records processes, controls and systems to ensure that records are always protected and available over time. RCM focuses on applying preventative maintenance tactics to reduce failure consequences. It enables the magnitude of risk to be used to make maintenance decisions.

**9.2.2.2** The necessary steps of applying an RCM technique in the context of records management are:

a) identify records, records processes, controls and systems that support business functions and activities, often best applied during the design and development phase of the records systems then implemented during the operation and maintenance stage;

b) articulate how and in what manner the records support the business activities and their productivity goals;

c) determine and address all plausible ways in which records processes and/or components of systems could be subject to risks or failures, and their cause and effect to the reliability and availability of the records;

d) establish and implement technically feasible and cost-effective maintenance tactics; and

e) review program and practice continuous improvement.

RCM is used to enable applicable and effective maintenance to be performed. It is generally applied during the design and development phase of a system, then implemented during operation and maintenance.

Successful application of RCM needs a good understanding of the recordkeeping principles and fundamentals, tools and structure involved, the operational environment and the associated subsystems, together with the consistently applied analysis of the possible failure and the consequences of those failures. The end result of working through the process is a judgment as to the necessity of performing a maintenance task or other action such as operational changes.

The output is appropriate failure management policies for each failure mode, such as condition monitoring, failure finding, schedule restoration, replacement based on an interval (such as calendar, running hours, or number of cycles) or run-to-failure. Other possible actions that can result from the analysis include redesign, changes to operating or maintenance procedures or additional training. An example is given in Table 3.

**Table 3 — Example of a list of maintenance tasks by applying an RCM technique**

| Functional failures affecting the integrity, availability of records and records systems | | | | |
|---|---|---|---|---|
| Records/Records processes, systems or controls | Failure mode | Causes | Task type | Mitigation task description and interval |
| Records: vital records | Loss | Damages to the system either by wilful attack or system failure or as a result of natural disaster | Proactive<br>Proactive | Set up a daily backup regime<br>Rehearse the backup restore process and coordination once a year, and address all the issues identified have been<br>Store vital records in a controlled environment<br>Copy/digitise or duplicating physical records |
| Records process: disposition | Loss | Unauthorised destruction | Preventative<br>Proactive | Limit the number of people who have permission to destroy records<br>Training and awareness about records disposal |
| Records controls: access to records | Unauthorised access | Breach by internal staff members | Proactive<br>Reactive | Review records access or access membership groups on an annual basis<br>Review of default access provision applied to the records classification scheme on an annual basis<br>Provide user awareness training continuously<br>Review access regime once every three months<br>Audit user access logs to identify possible breach on a quarterly basis.<br>Study the incident and understand the root cause, refine records control measures |
| Records system | Compromised | Cyber attack | Preventative<br>Proactive | Perform a cyber-security test once a year<br>Perform system security patching once a month<br>Improve network security (e.g. firewall) |
| Records system | System outage | Poor system performance or unstable platform<br>Power outage | Preventative<br>Proactive | Perform system health check twice a year<br>Set up backup power |



### 9.2.3 Risk indices

This technique provides a method for measuring risk using a scoring approach. It can be used to compare different risks, determining the most severe risk, and understanding how risk changes over time. Measuring risk by combining the likelihood and impact index, allows the seriousness and importance of the risks clearly identified.

The effectiveness of using this technique relies on a consistent approach in scoring each part of the system and maintain their correct relationship. The inputs are derived from the analysis process. This requires a good understanding of all the sources of risk and how consequences can arise.

Developing an index is interactive. Several different systems for combining the scores should be tried to validate the method.

The output is a series of numbers (composite indices) that relate to a particular risk and which can be compared with indices developed for other risks within the same system.

— Risk event, identified as part of the risk identification process

— Probability score, identified during risk analysis, and by assigning a score

— Impact score, obtained as part of the risk analysis and by assigning a score

— Risk score = IMPACT × PROBABILITY

— Risk index: 1-2 = Low; 3-4 = Medium ; 5-10 = High; and 12-16 = Extreme

**Table 4 — Example of risk index system using composite scoring**

| Risk EVENT | Probability | | | | IMPACT | | | | Risk Score | Risk Index |
|---|---|---|---|---|---|---|---|---|---|---|
| | Rare 1 | Low 2 | Medium 3 | High 4 | Minor 1 | Moderate 2 | Major 3 | Severe 4 | | |
| Records misclassified, wrong access status | | | | High Monthly or more | Recoverable under existing procedures | | | | 4 | Med |
| Changes to privacy protection law | | | Medium Once a year | | | Affects access restrictions; flow on to other operations | | | 6 | High |
| Indexing function of records system fails | | Low Once every 3 years | | | Recoverable under existing procedures | | | | 2 | Low |
| Records wrongly identified for destruction | | | Medium Once a year | | Recoverable under existing procedures | | | | 3 | Med |
| Unauthorised access to employee records | | Low Once every 3 years | | | | Not recoverable | | | 4 | Med |
| Interruption to power supplies for 8 h | | Low Once every 3 years | | | | | Affects all records systems; one day's transactions lost | | 6 | High |

**Table 4** *(continued)*

| Risk EVENT | Probability | | | | IMPACT | | | | Risk Score | Risk Index |
|---|---|---|---|---|---|---|---|---|---|---|
| | Rare 1 | Low 2 | Medium 3 | High 4 | Minor 1 | Moderate 2 | Major 3 | Severe 4 | | |
| Cyber-attack on records system, affecting personal data | | | | High Monthly or more | | | | Loss of public trust, and records integrity | 16 | Extreme |
| Fire destroys records repository | Rare Once every 10 years | | | | | | | Loss of significant records; disruption to operation; loss of public trust | 4 | Med |
| Uncoordinated system maintenance affecting critical business operations | | | Medium Once a year | | | | | Loss of public trust, and records and systems integrity | 12 | Extreme |

### 9.2.4 Cost/benefit analysis

Cost/benefit analysis is a risk evaluation technique of identifying, measuring and comparing the total expected costs of options in monetary terms against their total expected benefits. It is often used at operational and strategic levels to help decide between options.

NOTE Direct costs are those that are directly associated with the action. Indirect costs are those additional opportunity costs, such as loss of utility, distraction of management time or the diversion of capital away from other potential investments.

For example, an old payroll system that contains summary information of employment history is no longer actively used but needs to be maintained in a read-only mode to deal with queries on employment history or verify benefit claims. The employment summary records, constituted by the data in the old payroll system, need to be retained in context for a minimum of 50 years or more for the organization to discharge its legal obligations, and to deal with possible law suits or benefits claims. Using the cost/benefit analysis can help the organization to make a sound decision on the most cost-effective way to retain the authenticity and availability of the summary of employment history records.

The output of a cost/benefit analysis is information on relative costs and benefits of different options or actions, as outlined in Table 5.

**Table 5 — Example of cost/benefit options analysis**

| | Option 1 | Option 2 | Option 3 |
|---|---|---|---|
| **Description** | Keep the old payroll system running for another 20 years and then deal with it. | Migrate records to the new payroll system. | Hire a Database Specialist to construct a summary of employment history report for each record (employee) in the system and have the reports archived in an organization's recordkeeping system. |
| **Benefits** | Records retained in its original environment, most reliable for the next 2-3 years. | Mitigate records loss and privacy breach. | Fully and accurately maintained employment summary records, as well as having the records available over time by keeping them in a recordkeeping system. |
| **Risk consideration** | The risk of a total loss of records and data caused by corruption of the read-only system as it is no longer actively supported.<br>Either apply the most stringent maintenance regime (more costly) or low maintenance, meant a higher risk for it to be subject to cyber-attack, which then causes data and privacy breaches.<br>This risk increases proportionally as the longer the years the system has been left unmanaged. | The metadata schema crosswalk between the two systems is not a direct match. The old records should be remediated in order to be migrated to the new system. This can compromise or damage the authenticity of the employment summary records when their old contextual data scheme is no longer available. | It requires a Database Specialist who is fully skilled and has in-depth knowledge of the old payroll system to ensure the reports are generated to maintain its authenticity and reliability. The risk is reduced significantly if this activity is undertaken while the existing Database Specialist resource is still available, either before or immediately after the adoption of the new payroll system. |
| Cost | The cost to maintain the old system is $30 000 a year.<br>The cost of total ownership is increasing every year.<br>The total cost increases with time, the longer the system has been left unmanaged.<br>5 years = $30 000 x 5 years plus the cost of option 2 or 3 (e.g. $350 000 or $200 000).<br>10 years = $30 000 x 10 years plus the cost of option 2 or 3 (e.g. $550 000 or $350 000).<br>50 years = $30 000 x 50 years is $1 500 000. | The project cost for records and data migration is a one-time cost of $200 000. | The cost for a Database Specialist to construct a summary of employment history report is a one-time cost of $50 000. |

This cost/benefit analysis gives a clear indication that option 3 is the most cost-effective way of maintaining the authenticity and availability of an organisation's summary of employment records from its old payroll system.

NOTE Table 5 aims to provide an example of a cost/benefits analysis with a focus on mitigating the risk of losing access and not inability to retain full and accurate records. The actual possible cost/benefits situation can be vastly different pending on the individual circumstance and objectives of an organization or the environment it operates within.

# Annex A
(informative)

# Categorization of techniques following IEC 31010

## A.1 Introduction to categorization of techniques following IEC 31010

Table A.1 explains the characteristics of techniques that can be used for selecting which technique or techniques to use.

**Table A.1 — Characteristics of techniques**

| Characteristic | Description | Details (e.g. features indicators) |
|---|---|---|
| Application | How the technique is used in risk assessment (see B.1 to B.10) | Elicit views, identify, analyse cause, analyse controls, etc. |
| Scope | Applies to risk at organizational level, departmental or project level or individual processes or equipment level | organization (org)<br>project/department (dep)<br>equipment/process (equip/proc) |
| Time horizon | Looks at short-, medium- or long-term risk or is applicable to any time horizon | Short, medium, long, any |
| Decision level | Applies to risk at a strategic, tactical or operational level | Strategic (1), tactical (2), operational (3) |
| Starting info/data needs | The level of starting information or data needed | High, medium, low |
| Specialist expertise | Level of expertise required for correct use | low: intuitive or one to two days' training<br>moderate: training course of more than two days<br>high: requires significant training or specialist expertise |
| Qualitative – quantitative | Whether the method is qualitative, semi-quantitative or quantitative | quantitative (quant)<br>qualitative (qual)<br>semi-quantitative (semi-quant)<br>can be used qualitatively or quantitatively (either) |
| Effort to apply | Time and cost required to apply technique | high, medium, low |



## A.2 Application of categorization of techniques following IEC 31010

Table A.2 lists a range of techniques classified according to these characteristics. The techniques described represent structured ways of looking at the problem in hand that have been found useful in particular contexts. The list is not intended to be comprehensive but covers a range of commonly used techniques from a variety of sectors. For simplicity the techniques are listed in alphabetical order without any priority.

**Table A.2 — Techniques and indicative characteristics**

| Clause | Technique | Description | Application | Scope | Time horizon | Decision level | Starting info/data needs | Specialist expertise | Qual/ quant/ semi-quant | Effort to apply |
|---|---|---|---|---|---|---|---|---|---|---|
| 9.2.1 | ALARP/SFAIRP | Criteria for deciding significance of risk and means of evaluating tolerability of risk. | evaluate. risk | 1 | any | 1/2 | high | high | qual/ quant | high |
| 8.2.4 | Bow tie analysis | A diagrammatic way of describing the pathways from sources of risk to outcomes, and of reviewing controls. | Analyse risk<br>analyse controls<br>describe risk | 2/3 | short/ medium | any | low | low/ moderate | qual/semi-quant | low |
| 8.2.2 | Business impact analysis | The BIA process analyses the consequences of a disruptive incident on the organization which determines the recovery priorities of an organization's products and services and, thereby, the priorities of the activities and resources which deliver them. | analyse conseq.<br>analyse controls | 1 | short/ medium | 2 | medium | low | quant/ qual | medium |
| 7.2.2 | Checklists classifications, taxonomies | Lists based on experience or on concepts and models that can be used to help identify risks or controls. | identify risk or controls | 2/3 | any | any | high to develop, low to use | low/ moderate | qual | low/medium |
| 9.2.4 | Cost/benefit analysis | Uses money as a scale for estimating positive and negative, tangible and intangible, consequences of different options. | compare options | any | short/ medium | any | medium / high | moderate/ high | quant | medium/ high |
| 8.2.2 | Human reliability analysis (HRA) | A set of techniques for identifying the potential for human error and estimating the likelihood of failure. | analyse risk and sources of risk | 2/3 | any | 2/3 | medium | high | qual/ quant | medium to high |
| 9.2.2 | Reliability centred maintenance (RCM) | A risk based assessment used to identify the appropriate maintenance tasks for a system and its components. | evaluate risk<br>decide controls | 2/3 | medium | 2/3 | medium | high for facilitator, moderate to use | qual/semi-quant/ quant | medium/ high |
| 9.2.3 | Risk indices | Rates the significance of risks based on ratings applied to factors which are believed to influence the magnitude of the risk. | compare risks | any | any | any | medium | low to use, moderate to develop | semi-quant | low |