INTERNATIONAL STANDARD

ISO/IEC 27005

Fourth edition
2022-10

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information

Reference number
ISO/IEC 27005:2022(E)

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) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 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 or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC 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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This fourth edition cancels and replaces the third edition (ISO/IEC 27005:2018), which has been technically revised.

The main changes are as follows:

— all guidance text has been aligned with ISO/IEC 27001:2022, and ISO 31000:2018;

— the terminology has been aligned with the terminology in ISO 31000:2018;

— the structure of the clauses has been adjusted to the layout of ISO/IEC 27001:2022;

— risk scenario concepts have been introduced;

— the event-based approach is contrasted with the asset-based approach to risk identification;

— the content of the annexes has been revised and restructured into a single annex.

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 and www.iec.ch/national-committees.

Introduction

This document provides guidance on:

— implementation of the information security risk requirements specified in ISO/IEC 27001;

— essential references within the standards developed by ISO/IEC JTC 1/SC 27 to support information security risk management activities;

— actions that address risks related to information security (see ISO/IEC 27001:2022, 6.1 and Clause 8);

— implementation of risk management guidance in ISO 31000 in the context of information security.

This document contains detailed guidance on risk management and supplements the guidance in ISO/IEC 27003.

This document is intended to be used by:

— organizations that intend to establish and implement an information security management system (ISMS) in accordance with ISO/IEC 27001;

— persons that perform or are involved in information security risk management (e.g. ISMS professionals, risk owners and other interested parties);

— organizations that intend to improve their information security risk management process.

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

1 Scope

This document provides guidance to assist organizations to:

— fulfil the requirements of ISO/IEC 27001 concerning actions to address information security risks;

— perform information security risk management activities, specifically information security risk assessment and treatment.

This document is applicable to all organizations, regardless of type, size or sector.

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/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 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 related to information security risk

3.1.1
external context
external environment in which the organization seeks to achieve its objectives

Note 1 to entry: External context can include the following:

— the social, cultural, political, legal, regulatory, financial, technological, economic, geological environment, whether international, national, regional or local;

— key drivers and trends affecting the objectives of the organization;

— external interested parties' relationships, perceptions, values, needs and expectations;

— contractual relationships and commitments;

— the complexity of networks and dependencies.

[SOURCE: ISO Guide 73:2009, 3.3.1.1, modified — Note 1 to entry has been modified.]

3.1.2
internal context
internal environment in which the organization seeks to achieve its objectives

Note 1 to entry: Internal context can include:

— vision, mission and values;

— governance, organizational structure, roles and accountabilities;

— strategy, objectives and policies;

— the organization's culture;

— standards, guidelines and models adopted by the organization;

— capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

— data, information systems and information flows;

— relationships with internal interested parties, taking into account their perceptions and values;

— contractual relationships and commitments;

— internal interdependencies and interconnections.

[SOURCE: ISO Guide 73:2009, 3.3.1.2, modified — Note 1 to entry has been modified.]

3.1.3
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected, positive or negative.

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

Note 3 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an *event* (3.1.11), its *consequence* (3.1.14), or *likelihood* (3.1.13).

Note 4 to entry: Risk is usually expressed in terms of *risk sources* (3.1.6), potential events, their consequences and their likelihood.

Note 5 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.

Note 6 to entry: Information security risks are usually associated with a negative effect of uncertainty on information security objectives.

Note 7 to entry: Information security risks can be associated with the potential that *threats* (3.1.9) will exploit *vulnerabilities* (3.1.10) of an information asset or group of information assets and thereby cause harm to an organization.

[SOURCE: ISO 31000:2018, 3.1, modified — the phrase: “It can be positive, negative or both, and can address, create or result in opportunities and threats” has been replaced with “positive or negative” in Note 1 to entry; the original Note 3 to entry has been renumbered as Note 4 to entry; and Notes 3, 5, 6 and 7 to entry have been added.]

3.1.4
risk scenario
sequence or combination of *events* (3.1.11) leading from the initial cause to the unwanted *consequence* (3.1.14)

[SOURCE: ISO 17666:2016, 3.1.13, modified — Note 1 to entry has been deleted.]

3.1.5
risk owner
person or entity with the accountability and authority to manage a *risk* (3.1.3)

[SOURCE: ISO Guide 73:2009, 3.5.1.5]

3.1.6
risk source
element which alone or in combination has the potential to give rise to *risk* (3.1.3)

Note 1 to entry: A risk source can be one of these three types:

— human;

— environmental;

— technical.

Note 2 to entry: A human risk source type can be intentional or unintentional.

[SOURCE: ISO 31000:2018, 3.4, modified — Notes 1 and 2 to entry have been added.]

3.1.7
risk criteria
terms of reference against which the significance of a *risk* (3.1.3) is evaluated

Note 1 to entry: Risk criteria are based on organizational objectives, and *external context* (3.1.1) and *internal context* (3.1.2).

Note 2 to entry: Risk criteria can be derived from standards, laws, policies and other requirements.

[SOURCE: ISO Guide 73:2009, 3.3.1.3]

3.1.8
risk appetite
amount and type of *risk* (3.1.3) that an organization is willing to pursue or retain

[SOURCE: ISO Guide 73:2009, 3.7.1.2]

3.1.9
threat
potential cause of an *information security incident* (3.1.12) that can result in damage to a system or harm to an organization

3.1.10
vulnerability
weakness of an asset or *control* (3.1.16) that can be exploited so that an *event* (3.1.11) with a negative *consequence* (3.1.14) occurs

3.1.11
event
occurrence or change of a particular set of circumstances

Note 1 to entry: An event can have one or more occurrences, and can have several causes and several *consequences* (3.1.14).

Note 2 to entry: An event can also be something that is expected which does not happen, or something that is not expected which does happen.

[SOURCE: ISO 31000:2018, 3.5, modified — Note 3 to entry has been removed.]

3.1.12
information security incident
single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

3.1.13
likelihood
chance of something happening

Note 1 to entry: In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

[SOURCE: ISO 31000:2018, 3.7]

3.1.14
consequence
outcome of an *event* (3.1.11) affecting objectives

Note 1 to entry: A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Note 2 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 3 to entry: Any consequence can escalate through cascading and cumulative effects.

[SOURCE: ISO 31000:2018, 3.6]

3.1.15
level of risk
significance of a *risk* (3.1.3), expressed in terms of the combination of *consequences* (3.1.14) and their *likelihood* (3.1.13)

[SOURCE: ISO Guide 73:2009, 3.6.1.8, modified — the phrase: "magnitude of a risk or combination of risks" has been replaced with "significance of a risk".]

3.1.16
control
measure that maintains and/or modifies *risk* (3.1.3)

Note 1 to entry: Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO 31000:2018, 3.8]

3.1.17
residual risk
risk (3.1.3) remaining after *risk treatment* (3.2.7)

Note 1 to entry: Residual risk can contain unidentified risk.

Note 2 to entry: Residual risks can also contain retained risk.

[SOURCE: ISO Guide 73:2009, 3.8.1.6, modified — Note 2 to entry has been modified.]

3.2 Terms related to information security risk management

3.2.1
risk management process
systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing *risk* (3.1.3)

[SOURCE: ISO Guide 73:2009, 3.1]

3.2.2
risk communication and consultation
set of continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with interested parties regarding the management of *risk* (3.1.3)

Note 1 to entry: The information can relate to the existence, nature, form, *likelihood* (3.1.13), significance, evaluation, acceptance and treatment of risk.

Note 2 to entry: Consultation is a two-way process of informed communication between an organization and its interested parties on an issue prior to making a decision or determining a direction on that issue. Consultation is:

— a process which impacts on a decision through influence rather than power;

— an input to decision making, not joint decision making.

3.2.3
risk assessment
overall process of *risk identification* (3.2.4), *risk analysis* (3.2.5) and *risk evaluation* (3.2.6)

[SOURCE: ISO Guide 73:2009, 3.4.1]

3.2.4
risk identification
process of finding, recognizing and describing *risks* (3.1.3)

Note 1 to entry: Risk identification involves the identification of *risk sources* (3.1.6), *events* (3.1.11), their causes and their potential *consequences* (3.1.14).

Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and interested parties' needs.

[SOURCE: ISO Guide 73:2009, 3.5.1, modified — "interested party" has replaced "stakeholder" in Note 2 to entry.]

3.2.5
risk analysis
process to comprehend the nature of *risk* (3.1.3) and to determine the *level of risk* (3.1.15)

Note 1 to entry: Risk analysis provides the basis for *risk evaluation* (3.2.6) and decisions about *risk treatment* (3.2.7).

Note 2 to entry: Risk analysis includes risk estimation.

[SOURCE: ISO Guide 73:2009, 3.6.1]

3.2.6
risk evaluation
process of comparing the results of *risk analysis* (3.2.5) with *risk criteria* (3.1.7) to determine whether the *risk* (3.1.3) and/or its significance is acceptable or tolerable

Note 1 to entry: Risk evaluation assists in the decision about *risk treatment* (3.2.7).

[SOURCE: ISO Guide 73:2009, 3.7.1, modified — "significance" has replaced "magnitude".]

3.2.7
risk treatment
process to modify *risk* (3.1.3)

Note 1 to entry: Risk treatment can involve:

— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

— taking or increasing risk in order to pursue an opportunity;

— removing the *risk source* (3.1.6);

— changing the *likelihood* (3.1.13);

— changing the *consequences* (3.1.14);

— sharing the risk with another party or parties (including contracts and risk financing); and

— retaining the risk by informed decision.

Note 2 to entry: Information security risk treatment does not include "taking or increasing risk in order to pursue an opportunity" but the organization can have this option for general risk management.

Note 3 to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

Note 4 to entry: Risk treatment can create new risks or modify existing risks.

[SOURCE: ISO Guide 73:2009, 3.8.1, modified — Note 1 to entry has been added and the original Note 1 and 2 to entry have been renumbered as Note 2 and 3 to entry.]

3.2.8
risk acceptance
informed decision to take a particular *risk* (3.1.3)

Note 1 to entry: Risk acceptance can occur without *risk treatment* (3.2.7) or during the process of risk treatment.

Note 2 to entry: Accepted risks are subject to monitoring and review.

[SOURCE: ISO Guide 73:2009, 3.7.1.6]

3.2.9
risk sharing
form of *risk treatment* (3.2.7) involving the agreed distribution of *risk* (3.1.3) with other parties

Note 1 to entry: Legal or regulatory requirements can limit, prohibit or mandate risk sharing.

Note 2 to entry: Risk sharing can be carried out through insurance or other forms of contract.

Note 3 to entry: The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.

Note 4 to entry: Risk transfer is a form of risk sharing.

[SOURCE: ISO Guide 73:2009, 3.8.1.3]

3.2.10
risk retention
temporary acceptance of the potential benefit of gain, or burden of loss, from a particular *risk* (3.1.3)

Note 1 to entry: Retention can be restricted to a certain period of time.

Note 2 to entry: The *level of risk* (3.1.15) retained can depend on *risk criteria* (3.1.7).

[SOURCE: ISO Guide 73:2009, 3.8.1.5, modified — the word “temporary” has been added at the start of the definition and the phrase; “Risk retention includes the acceptance of residual risks” has replaced “Retention can be restricted to a certain period of time “ in Note 1 to entry.]

4 Structure of this document

This document is structured as follows:

— Clause 5: Information security risk management;

— Clause 6: Context establishment;

— Clause 7: Information security risk assessment process;

— Clause 8: Information security risk treatment process;

— Clause 9: Operation;

— Clause 10: Leveraging related ISMS processes.

Except for the descriptions given in general subclauses, all risk management activities as presented from Clause 7 to Clause 10 are structured as follows:

Input: Identifies any required information to perform the activity.

Action: Describes the activity.

Trigger: Provides guidance on when to start the activity, for example because of a change within the organization or according to a plan or a change in the external context of the organization.

Output: Identifies any information derived after performing the activity, as well as any criteria that such output should satisfy.

Guidance: Provides guidance on performing the activity, keyword and key concept.

5 Information security risk management

5.1 Information security risk management process

The information security risk management process is presented in Figure 1.

NOTE This process is based on the general risk management process defined in ISO 31000.

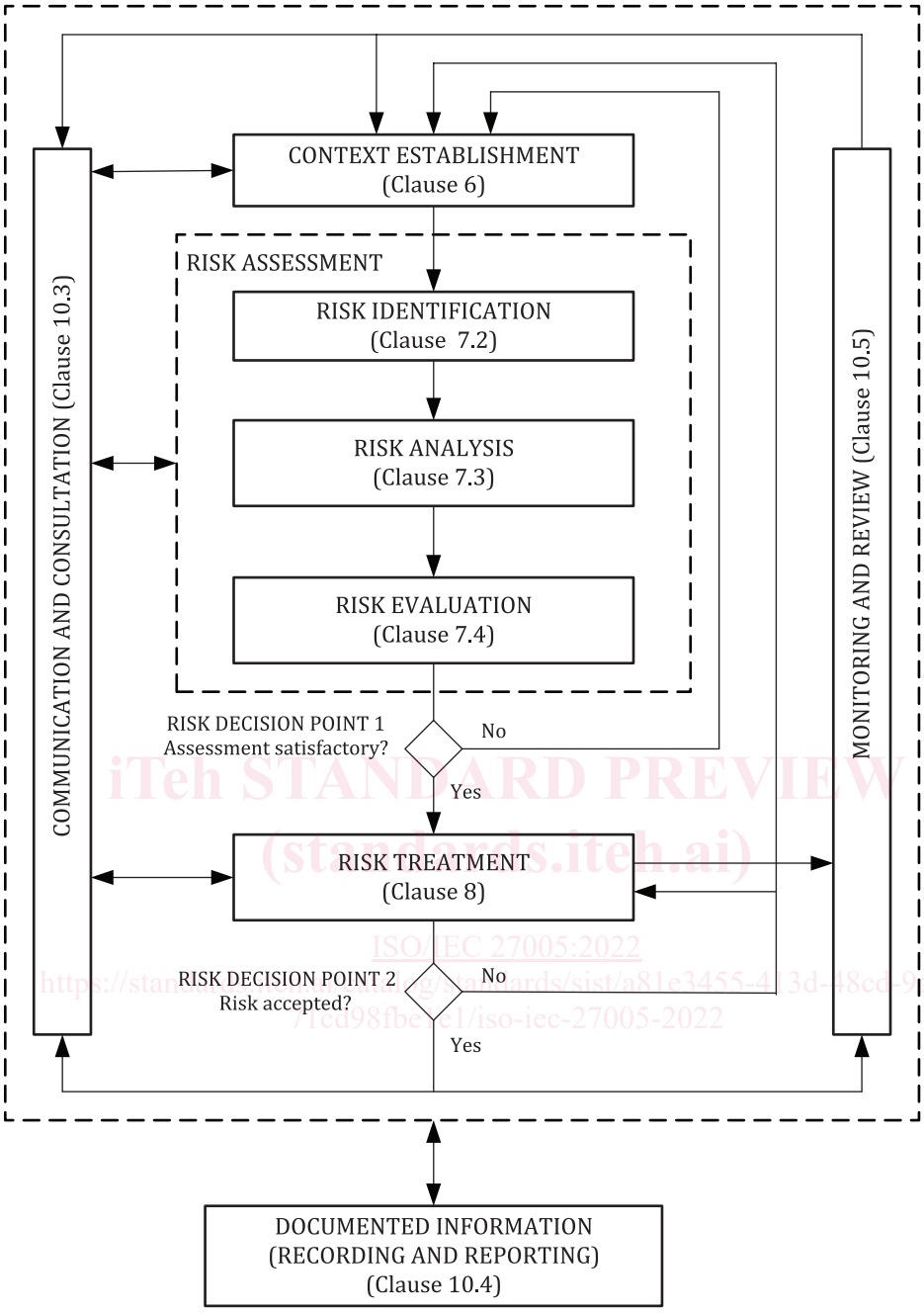

Figure 1 — Information security risk management process

As Figure 1 illustrates, the information security risk management process can be iterative for risk assessment and/or risk treatment activities. An iterative approach to conducting risk assessment can increase depth and detail of the assessment at each iteration. The iterative approach provides a good balance between minimizing the time and effort spent in identifying controls, while still ensuring that risks are appropriately assessed.

Context establishment means assembling the internal and external context for information security risk management or an information security risk assessment.

If the risk assessment provides sufficient information to effectively determine the actions required to modify the risks to an acceptable level, then the task is complete and the risk treatment follows. If the information is insufficient, another iteration of the risk assessment should be performed. This can involve a change of context of the risk assessment (e.g. revised scope), involvement of expertise in

the relevant field, or other ways to collect the information required to enable risk modification to an acceptable level (see "risk decision point 1" in Figure 1).

Risk treatment involves an iterative process of:

— formulating and selecting risk treatment options;

— planning and implementing risk treatment;

— assessing the effectiveness of that treatment;

— deciding whether the remaining risk is acceptable;

— taking further treatment if not acceptable.

It is possible that the risk treatment does not immediately lead to an acceptable level of residual risks. In this situation, another attempt to find further risk treatment can be performed, or there can be another iteration of the risk assessment, either as a whole or in parts. This can involve a change of context of the risk assessment (e.g. by a revised scope) and involvement of expertise in the relevant field. Knowledge about relevant threats or vulnerabilities can lead to better decisions about suitable risk treatment activities in the next iteration of the risk assessment (see "risk decision point 2" in Figure 1).

Context establishment is discussed in detail in Clause 6, risk assessment activities in Clause 7 and risk treatment activities in Clause 8.

Other activities necessary for managing information security risks are discussed in Clause 10.

5.2 Information security risk management cycles

The risk assessment and the risk treatment should be updated on a regular basis and based on changes. This should apply to, the entire risk assessment and the updates can be divided into two risk management cycles:

— strategic cycle, where business assets, risk sources and threats, target objectives or consequences to information security events are evolving from changes in the overall context of the organization. This can result as inputs for an overall update of the risk assessment or risk assessments and the risk treatments. It can also serve as an input for identifying new risks and initiate completely new risk assessments;

— operational cycle, where the above-mentioned elements serves as input information or changed criteria that will affect a risk assessment or assessment where the scenarios should be reviewed and updated. The review should include updating of the corresponding risk treatment as applicable.

The strategic cycle should be conducted at longer time basis or when major changes occur while the operational cycle should be shorter depending on the detailed risks that are identified and assessed as well as the related risk treatment.

The strategic cycle applies to the environment in which the organization seeks to achieve its objectives, while the operational cycle applies to all risk assessments considering the context of the risk management process. In both cycles, there can be many risk assessments with different contexts and scope in each assessment.

6 Context establishment

6.1 Organizational considerations

NOTE This subclause relates to ISO/IEC 27001:2022, 4.1.

An organization is defined as person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives. An organization is not necessarily a company,