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)

COPYRIGHT PROTECTED DOCUMENT

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.

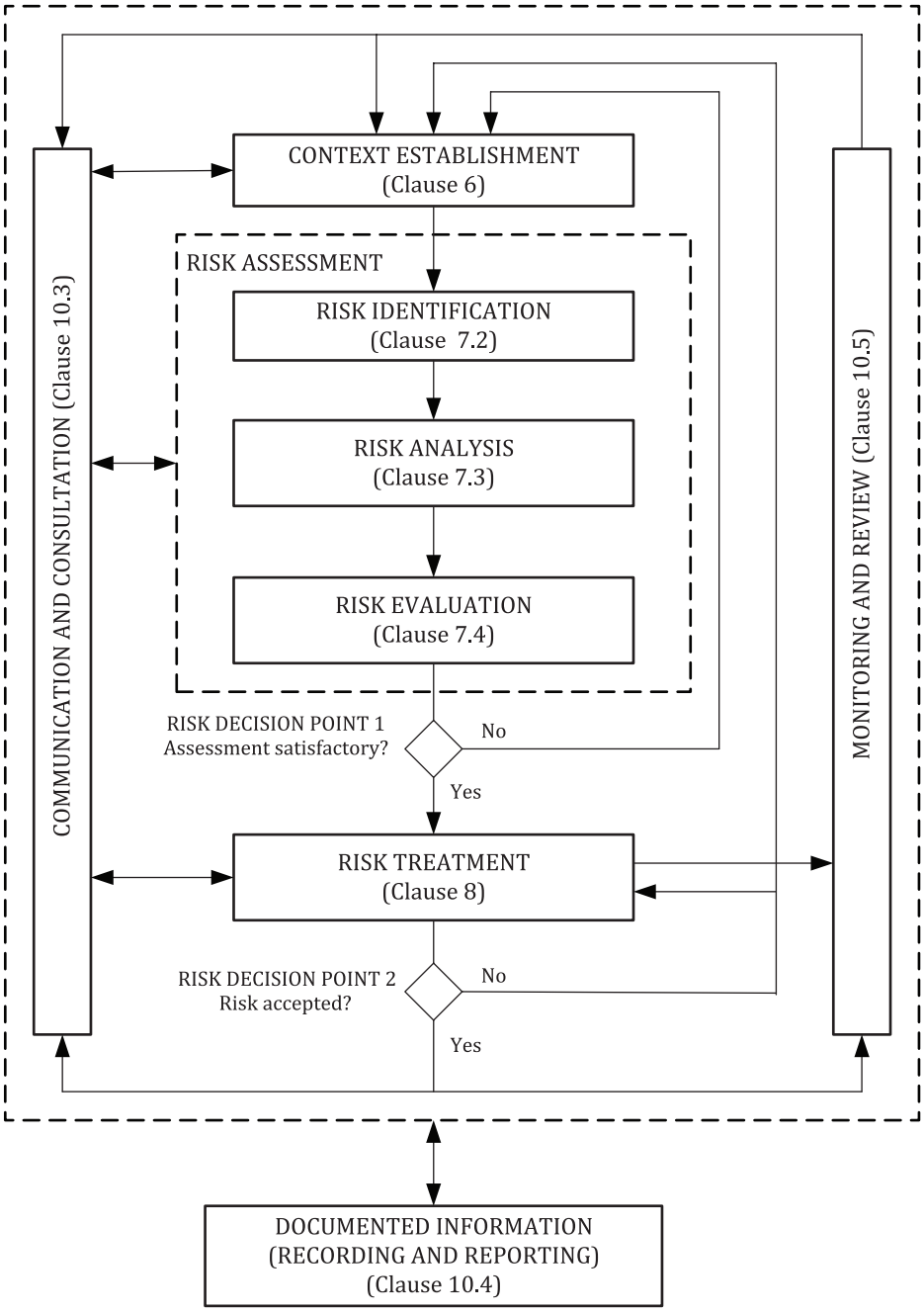


Figure 1 — Information security risk management process

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,

other corporate body or legal entity, it can also be a subset of a legal entity (e.g. the IT department of a company), and can be considered as the "organization" within the context of ISMS.

It is important to understand that risk appetite, defined as the amount of risk an organization is willing to pursue or accept, can vary considerably from organization to organization. For instance, factors affecting an organization's risk appetite include size, complexity and sector. Risk appetite should be set and regularly reviewed by top management.

The organization should ensure that the role of the risk owner is determined in terms of the management activities regarding the identified risks. Risk owners should have appropriate accountability and authority for managing identified risks.

6.2 Identifying basic requirements of interested parties

NOTE This subclause relates to ISO/IEC 27001:2022, 4.2.

The basic requirements of relevant interested parties should be identified, as well as the status of compliance with these requirements. This includes identifying all the reference documents that define security rules and controls and that apply within the scope of the information security risk assessment.

These reference documents can include, but are not limited to:

a) ISO/IEC 27001:2022, Annex A;

b) additional standards that cover ISMS;

c) additional standards applicable to a specific sector (e.g. financial, healthcare);

d) specific international and/or national regulations;

e) the organization's internal security rules;

f) security rules and controls from contracts or agreements;

g) security controls implemented based on previous risk treatment activities.

Any non-compliance with the basic requirements should be explained and justified. These basic requirements and their compliance should be the input for the likelihood assessment and for the risk treatment.

6.3 Applying risk assessment

NOTE This subclause relates to ISO/IEC 27001:2022, 4.3.

Organizations can perform risk assessments embedded within many different processes, such as project management, vulnerability management, incident management, problem management, or even on an impromptu basis for a given identified specific topic. Regardless of how risk assessments are performed, they should collectively cover all the issues relevant to the organization within the scope of an ISMS.

The risk assessment should help the organization make decisions about the management of the risks that affect the achievement of its objectives. This should therefore be targeted at those risks and controls that, if managed successfully, will improve the likelihood of the organization achieving its objectives.

More information about the context of an ISMS and the issues to be understood through risk assessment is given in ISO/IEC 27003.

6.4 Establishing and maintaining information security risk criteria

6.4.1 General

ISO/IEC 27001:2022, 6.1.2 a), specifies requirements for organizations to define their risk criteria, i.e. the terms of reference by which they evaluate the significance of the risks that they identify and make decisions concerning risks.

ISO/IEC 27001 specifies requirements for an organization to establish and maintain information security risk criteria that include:

a) the risk acceptance criteria;

b) criteria for performing information security risk assessments.

In general, to set risk criteria, the following should be considered:

— the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible);

— how consequence and likelihood will be defined, predicted and measured;

— time-related factors;

— consistency in the use of measurements;

— how the level of risk will be determined;

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

— the organization's capacity.

Further considerations on risk criteria are presented in Annex A.

6.4.2 Risk acceptance criteria

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 a) 1).

In risk evaluation, risk acceptance criteria should be used to determine whether a risk is acceptable or not.

In risk treatment, risk acceptance criteria can be used to determine whether the proposed risk treatment is sufficient to reach an acceptable level of risk, or if further risk treatment is needed.

An organization should define levels of risk acceptance. The following should be considered during development:

a) consistency between the information security risk acceptance criteria and the organization's general risk acceptance criteria;

b) the level of management with delegated authority to make risk acceptance decisions is identified;

c) risk acceptance criteria can include multiple thresholds, and authority for acceptance can be assigned to different levels of management;

d) risk acceptance criteria can be based on likelihood and consequence alone, or can be extended to also consider the cost/benefit balance between prospective losses and the cost of controls;

e) different risk acceptance criteria can apply to different classes of risk (e.g. risks that can result in non-compliance with regulations or laws are not always retained, while acceptance of risks can be allowed if the acceptance is a result of a contractual requirement);

f) risk acceptance criteria can include requirements for future additional treatment (e.g. a risk can be retained on a short-term basis even when the level of risk exceeds the risk acceptance criteria if there is approval and commitment to take action to implement a chosen set of controls to reach an acceptable level within a defined time period);

g) risk acceptance criteria should be defined based upon the risk appetite that indicates amount and type of risk that the organization is willing to pursue or retain;

h) risk acceptance criteria can be absolute or conditional depending on the context.

Risk acceptance criteria should be established considering the following influencing factors:

— organizational objectives;

— organizational opportunities;

— legal and regulatory aspects;

— operational activities;

— technological constraints;

— financial constraints;

— processes;

— supplier relationships;

— human factors (e.g. related to privacy).

The list of influencing factors is not exhaustive. The organization should consider the influencing factors based on the context.

A simple acceptance criterion (yes/no) does not always suffice in practice.

In many cases, the decision to accept risk can be made at specific levels of risk (specific combinations of likelihood and consequence). However, there can be circumstances where it is necessary to set thresholds of acceptance for extreme consequences regardless of their likelihood, or extremely high likelihoods regardless of consequences, where the effect on the organization primarily results from one or the other.

For example, acceptance of a rare event that wipes out the stock value of a company, or a constant drain on resources resulting from the need to control frequent minor infractions of a policy, should be considered primarily based on which of the two factors have the dominant effect on the organization.

Consequently, risk acceptance criteria should ideally include consideration of likelihood and consequence independently, as well as costs of management, rather than merely level of risk as a combination of likelihood and consequence.

An organization with a keen risk appetite can set a higher threshold of acceptance, thereby accepting more risks than an organization with a lower risk appetite. This protects the organization from over-control, i.e. having so many information security controls that they prevent the ability of the organization to achieve its objectives.

Risk acceptance criteria can differ depending on how long the risks are expected to exist (e.g. the risks can be associated with a temporary or short-term activity).

The risk criteria should be kept under review and updated as necessary as a result of any changes in the context of information security risk management.

EXAMPLE A small company can initially have a keen risk appetite but as it grows, it can lower its risk appetite.

The risk acceptance criteria should be approved by the authorized management level.

6.4.3 Criteria for performing information security risk assessments

6.4.3.1 General

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 a) 2).

Risk assessment criteria specify how the significance of a risk is determined in terms of its consequences, likelihood and level of risk.

Information security risk assessment criteria should take into account the appropriateness of risk management activities.

Considerations for achieving this include:

a) the classification level of information;

b) the quantity, and any concentration of information;

c) the strategic value of the business processes that make use of the information;

d) the criticality of the information and assets related to information involved;

e) operational and business importance of availability, confidentiality and integrity;

f) the expectations and perceptions of interested parties (e.g. top management);

g) negative consequences such as loss of goodwill and reputation;

h) consistency with the organizational risk criteria.

Risk assessment criteria, or a formal basis for defining them, should be standardized across the organization for all types of risk assessment, as this can facilitate the communication, comparison and aggregation of risks associated with multiple business domains.

Information security risk assessment criteria typically include:

— consequences;

— likelihood;

— level of risk.

6.4.3.2 Consequence criteria

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 a) 2).

ISO/IEC 27001 is concerned with the consequences which are directly or indirectly affected by the preservation or loss of confidentiality, integrity and availability of information in the scope of the ISMS. Consequence criteria should be developed and specified in terms of the extent of damage or loss, or harm to an organization or individual resulting from the loss of confidentiality, integrity and availability of information. When defining consequence criteria, the following should especially be considered:

a) loss of life or harm to individuals or groups;

b) loss of freedom, dignity or right to privacy;

c) loss of staff and intellectual capital (skills and expertise);

d) impaired internal or third-party operations (e.g. damage to a business function or process);

e) effects to plans and deadlines;

f) loss of business and financial value;

g) loss of business advantage or market share;

h) damage to public trust or reputation;

i) breaches of legal, regulatory or statutory requirements;

j) breaches of contracts or service levels;

k) adverse impact on interested parties;

l) negative impact on the environment, pollution.

Consequence criteria define how an organization categorizes the significance of potential information security events to the organization. It is essential to determine how many categories of consequences are used, how they are defined, and what consequences are associated with each category. Usually, consequence criteria are different for different organizations depending on the organization's internal and external context.

EXAMPLE 1 The maximum amount the organization is prepared to write off in a fiscal year and the minimum amount in the same period that would force it into liquidation can create realistic upper and lower limits of an organization's consequence scale expressed in monetary terms.

This context-dependent range can then be divided into several consequence categories, the number and distribution of which should depend on the risk perception and appetite of the organization. Monetary consequence scales are commonly expressed in a logarithmic scale such as in decades or powers of 10 (e.g. 100 to 1 000; 1 to 10 000, etc.), but alternative quantization schemes can be used where they fit the organization's context better.

Because consequences in different domains or departments of an organization can initially be expressed in various ways rather than strictly in monetary terms, it is useful if these various expressions can be cross-referenced to a common anchoring scale to ensure approximately equivalent levels of consequence in the different domains are correctly compared with each other. This should enable an aggregation of risks across domains to be performed.

EXAMPLE 2 A data breach, as well as possibly impacting individual privacy, can result in the loss of confidentiality, integrity or availability of information in the scope of the ISMS. This can also lead to non-compliance with applicable data protection legislation. Potential consequences range from information loss, loss of information-related assets and information process, to loss of operational business goals and projected business.

6.4.3.3 Likelihood criteria

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 a) 2).

Determining likelihood criteria depends on aspects such as:

a) accidental or natural events;

b) the degree of exposure of relevant information or the asset related to information to the threat;

c) the degree to which vulnerability of the organization is exploited;

d) technology failure;

e) human acts or omissions.

Likelihood can be expressed in probabilistic terms (the chance that an event will occur in a given time frame) or in frequentist terms (the notional average number of occurrences in a given time frame). The likelihood expressed in terms related to frequency is often used when it is communicated, although only the likelihood expressed in probabilistic terms can be used when aggregation of likelihoods is performed.

Likelihood criteria should cover the predictably manageable range of anticipated event likelihoods. Beyond the limits of practicable manageability, it is typically only necessary to recognize that one or another limit has been exceeded in order to make an adequate risk management decision (designation as an extreme case). If finite scales are too wide, this typically results in excessively coarse quantization and can lead to error in assessment. This is particularly the case where likelihoods fall into the high end of exponentially represented scales, as the increments in the upper ranges are intrinsically very wide.

Although almost anything is "possible", the risk sources that should be given primary attention are those with likelihoods most relevant to the organization's context and the scope of its ISMS.

6.4.3.4 Criteria for determining the level of risk

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 a) 2).

The purpose of scales for level of risk is to help risk owners to decide about retaining or otherwise treating risks and to prioritize them for risk treatment. The assessed level of a particular risk should help the organization to determine the urgency for addressing that risk.

Depending on the situation, it is recommended to consider the inherent level of risk (without considering any controls), or the current level of risk (allowing for the effectiveness of any controls already implemented). The organization should develop a risk ranking, taking into account the following:

a) the consequence criteria and likelihood criteria;

b) the consequences that information security events can have on strategic, tactical and operational levels (this can be defined as worst case or in other terms provided the same basis is used consistently);

c) legal and regulatory requirements, and contractual obligations;

d) risks that appear beyond the boundaries of the organization's scope, including unforeseen effects on third parties.

Criteria for level of risk are necessary in order to evaluate analysed risks.

Criteria for level of risk can be qualitative (e.g. very high, high, medium, low) or quantitative (e.g. expressed in terms of expected value of monetary loss, loss of lives or market share over a given period of time).

EXAMPLE Risks can be quantified as annual loss expectancy, i.e. the average monetary value of the consequence per year taken over the next year.

Whether quantitative or qualitative criteria are used, evaluation scales should ultimately be anchored to a reference scale that is understood by all interested parties, and both risk analysis and risk evaluation should include at least periodic formal calibration against the reference scale to ensure validity, consistency and comparability of results.

If a qualitative approach is used, the levels of any qualitative scale should be unambiguous, its increments should be clearly defined, the qualitative descriptions for each level should be expressed in objective language and the levels should not overlap. When different scales are used (e.g. to address risks in different business domains), there should be an equivalency to allow comparable results.

6.5 Choosing an appropriate method

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 b).

In general, the information security risk management approach and methods should be aligned with the approach and methods used to manage the other risks of the organization.

The chosen approach should be documented.

According to ISO/IEC 27001:2022, 6.1.2 b), the organization in the scope of the ISMS is required to ensure that repeated information security risk assessments produce consistent, valid and comparable results. It means the chosen method should ensure the following properties of results:

— consistency: assessments of the same risks performed by different persons, or by the same persons on different occasions, in the same context, should produce similar results;

— comparability: risk assessment criteria should be defined to ensure that assessments performed for different risks produce comparable results when representing equivalent levels of risk;

— validity: assessments should produce the results that accord as closely as possible with reality.

Operational risk management methods are typically used for information security risk management. The method chosen can use any appropriate approach with respect to the use of residual risk. The most commonly used approaches for information security risk management use current risk when assessing the likelihood and consequence of risks.

7 Information security risk assessment process

7.1 General

The organization should use the organizational risk assessment process (if established) to assess risks to information or to define an information security risk assessment process.

Risk assessment enables risk owners to prioritize risks aligned with the treatment perspective, based primarily on their consequences and likelihood or other established criteria.

The context of the risk assessment should be determined including a description of scope and purpose as well as internal and external issues that affect the risk assessment.

Risk assessment consists of the following activities:

a) risk identification, which is a process to find, recognize and describe risks (further details on risk identification are provided in 7.2);

b) risk analysis, which is a process to comprehend the types of risk and to determine the level of risk. Risk analysis involves consideration of the causes and sources of risk, the likelihood that a specific event occurs, the likelihood that this event has consequences and the severity of those consequences (further details on risk analysis are provided in 7.3);

c) risk evaluation, which is a process to compare the results of risk analysis with risk criteria to determine whether the risk and/or its significance is acceptable and to prioritize the analysed risks for risk treatment. Based on this comparison, the need for treatment can be considered (further details on risk evaluation are provided in 7.4).

The risk assessment process should be based on methods (see 6.5) and tools designed in sufficient detail to ensure, as far as is possible, consistent, valid and reproducible results. Furthermore, the outcome should be comparable, e.g. to determine whether the level of risk increased or decreased.

The organization should ensure that its information security risk management approach aligns with the organizational risk management approach, so that any information security risks can be compared with other organizational risks and not only considered in isolation.

ISO/IEC 27001 does not mandate a particular approach to be used to fulfil the requirements in ISO/IEC 27001:2022, 6.1.2. Nevertheless, there are two main approaches for assessment: an event-based approach and an asset-based approach. They are discussed in more detail in 7.2.1.

7.2 Identifying information security risks

7.2.1 Identifying and describing information security risks

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 c) 1).

Input: Events that can negatively influence the achievement of information security objectives in the organization or in other organizations.

Action: Risks associated with the loss of confidentiality, integrity and availability of information should be identified.

Trigger: Risk owners, interested parties and/or experts detect, or have a need to search for, new or changed events or situations that can affect the achievement of the information security objectives.

Output: A list of identified risks.

Implementation guidance:

Risk identification is the process of finding, recognizing and describing risks. This involves the identification of risk sources and events.

The aim of risk identification is to generate a list of risks based on those events that can prevent, affect or delay the achievement of information security objectives.

The risks identified should be those that, if they materialize, can have an effect on the achievement of the objectives.

ISO/IEC 27001:2022, 6.1.2 c), requires the organization to define and apply an information security risk assessment process that identifies the information security risks. There are two approaches commonly used to perform risk identification.

a) Event-based approach: identify strategic scenarios through a consideration of risk sources, and how they use or impact interested parties to reach those risk's desired objective.

b) Asset-based approach: identify operational scenarios, which are detailed in terms of assets, threats and vulnerabilities.

In an event-based approach, the underlying concept is that risks can be identified and assessed through an evaluation of events and consequences. Events and consequences can often be determined by a discovery of the concerns of top management, risk owners and the requirements identified in determining the context of the organization (ISO/IEC 27001:2022, Clause 4). Interviews with top management and those people in the organization who have a responsibility for a business process can assist in identifying not only the relevant events and consequences, but also the risk owners.

An event-based approach can establish high level or strategic scenarios without spending a considerable amount of time in identification of assets on a detailed level. This allows the organization to focus its risk treatment efforts on the critical risks. Evaluation of events using this approach can make use of historical data where risks remain unchanging for long periods, and allows the interested parties involved to reach their objectives. However, in the case of risks for which historical data are not available or reliable, the advice based on knowledge and experience of experts or investigation of risk sources can assist evaluation.

With an asset-based approach, the underlying concept is that risks can be identified and assessed through an inspection of assets, threats and vulnerabilities. An asset is anything that has value to the organization and therefore requires protection. Assets should be identified, taking into account that an information system consists of activities, processes and information to be protected. The assets can be identified as the primary and the supporting assets according to their type and priority, highlighting their dependencies, as well as their interactions with their risk sources and the organization's interested parties. A threat exploits a vulnerability of an asset to compromise the confidentially, integrity and/or availability of corresponding information. If all valid combinations of assets, threats and vulnerabilities

can be enumerated within the scope of the ISMS, then, in theory, all the risks would be identified. For further steps of risk assessment, a list of assets associated with information and information-processing facilities should be drawn up.

The asset-based approach can identify asset-specific threats and vulnerabilities and allows the organization to determine specific risk treatment on a detailed level.

More information on both approaches is given in Annex A.

In principle, the two approaches differ only in regard to the level at which identification is initiated. Both approaches can describe the same risk scenario, e.g. where an information asset is at the detail level and a business exposure is at the general level. Identifying the contributory risk sources using an event-based assessment typically requires drilling down from the general level of the scenario to the detail level, but an asset-based assessment typically searches upwards from the asset to the scenario, in order to provide visibility regarding how consequences accumulate.

Risk identification is critical, because an information security risk that is not identified at this stage is not included in further analysis.

Risk identification should consider risks regardless of whether their source is under the control of the organization, even if no specific risk sources are evident. Particularly when assessing complex risk scenarios, iterative risk assessment should be conducted. The first round should concentrate on high-level observations and successive rounds should address additional levels of detail until root causes of risks can be identified.

Any other risk identification approach can be used as long as it ensures the production of consistent, valid and comparable results, fulfilling the requirement of ISO/IEC 27001:2022, 6.1.2 b).

Management of information security risks should not be constrained by arbitrary or restrictive views of how risks should be structured, grouped, aggregated, split or described. Risks can appear to overlap or be subsets or specific instances of other risks. However, controls for individual risks should be considered and identified separately from wider risks or aggregated risks for the purposes of risk treatment.

EXAMPLE 1 An example of two overlapping risks: (1) there is a risk of a fire in the head office; (2) there is a risk of a fire affecting the operation of the accounts department where the accounts department is in head office but also in several other buildings.

An example of specific instances of a risk: (1) there is a data loss incident; (2) there is a data loss incident of personal data.

The second risk is a specific instance of the first risk, but it is likely to have different attributes and controls to the first risk, and it can be important to manage it separately from the much wider first risk.

Aggregation of risks should not be undertaken unless they are relevant to each other at the level at which the organization's context is being considered. It can be necessary to consider separately risks which are merged for the purpose of overall risk management budgeting, when planning treatment options, as different controls can be needed to manage them.

EXAMPLE 2 A data centre can be subject to several independent hazards: flooding, fire, electric power spikes and vandalism.

To estimate the overall level of corporate risk, the individual risks of these events can be combined into an overall level of risk, but as each of these events require different controls to manage the risk, they should be considered and identified separately for the purposes of risk treatment. Risks (combinations of likelihoods and consequences) cannot always be aggregated directly.

7.2.2 Identifying risk owners

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 c) 2).

Input: List of identified risks.

Action: Risks should be associated to risk owners.

Trigger: Identification of risk owners becomes necessary when:

— it has not been done before;

— there is a change in personnel in the relevant business area where the risks reside;

Output: List of risk owners with associated risks.

Implementation guidance:

Top management, the security committee, process owners, functional owners, department managers and asset owners can be the risk owners.

An organization should use the organizational risk assessment process (if established) regarding identifying risk owners, otherwise it should define criteria for identifying risk owners. Such criteria should take into consideration that risk owners:

— are accountable and have the authority for managing the risks they own, i.e. they should have a position in the organization that allows them to actually exercise this authority;

— understand the issues at hand, and are in a position to make informed decisions (e.g. regarding how to treat the risks).

The level of risk and to what asset the risk should apply can serve as the basis for identifying risk owners.

The allocation should take place as part of the risk assessment process.

7.3 Analysing information security risks

7.3.1 General

Risk analysis has the objective to determine the level of the risk.

ISO 31000 is referenced in ISO/IEC 27001 as a general model. ISO/IEC 27001:2022, 6.1.2, requires that for each identified risk, the risk analysis is based on assessing the consequences resulting from the risk and assessing the likelihood of the risk to determine a level of risk.

Techniques for risk analysis based on consequences and likelihood can be:

a) qualitative, using a scale of qualifying attributes (e.g. high, medium, low); or

b) quantitative, using a scale with numerical values (e.g. monetary cost, frequency or probability of occurrence); or

c) semiquantitative, using qualitative scales with assigned values.

Risk analysis should be targeted at those risks and controls that, if managed successfully, improve the likelihood of the organization achieving its objectives. It is easy to spend significant time on a risk assessment, notably the assessment of likelihoods and consequences. To enable efficient decision-making on the management of risks, it can be sufficient to use initial, and rough estimates of likelihood and consequence.

7.3.2 Assessing potential consequences

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 d) 1).

Input: A list of identified relevant event or risk scenarios, including identification of risk sources, and business processes, business objectives and consequence criteria. Furthermore, lists of all existing controls, their effectiveness, implementation and usage status.

Action: The consequences resulting from the failure to adequately preserve confidentiality, integrity or availability of information should be identified and assessed.

Trigger: Assessment of the consequences becomes necessary when:

— it has not been done before;

— the list produced by "risk identification" is changed;

— risk owners or interested parties have changed the units in which they want consequences to be specified; or

— changes in the scope or context are determined that affect consequences.

Output: A list of potential consequences related to risk scenarios with their consequences related to assets or events, depending on the approach applied.

Implementation guidance:

Failure to adequately preserve the security of information can lead to loss of its confidentiality, integrity or availability. Loss of confidentiality, integrity or availability can have further consequences for the organization and its objectives. Consequence analysis can be performed bottom up from the information security consequences by considering what can happen if there is a loss of confidentiality, integrity or availability of the information in question. Typically, the risk owner can estimate the consequence if the event occurs. The following elements should be taken into consideration:

— estimation (or measure based on experience) of the losses (time or data) due to the event as result of interrupting or disturbing operations;

— estimation/perception of severity of the consequence (e.g. expressed in money);

— recovery costs depending on whether recovery can be done internally (by the risk owner team), or there is a need to call an external entity.

7.3.3 Assessing likelihood

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 d) 2).

Input: A list of identified relevant event or risk scenarios, including identification of risk sources, and business processes, business objectives and likelihood criteria. Additionally, lists of all existing controls, their effectiveness, implementation and usage status.

Action: The likelihood of occurrence of possible or actual scenarios should be assessed and expressed using established likelihood criteria.

Trigger: Along with consequence, assessing the likelihood is a key activity of the risk assessment process when determining the level of risk.

Assessment of the likelihood becomes necessary when:

— it has not been done before;

— changes in the scope or context are determined that can affect likelihood;

— vulnerabilities are discovered in implemented controls;

— control effectiveness tests/audits result in unexpected outcomes;

— changes are discovered in the threat environment (e.g. new threat actors/sources).

Output: A list of events or risk scenarios complemented by likelihoods that these occur.

Implementation guidance:

After identifying the risk scenarios, it is necessary to analyse the likelihood of each scenario and consequence occurring, using qualitative or quantitative analysis techniques. Assessing the likelihood is not always easy and should be expressed in different ways. This should take into account how often the risk sources occur or how easily some of them (e.g. vulnerabilities) can be exploited, considering:

— experience and applicable statistics for risk source likelihood;

— for deliberate risk sources: the degree of motivation [e.g. the viability (cost/benefit) of the attack] and capabilities (e.g. the level of the skill of possible attackers), which change over time, resources available to possible attackers, and influences on possible attackers such as serious crime, terrorist organizations or foreign intelligence, as well as the perception of attractiveness and vulnerability of information for a possible attacker;

— for accidental risk sources: geographical factors (e.g. proximity to dangerous facilities or activities), the possibility of natural disasters such as extreme weather, volcanic activity, earthquakes, flooding, tsunami and factors that can influence human errors and equipment malfunction;

— known weaknesses and any compensating controls, both individually and in aggregation;

— existing controls and how effectively they reduce known weaknesses.

Estimation of likelihood is intrinsically uncertain, not only because it considers things that have not yet happened and are therefore not fully known, but also because likelihood is a statistical measure and is not directly representative of individual events. The three basic sources of assessment uncertainty are:

— personal uncertainty originating in the judgement of the assessor, which derives from variability in the mental heuristics of decision making;

— methodological uncertainty, which derives from the use of tools that inevitably model events simplistically;

— systemic uncertainty about the anticipated event itself, which derives from insufficient knowledge (in particular, if evidence is limited or a risk source changes with time).

To increase the reliability of estimating likelihood, organizations should consider using:

a) team assessments rather than individual assessments;

b) external sources, such as information security breach reports;

c) scales with range and resolution appropriate to the organization's approach;

d) unambiguous categories, such as “once a year”, rather than “infrequent”.

When assessing the likelihood of events, it is important to recognize the difference between independent and dependent events. The likelihood of events that depend on each other is conditioned by the relationship between them (e.g. a second event can be inevitable if a first event occurs) so that separate assessment of both their likelihoods is not necessary. The likelihood of relevant independent events are all essential contributors to the likelihood of a consequence to which they contribute.

EXAMPLE The likelihood of a Denial-of-Service attack on a server depends on the current threat landscape and the vulnerability and accessibility of the server. However, the likelihood of malicious packets can be 100 % once the attack has started and its assessment does not help the assessment of the likelihood of the Denial-of-Service attack.

To avoid unnecessary complexity of assessment, it is important to identify any dependencies between the events contributing to a risk scenario and in the first instance to assess the likelihoods of those events that are independent of each other.

The overall likelihood of business consequences of an information security event typically depends on the likelihood of potentially several lower-level contributory events and their consequences. Rather than attempting to estimate the likelihood of business consequences in a single high-level assessment,

it can be more valid to start by aggregating the likelihoods of the individually assessed lower-level events that contribute to it.

7.3.4 Determining the levels of risk

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 d) 3).

Input: A list of risk scenarios with their consequences related to assets or events and their likelihood (quantitative or qualitative).

Action: The level of risk should be determined as a combination of the assessed likelihood and the assessed consequences for all relevant risk scenarios.

Trigger: Determining levels of risk becomes necessary if the information security risks are to be evaluated.

Output: A list of risks with level values assigned.

Implementation guidance:

The level of risk can be determined in many possible ways. It is commonly determined as a combination of the assessed likelihood and the assessed consequences for all relevant risk scenarios. Alternative calculations can include an asset value as well as likelihood and consequence. In addition, the calculation is not necessarily linear, e.g. it can be likelihood squared combined with consequence. In any case the level of risk should be determined using the criteria established as described in 6.4.3.4.

7.4 Evaluating the information security risks

7.4.1 Comparing the results of risk analysis with the risk criteria

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 e) 1).

Input: A list of risk criteria and risks with level values assigned.

Action: Level of risks should be compared against risk evaluation criteria, particularly risk acceptance criteria.

Trigger: Comparing the results of risk analysis with the risk criteria becomes necessary if the information security risks are to be prioritized for treatment.

Output: A list of suggestions for decisions on additional actions regarding the management of risks.

Implementation guidance:

Once the risks have been identified and both likelihood and severity of consequence values assigned, organizations should apply their risk acceptance criteria to determine whether or not the risks can be accepted. If they cannot be accepted, then they should be prioritized for treatment.

To evaluate risks, organizations should compare the assessed risks with the risk criteria defined during the establishment of context.

Risk evaluation decisions should be based on the comparison of assessed risk with defined acceptance criteria, ideally taking into account the degree of confidence in the assessment. In some cases, such as the frequent occurrence of relatively low consequence events, it can be helpful to consider their cumulative effect over some timescale of interest, rather than the risk of each event considered individually, as this can provide a more realistic representation of overall risks.

There can be uncertainties in defining the boundary between those risks that require treatment and those that do not. Under certain circumstances, using a single level as the acceptable level of risk that divides risks that require treatment from those which do not is not always appropriate. In some cases,

it can be more effective to include an element of flexibility into the criteria by incorporating additional parameters such as cost and effectiveness of possible controls.

The levels of risk can be validated based on consensus among risk owners and business and technical specialists. It is important that risk owners have a good understanding of the risks they are accountable for that accords with the results of objective assessment. Consequently, any disparity between assessed levels of risk and those perceived by risk owners should be investigated to determine which better approximates to reality.

7.4.2 Prioritizing the analysed risks for risk treatment

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.2 e) 2).

Input: A list of the results of risks compared with risk criteria.

Action: The risks on the list should be prioritized for risk treatment, considering assessed levels of risks.

Trigger: Prioritizing the analysed risks for risk treatment becomes necessary if the information security risks are to be treated.

Output: A list of prioritized risks with risk scenarios that lead to those risks.

Implementation guidance:

Risk evaluation uses the understanding of risk obtained by risk analysis to make proposals for deciding about the next step to take. Those should refer to:

— whether a risk treatment is required;

— priorities for risk treatment considering assessed levels of risks.

Risk criteria used to prioritize risks should consider the objectives of the organization, contractual, legal and regulatory requirements and the views of relevant interested parties. Prioritization as taken in the risk evaluation activity are mainly based on the acceptance criteria.

8 Information security risk treatment process

8.1 General

The input of the information security risk treatment is based on the risk assessment process outcomes in the form of a prioritized set of risks to be treated, based on risk criteria.

The output of this process is a set of necessary information security controls [see ISO/IEC 27001:2022, 6.1.3 b)] that are to be deployed or enhanced in relation to one another, in accordance with the risk treatment plan [see ISO/IEC 27001:2022, 6.1.3 e)]. Deployed in this way, the effectiveness of the risk treatment plan is to modify the information security risk facing the organization so that it meets the organization's criteria for acceptance.

8.2 Selecting appropriate information security risk treatment options

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.3 a).

Input: A list of prioritized risks with event or risk scenarios that lead to those risks.

Action: Risk treatment options should be chosen.

Trigger: Selecting appropriate information security risk treatment options becomes necessary if no risk treatment plan is existing or the plan is incomplete.

Output: A list of prioritized risks with the selected risk treatment options.

Implementation guidance:

Several options for risk treatment include:

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

— risk modification, by changing the likelihood of the occurrence of an event or a consequence or changing the severity of the consequence;

— risk retention, by informed choice;

— risk sharing, by splitting responsibilities with other parties, either internally or externally (e.g. sharing the consequences via insurance);

EXAMPLE 1 An example of risk avoidance is an office location situated in a flood-zone, where there is the potential of a flood and resultant damages to the office and restrictions to the availability of and/or access to the office. The relevant physical controls can prove insufficient to reduce this risk, in which case, the treatment option of risk avoidance can be the best available option. This can involve closing or stopping operation of that office.

EXAMPLE 2 Another example of risk avoidance is choosing not to collect certain information from individuals so that it is not necessary for the organization to manage, store and transmit the information in its information systems.

In the case of risk sharing, at least one control is required to modify the likelihood or consequence, but the organization delegates the responsibility of implementing the control to another party.

Risk treatment options should be selected based on the outcome of the risk assessment, the expected costs for implementing these options and the expected benefits from these options, both individually and in the context of other controls. Risk treatment should be prioritized according to levels of risk as defined, time constraints and necessary sequence of implementations, and risk evaluation outcomes established in 7.4. While choosing the option, it can be considered how a particular risk is perceived by affected parties, and the most appropriate ways of communicating risk to these parties.

8.3 Determining all controls that are necessary to implement the information security risk treatment options

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.3 b).

Input: A list of prioritized risks with the selected risk treatment options.

Action: Determine all controls, from the chosen control sets as selected from an appropriate source, that are necessary for treating the risks based on the risk treatment options chosen, such as to modify, retain, avoid or share the risks.

Trigger: ISMS conformity; managing information security risks.

Output: All necessary controls.

Implementation guidance:

Special attention should be given to determine the necessary controls. Each control should be checked to determine if it is necessary by asking:

— what effect this control has on the likelihood or consequence of this risk;

— in which way the control maintains the risk level.

Only controls that have more than a negligible effect on the risk should be designated as “necessary”. One or more controls should be applied to every risk evaluated as requiring treatment.

There are many sources of control sets. They can be found in ISO/IEC 27001:2022, Annex A, in sector-specific codes of practice (e.g. ISO/IEC 27017) and other national, regional, industrial control sets. An organization can also determine one or more "custom" controls (see ISO/IEC 27003).

If a custom control is defined, the control wording should accurately and fairly describe what the control is and how it operates. As applicable and appropriate, this wording can usefully include such aspects as:

— is it a documented control;

— who owns the control;

— how it is monitored;

— how it can be evidenced;

— any exceptions;

— frequency of operation of the control;

— the tolerance for the control;

— if it is not obvious then the reason why the control exists.

If the control is outside the tolerance, the control is not operating effectively enough to manage the identified risk.

EXAMPLE 1 "A documented malware management process is in place, owned by the IT security manager. This excludes Macs and is monitored through the vendor console with reports on performance sent weekly to the CIO."

Such a detailed approach to control wording can be useful if the custom controls are also intended to support the organization in control assurance reporting. However, it is more important that the wording of controls should have meaning to people in the organization and help them make decisions about the management of those controls and associated risks.

The determination of controls can include new controls not yet implemented, or can include using controls that exist in the organization. However, a control that is already in operation should not automatically be included in the risk assessment because:

— the control is not necessary to manage one or more information security risks;

— it can be a control that does in some way help manage one or more information security risks but is not sufficiently effective to be included in the risk assessment or managed by the ISMS, or;

— it can be currently operating for reasons not related to information security (e.g. quality, efficiency, effectiveness or compliance), or;

— it is currently operating but from an information security perspective can be removed as it does not have enough effect to justify its continuing status as an essential control.

If a control is used for purposes other than solely the management of information security risks, care should be taken to ensure that the control is managed to achieve the information security objectives as well as the non-information security objectives.

EXAMPLE 2 Internal CCTV to control quality of the production process as well as for information security reasons (to protect from fraud).

When determining controls from an existing control set (e.g. ISO/IEC 27001:2022, Annex A, or a sector specific control list) the wording of the control should match what is necessary to manage the risk and accurately reflect what the control is or should be. If the overall approach is to use an existing control set (e.g. ISO/IEC 27001:2022, Annex A, or a sector specific control list) and the control set does not contain a control that accurately describes the necessary control, then consideration should be given to defining a custom control that accurately describes the control.

Controls can be classified as preventive, detective and corrective:

a) preventive control: a control that is intended to prevent the occurrence of an information security event that can lead to the occurrence of one or more consequences;

b) detective control: a control that is intended to detect the occurrence of an information security event;

c) corrective control: a control that is intended to limit the consequences of an information security event.

Control-type describes whether a control acts, or intends to act, to prevent or detect an event or react to its consequence(s).

EXAMPLE 3 An information security policy is a control that maintains risk, but policy compliance is intended to reduce the likelihood of the occurrence of risk and can be therefore categorized as being preventive.

The utility of categorizing controls as preventive, detective and corrective lies in their use, to ensure the construction of risk treatment plans are resilient to control failures. Provided there is an appropriate mix of preventive, detective and corrective controls:

— detective controls should mitigate risk if the preventive controls fail;

— corrective controls should mitigate risk if the detective controls fail;

— preventive controls should reduce the likelihood that the corrective controls should ever have to be used.

When utilizing controls, organizations should first decide if it is possible to detect the occurrence of an event. If that is the case, detective controls should be implemented. If it is not possible to detect an event, detective controls can be ineffective, with no way of telling whether a preventive control is working.

EXAMPLE 4 If it is not clear if a computer has become part of a "botnet", it cannot be known if the controls being used to prevent it becoming part of a botnet work as intended.

Detective controls can work as appropriate but they can still be ineffective.

EXAMPLE 5 Implementing Intrusion Detection/Prevention Systems can be an effective way to prevent malware traversing the network but they are of no use if there is no monitoring of the systems/alerts to action in the event there is an outbreak that is not contained.

In general, detective controls are ultimately ineffective in instances where they can be bypassed, or where their notification does not result in appropriate action. Corrective controls should be looked at next. If the detective controls fail, then there is likely to be one or more undesirable consequences. Implementation of the corrective controls can assist in the limitation of those consequences. Although corrective controls take effect after the onset of the consequence, it is often necessary to deploy them well in advance of the occurrence of any event.

EXAMPLE 6 Hard disk encryption does not prevent a laptop from being stolen or subsequent attempts to extract the data. It does, however, reduce the severity of the consequences linked to a disclosure. The control, of course, needs to be deployed before the laptop is stolen.

The categorization of controls is not absolute and depends on the context in which use of a control is described.

EXAMPLE 7 Backup does not prevent the occurrence of an event that would otherwise result in data loss (e.g. a disc head crash or loss of a laptop), but it does assist to reduce the consequence. Some organizations can therefore consider this to be a corrective control rather than a preventive control. Similarly, encryption does not prevent the loss of information, but if the event is described as "personal data revealed to attacker", then encryption is a preventive, rather than a corrective control.

The order in which the controls addressing the risks are organized depends on various factors. Many techniques can be used. It is the respective risk owners' responsibility to decide the balance between the costs of investing in controls and assuming consequences in case the risks are materialized.

The identification of existing controls can determine that these controls exceed current needs. A cost–benefit analysis should be undertaken before removing redundant or unnecessary controls (especially if the controls have high maintenance costs). Since controls can influence each other, removing redundant controls can reduce the overall security in place. Controls should not be included in the risk treatment unless they are necessary controls to manage one or more of the identified information security risks. A control should have an effect on the consequence or likelihood of the identified information security risks. Controls should not be included in the risk treatment if they are operating for reasons not related to information security.

Consideration should be given to controls that are implemented but known to have some weaknesses. If the assessment of all the risks that a control with weaknesses is managing are within the acceptance criteria, then it is not necessary to improve the control. Even though the control is not operating fully effectively, it is not always necessary to improve it to make it fully effective. It should not be assumed that all controls must operate at full effectiveness for the organization to manage its risks successfully. It is possible to specify that each individual control has a level of tolerance for failure below which the control can be regarded as not operating effectively enough to manage the identified risks. As long as the control is operating inside the tolerance, it does not need any improvement.

8.4 Comparing the controls determined with those in ISO/IEC 27001:2022, Annex A

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.3 c).

Input: All necessary controls (see 8.3).

Action: Compare all necessary controls with those listed in ISO/IEC 27001:2022, Annex A.

Trigger: Identification of any missing controls becomes necessary if risk treatment plans are formulated.

Output: All controls applicable to the risk treatment.

Implementation guidance:

ISO/IEC 27001:2022, 6.1.3 c), requires an organization to compare the controls that it has determined as being necessary to implement its chosen risk treatment options with the controls listed in ISO/IEC 27001:2022, Annex A. The purpose of this is to act as a safety check to verify that no necessary controls have been omitted from the risk assessment. This safety check is not in place to identify any omitted controls from ISO/IEC 27001:2022, Annex A, in the risk assessment. It is a safety check to identify any missing necessary controls from any source by comparing the controls with other standards and lists of controls. Omitted controls identified during this check can be sector specific or custom controls or from ISO/IEC 27001:2022, Annex A. The guidelines for determining controls in 8.3 should be followed when considering if any missing controls should be added to the risk assessment.

EXAMPLE It is important that a control that is already operating in the organization is not automatically added into the risk assessment without further consideration.

It is important to remember that this comparison of the controls is undertaken using the risk assessment and is not undertaken using the Statement of Applicability. The principle is to look at each risk in turn and compare the controls determined as necessary for the risk with the controls in ISO/IEC 27001:2022, Annex A, to help identify if there are any missing necessary controls for each risk.

8.5 Producing a Statement of Applicability

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.3 d).

Input: All controls applicable to the risk treatment (see 8.4).

Action: Produce a Statement of Applicability.

Trigger: Documentation of all necessary controls, their justification and implementation status.

Output: Statement of Applicability.

Implementation guidance:

In accordance with ISO/IEC 27001:2022, 6.1.3 d), the Statement of Applicability (SOA) should contain at least:

a) the necessary controls;

b) justification for their inclusion;

c) whether they are implemented or not;

d) justification for exclusions of controls from ISO/IEC 27001:2022, Annex A.

The SOA can easily be produced by examining the risk assessment to identify the necessary controls and risk treatment plan to identify those that are planned to be implemented. Only controls identified in the risk assessment can be included in the SOA. Controls cannot be added to the SOA independent of the risk assessment. There should be consistency between the controls necessary to realize selected risk treatment options and the SOA. The SOA can state that the justification for the inclusion of a control is the same for all controls and that they have been identified in the risk assessment as necessary to treat one or more risks to an acceptable level. No further justification for the inclusion of a control is needed for any of the controls. The implementation status of all of the controls contained in the SOA can be stated as "implemented", "partially implemented" or "not implemented". This can be either individually against each control or as an overall statement.

EXAMPLE The SOA contains the statement: "All the controls have been implemented". No additional analysis or information is required to complete the SOA.

8.6 Information security risk treatment plan

8.6.1 Formulation of the risk treatment plan

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.3 e).

Input: Results from risk assessments.

Action: Formulate risk treatment plan.

Trigger: The need of the organization to treat risks.

Output: Risk treatment plan.

Implementation guidance:

The purpose of this activity is to create plan(s) for treating specific sets of the risks that are on the list of prioritized risks (see Clause 7). A risk treatment plan is a plan to modify risk such that it meets the organization's risk acceptance criteria (see 6.4.2). There are two possible interpretations of the term "plan" in the context of risk treatment. The first is a project plan, i.e. a plan to implement the organization's necessary controls. The second is a design plan, i.e. the plan that not only identifies necessary controls but also describes how the controls interact with their environment and each other to modify risks. In practice, both can be used.

Once the controls are in place, the project plan ceases to have any value other than as a historical record, whereas the design plan is still useful.

Every risk that needs treatment should be treated in one of the risk treatment plans. An organization can choose to have several risk treatment plans, which together implement all required aspects of risk treatment. These can be organized on the basis of where the information resides (e.g. one plan

for the data centre, another for mobile computing, etc.), by asset (e.g. different plans for different asset classifications) or by events (such as those used when assessing risk using the event-based method).

While creating the risk treatment plan, organizations should consider the following:

— priorities in relation with the level of risk and urgency of treatment;

— whether different types of controls (preventive, detective, corrective) or their composition are applicable;

— whether it is necessary to wait for a control to be settled before starting to implement a new one on the same asset;

— whether there is a delay between the time the control is implemented and the moment where it is fully effective and operational.

For each treated risk the treatment plan should include the following information:

— the rationale for selection of the treatment options, including the expected benefits to be gained;

— those who are accountable and responsible for approving and implementing the plan;

— the proposed actions;

— the resources required, including contingencies;

— the performance indicators;

— the constraints;

— the required reporting and monitoring;

— when actions are expected to be undertaken and completed;

— implementation status.

The risk treatment plan actions should be ranked by priority in relation with the level of risk and urgency of treatment. The higher the level of risk, and in some cases the frequency of risk occurrence, the sooner the control is to be implemented.

For each listed risk within the risk treatment plan, detailed implementation information should be tracked and can include but is not limited to:

— names of risk owners and persons responsible for the implementation;

— implementation dates or timelines;

— control activities planned to test the implementation result;

— implementation status;

— cost level (investment, operation).

8.6.2 Approval by risk owners

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.3 f).

Input: Risk treatment plan(s).

Action: Approval of risk treatment plan(s) by risk owners.

Trigger: The need for risk treatment plan(s) to be approved.

Output: Approved risk treatment plan(s).

Implementation guidance:

The information security risk treatment plan should be approved by the risk owners once it is formulated. Risk owners should also decide on the acceptance of residual information security risks. This decision should be based on defined risk acceptance criteria.

The results of the risk assessment, the risk treatment plan and the remaining risks should be understandable to the risk owners so that they can discharge their accountabilities properly.

8.6.3 Acceptance of the residual information security risks

NOTE This subclause relates to ISO/IEC 27001:2022, 6.1.3 f).

Input: Approved risk treatment plan(s) and risk acceptance criteria.

Action: Determine whether the residual risks are acceptable.

Trigger: The need for the organization to decide on retaining residual risks.

Output: Accepted residual risks.

Implementation guidance:

In order to determine the residual risks, risk treatment plans should feed into the follow up assessment of residual likelihood and consequence. The proposed controls outlined in the risk treatment plans and related effectiveness should be considered in light of whether they will reduce the likelihood or the consequence, or both, and whether the level of residual risks is allocated to the risks. The level of residual risks is then considered by the risk owner to determine whether the residual risks are acceptable.

Risk treatment plans should describe how assessed risks are to be treated to meet risk acceptance criteria.

In some cases, the level of residual risk does not always meet risk acceptance criteria, because the criteria being applied do not take into account prevailing circumstances.

EXAMPLE It can be argued that it is necessary to retain risks because the benefits accompanying the risks are an important business opportunity, or because the cost of risk modification is too high.

However, it is not always possible to revise the risk acceptance criteria in a timely manner. In such cases, risk owners can retain risks that do not meet normal acceptance criteria. If this is necessary, the risk owner should explicitly comment on the risks and include a justification for the decision to override normal risk acceptance criteria.

Risk acceptance can involve a process to achieve endorsements of treatments prior to a final risk acceptance decision. It is important for risk owners to review and approve proposed risk treatment plans and resulting residual risks, and record any conditions associated with such approval. Depending on the risk assessment process and risk acceptance criteria, this can require a manager with a higher level of authority than the risk owner to agree to the risk acceptance.

It can take some time to implement a plan to treat assessed risks. Risk criteria can allow levels of risk to exceed a desired threshold to a defined extent if there is a plan in place to reduce that risk in an acceptable time. Risk acceptance decisions can take into account timeframes in risk treatment plans and whether or not risk treatment implementation progress is in line with what is planned.

Some risks can vary over time (regardless of whether this change is due to implementation of a risk treatment plan). Risk acceptance criteria can consider this and have risk acceptance thresholds that depend on the length of time that an organization can be exposed to an assessed risk.

9 Operation

9.1 Performing information security risk assessment process

NOTE This subclause relates to ISO/IEC 27001:2022, 8.2.

Input: Documents about the information security risk assessment process including risk assessment and risk acceptance criteria.

Action: The risk assessment process should be performed in accordance with Clause 7.

Trigger: The need of the organization to assess risks, at planned intervals or based on events.

Output: Evaluated risks.

Implementation guidance:

The information security risk assessment process defined and applied in ISO/IEC 27001:2022, 6.1, should be integrated into the organizational operations and it should be performed at planned intervals or when significant changes are proposed or occur. The information security risk assessment process should take into account the criteria established in ISO/IEC 27001:2022, 6.1.2 a). The intervals at which the risk assessment is performed should be appropriate to the ISMS. When a significant change of the ISMS (or its context) or a change in the threat landscape (e.g. a new type of information security attack) has occurred, the organization should determine if this change requires an additional information security risk assessment.

When making plans for routine risk assessments, organizations should take account of any calendar that applies to their general business processes and associated budget cycles.

EXAMPLE If there is an annual budget cycle, the organization can be required to submit funding requests at a certain time of year. Funds are then granted (diminished or denied) later.

If the procurement processes are involved, there can be another budget cycle before risk treatment recommendations can be implemented and their effectiveness assessed prior to the next routine risk assessment. In such cases, risk assessments should be scheduled:

a) to make their risk treatment recommendations in time for funding application;

b) to be reassessed following the results of budget allocations;

c) to perform the next routine assessment, once recommendations have been implemented, after any procurement activity.

9.2 Performing information security risk treatment process

NOTE This subclause relates to ISO/IEC 27001:2022, 8.3.

Input: Evaluated risk(s).

Action: The risk treatment process should be performed in accordance with Clause 8.

Trigger: The need of the organization to treat risks, at planned intervals or based on events.

Output: Retained or accepted residual risks.

Implementation guidance:

ISO/IEC 27001:2022, 8.3, specifies requirements for organizations to implement their risk treatment plans. Considerations included in 8.6 are also relevant to this subclause.

10 Leveraging related ISMS processes

10.1 Context of the organization

NOTE This subclause relates to ISO/IEC 27001:2022, Clause 4.

Input: Information on the organization, its internal and external context.

Action: All relevant data should be considered to identify and describe internal and external issues influencing information security risk management and requirements of interested parties.

Trigger: ISO/IEC 27001:2022 specifies requirements for such information to be able to establish information security objectives.

Output: Risk-related internal and external issues influencing information security risk management.

Implementation guidance:

The organization should have a high-level (e.g. strategic) understanding of the important issues that can affect the ISMS, either positively or negatively. It should further know the internal and external context that is relevant to its purpose and that affect its ability to achieve the intended outcome of its ISMS. The intended outcomes should ensure preservation of the confidentiality, integrity and availability of information by applying the risk management process and knowing which risks are adequately managed.

To reliably identify risks, the organization should understand in sufficient detail the circumstances in which the organization operates. This means the organization should gather information concerning the internal and external context of the organization, its interested parties and their requirements (see ISO/IEC 27001:2022, 4.1 and 4.2). Gathering this information should be done before any attempt is made by the organization to assess its information security risks, or indeed any other risks that can affect the intended outcome of the ISMS (see ISO/IEC 27001:2022, 6.1.1).

The organization should consider all internal and external risk sources. The organization's understanding of interested parties that are opposed to the organization and their interests is highly relevant.

EXAMPLE 1 An example of an interested party with interests that are opposed to the organization's objectives is the attacker. The attacker desires an organization with weak security level. The organization takes account of this party's interest by having the opposite (strong security level), i.e. the organization considers possible conflicts with the objectives of the ISMS. The organization ensures, through effective information security controls, that these interests are not met.

Interfaces with services or activities that are not completely within the scope of the ISMS should be considered in the organization's information security risk assessment.

EXAMPLE 2 An example of such a situation is the sharing of assets (e.g. facilities, IT systems and databases) with other organizations or the outsourcing of a business function.

How other relevant factors influencing information security are considered depends on the organization's choice of risk identification and analysis methods.

The organization's information security objectives (see ISO/IEC 27001:2022, 6.2) can constrain the risk acceptance criteria (e.g. the acceptable level of risk can be a function of the potential rewards associated with different business activities). Furthermore, the information security policy can constrain risk treatment (e.g. certain risk treatment options can be excluded by that policy).

10.2 Leadership and commitment

NOTE This subclause relates to ISO/IEC 27001:2022, 5.1.

Input: Information on information security risk assessment results or information security risk treatment results requiring approval or endorsement.

Action: Appropriate level of management should consider results related to information security risks, to decide on or endorse further actions.

Trigger: ISO/IEC 27001 requires appropriate level of management to be involved in all information security risk related activities.

Output: Information security risk related decisions or endorsement.

Implementation guidance:

Top management is accountable for managing risks and should lead and drive risk assessments, including:

— ensuring that the necessary resources are allocated to managing risk;

— assigning authority, responsibility and accountability at appropriate levels within the organization as it relates to risk management;

— communicating with appropriate interested parties.

10.3 Communication and consultation

NOTE 1 This subclause relates to ISO/IEC 27001:2022, 7.4.

NOTE 2 ISO/IEC 27001 refers directly to the communication part of this activity.

Input: Information on risks, their causes, consequences and their likelihood identified through the risk management processes.

Action: Information on risks, their causes, consequences, their likelihood and the controls being taken to treat them should be communicated to, or obtained from, the external and internal interested parties.

Trigger: ISO/IEC 27001 requires such communication.

Output: Relevant interested parties' perceptions and continual understanding of the organization's information security risk management process and results.

Implementation guidance:

The communication and consultation activity aims to achieve agreement on how to manage risks by exchanging and/or sharing information about risk with the risk owners and other relevant interested parties. The information includes, but is not limited to, the existence, nature, form, likelihood, consequence, significance, treatment and acceptance of risks.

ISO/IEC 27001:2022, 6.1.2 c) 2), requires that owners of the information security risks be identified. Risk ownership can be deliberately confused or concealed. Even when risk owners can be identified, they can be reluctant to acknowledge that they are responsible for the risks that they own, and obtaining their participation in the risk management process can be difficult. There should be a defined communication procedure for informing those concerned about risk ownership.

ISO/IEC 27001:2022, 6.1.3 f), requires the risk owners to approve the risk treatment plan(s) and to decide on the acceptance of residual risks. Communication between risk owners and staff responsible for the implementation of the ISMS is an important activity. There should be an agreement on how to manage risks by exchanging and/or sharing information about risk with the risk owners, and perhaps other interested parties and decision-makers. The information includes, but is not limited to, the existence, nature, form, likelihood, significance, treatment and acceptance of risks. Communication should be bi-directional.

Depending on the nature and sensitivity of the risk(s), there can be a need to limit some information about risks, their assessment and treatment on a need-to-know basis to those responsible for identifying, assessing and treating them. Risk communication should be controlled on a "need to know" basis, taking into account the level of detail required by different interested parties, in consultation with the risk owners or potential owners, with the aim of avoiding publicizing the more sensitive risks and their associated known weaknesses.

Perceptions of risk can vary due to differences in assumptions, concepts, needs, issues and concerns of the appropriate interested parties as they relate to risk or the issues under discussion. Interested parties are likely to make judgments on the acceptance of risk, based on their perception of risk. This is especially important to ensure that the interested parties' perceptions of risk, as well as their perceptions of benefits, can be identified and documented and the underlying reasons clearly understood and addressed.

Communication and consultation concerning risks can result in improved interested parties' engagement with what is being done and appropriate interested parties taking ownership of decisions and outcomes. Communication and consultation with interested parties, as criteria are developed and as methods for risk assessment are selected, can also improve ownership of outcomes by interested parties. Interested parties are less likely to question the outcomes of processes that they have helped design. As a result, the likelihood that they accept findings and support action plans is often increased. In cases where interested parties are managers, this can build commitment to achieving risk management objectives and providing the necessary resources.

Risk communication should be carried out in order to:

— provide assurance of the outcome of the organization's risk management;

— collect risk information;

— share the results from the risk assessment and present the risk treatment plan;

— avoid or reduce both the occurrence and consequence of information security breaches due to the lack of mutual understanding among risk owners and interested parties;

— support risk owners;

— obtain new information security knowledge;

— coordinate with other parties and plan responses to reduce the consequences of any incident;

— give a sense of responsibility to risk owners and other parties with a legitimate interest at risk;

— improve awareness.

An organization should develop risk communication plans for normal operations as well as for emergencies. The risk communication and consultation activity should be performed continually.

The coordination between major risk owners and relevant interested parties can be achieved by the formation of a committee where debate about risks, their prioritization and appropriate treatment, and acceptance can take place.

Risk communications can be voluntarily forwarded to external third parties for enabling better risk management or response coordination or awareness and can also be required by regulators or business partners under certain circumstances.

It is important to cooperate with the appropriate public relations or communications unit within the organization to coordinate all tasks related to risk communication. This is crucial in the event of crisis communication activation, e.g. in response to particular incidents.

10.4 Documented information

10.4.1 General

NOTE This subclause relates to ISO/IEC 27001:2022, 7.5.

ISO/IEC 27001 specifies requirements for organizations to retain documented information concerning the risk assessment process (see ISO/IEC 27001:2022, 6.1.2) and results (see ISO/IEC 27001:2022, 8.2); the risk treatment process (ISO/IEC 27001:2022, 6.1.3) and results (ISO/IEC 27001:2022, 8.3).

10.4.2 Documented information about processes

Input: Knowledge on the information security risk assessment and treatment processes in accordance with Clauses 7 and 8, defined by the organization.

Action: Information about the information security risk assessment and treatment processes should be documented and retained.

Trigger: ISO/IEC 27001 requires documented information about the information security risk assessment and treatment processes.

Output: Documented information required by interested parties (e.g. certification body) or determined by the organization as being necessary for the effectiveness of the information security risk assessment process or information security risk treatment process.

Implementation guidance:

Documented information about the information security risk assessment process should contain:

a) a definition of the risk criteria (including the risk acceptance criteria and the criteria for performing information security risk assessments);

b) reasoning for the consistency, validity and comparability of results;

c) a description of the risk identification method (including the identification of risk owners);

d) a description of the method for analysing the information security risks (including the assessment of potential consequences, realistic likelihood and resultant level of risk);

e) a description of the method for comparing the results with the risk criteria and the prioritization of risks for risk treatment.

Documented information about the information security risk treatment process should contain descriptions of:

— the method for selecting appropriate information security risk treatment options;

— the method for determining necessary controls;

— how ISO/IEC 27001:2022, Annex A, is used to determine that necessary controls have not been inadvertently overlooked;

— how risk treatment plans are produced;

— how risk owners' approval is obtained.

10.4.3 Documented information about results

Input: The information security risk assessment and treatment results.

Action: Information about the information security risk assessment and treatment results should be documented and retained.

Trigger: ISO/IEC 27001 requires documented information about the information security risk assessment and treatment results.

Output: Documented information about the information security risk assessment and treatment results.

Implementation guidance:

As organizations are required to perform risk assessments at planned intervals or when significant changes are proposed or occur, there should at least be evidence of a schedule, and risk assessments being performed in accordance with that schedule. If a change is proposed, or has occurred, then there should be evidence of the performance of an associated risk assessment. Otherwise, the organization should explain why the change is significant or not.

Documented information about the information security risk assessment results should contain:

a) the identified risks, their consequence and likelihood;

b) the identity of the risk owner(s);

c) the results of applying the risk acceptance criteria;

d) the priority for risk treatment.

Recording of the rationale for risk decisions is also recommended, in order to both learn from error in individual cases and facilitate continual improvement.

Documented information about the information security risk treatment results should contain:

— identification of the necessary controls;

— where appropriate and available, evidence that these necessary controls act to modify risks, so as to meet the organization's risk acceptance criteria.

10.5 Monitoring and review

10.5.1 General

NOTE This subclause relates to ISO/IEC 27001:2022, 9.1.

The organization's monitoring process (see ISO/IEC 27001:2022, 9.1) should encompass all aspects of the risk assessment and risk treatment processes for the purposes of:

a) ensuring that the risk treatments are effective, efficient and economical in both design and operation;

b) obtaining information to improve future risk assessments;

c) analysing and learning lessons from incidents (including near misses), changes, trends, successes and failures;

d) detecting changes in the internal and external context, including changes to risk criteria and the risks themselves, which can require revision of risk treatments and priorities;

e) identifying emerging risks.

Retained risk scenarios, coming from the risk management activities, can be transposed into monitoring scenarios in order to ensure an effective monitoring process. Further details about monitoring scenarios are given in A.2.7.

10.5.2 Monitoring and reviewing factors influencing risks

NOTE This subclause relates to ISO/IEC 27001:2022, 9.1.

Input: All risk information obtained from the risk management activities.

Action: Risks and their factors (i.e. value of assets, consequences, threats, vulnerabilities, likelihood of occurrence) should be monitored and reviewed to identify any changes in the context of the organization at an early stage, and to maintain an overview of the complete risk picture.

Trigger: Reviewing organizational policy and any detection of changes to the current operating or threat environment.

Output: Continual alignment of the management of risks with the organization's business objectives, and with risk acceptance criteria.

Implementation guidance:

ISO/IEC 27001:2022, 9.1, requires organizations to evaluate their information security performance (and ISMS effectiveness). In accordance with this requirement, organizations should use their risk treatment plan(s) as a subject for their performance evaluations. To do this, an organization should first define one or more information needs, e.g. to describe what top management wishes to know about the organization's ability to defend itself against threats. Using this as a top-level specification, an organization should then determine the measurements that it needs to make and how such measures should be combined in order to satisfy the information need.

Risks are not static. Event scenarios, asset values, threats, vulnerabilities, likelihoods and consequences can change abruptly without any indication. Constant monitoring should be carried out to detect these changes. This can be supported by external services that provide information regarding new threats or vulnerabilities. Organizations should ensure the continual monitoring of relevant factors, such as:

a) new sources of risk, including freshly reported vulnerabilities in IT;

b) new assets that have been included in the risk management scope;

c) necessary modification of asset values (e.g. due to changed business requirements);

d) identified vulnerabilities to determine those becoming exposed to new or re-emerging threats;

e) changes in patterns of use of existing or new technologies that can open up new possible opportunities for attack;

f) changes in laws and regulations;

g) changes in risk appetite and perceptions of what is now acceptable and what is no longer acceptable;

h) information security incidents, both inside and outside of the organization.

New sources of risk or changes in likelihood or consequences can increase risks previously assessed. Review of low and retained risks should examine each risk separately, and all such risks as an aggregate as well, to assess their potential accumulated consequence. If risks no longer fall into the low or acceptable risk category, they should be treated using one or more of the options in 8.2.

Factors that affect the likelihood of the occurrence of events and their corresponding consequences can change, as can factors that affect the suitability or cost of the various treatment options. Major changes affecting the organization should be a reason for a more specific review. The risk monitoring activities should be regularly repeated and the selected options for risk treatment should be reviewed periodically.

New threats, vulnerabilities or changes in likelihood or consequences can increase risks previously assessed as low ones. Review of low and retained risks should consider each risk separately, and all such risks as an aggregate as well, to assess their potential accumulated consequence. If risks do not fall into the low or acceptable risk category, they should be treated using one or more of the options considered in Clause 8.

Factors that affect the likelihood of the occurrence of threats and their corresponding consequences can change, as can factors that affect the suitability or cost of the various treatment options. Major changes affecting the organization should be reason for a more specific review. The risk monitoring activities should be regularly repeated and the selected options for risk treatment should be reviewed periodically.

The outcome of risk monitoring activities can be input to other risk review activities. The organization should review all risks regularly, and when major changes are proposed or occur in accordance with ISO/IEC 27001:2022, Clause 8.

10.6 Management review

NOTE This subclause relates to ISO/IEC 27001:2022, 9.3.

Input: Results of information security risk assessment(s), status of information security risk treatment plan.

Action: The results of information security risk assessment and status of the information security risk treatment plan should be reviewed to confirm that residual risks meet risk acceptance criteria, and that the risk treatment plan addresses all relevant risks and their risk treatment options.

Trigger: A part of scheduled calendar of review activities.

Output: Changes of the risk acceptance criteria and the criteria for performing information security risk assessments, updated information security risk treatment plan or SOA.

10.7 Corrective action

NOTE This subclause relates to ISO/IEC 27001:2022, 10.1.

Input: The risk treatment plan is proving ineffective, meaning that the residual risk will remain at unacceptable levels after the treatment plan is complete.

Action: Revise the risk treatment plan and implement it to modify the residual risk to an acceptable level.

Trigger: The decision for revising the risk treatment plan.

Output: A revised risk treatment plan and its implementation.

Implementation guidance:

Nonconformities related to effectiveness of the risk treatment plan can be raised by an internal or external audit, or through monitoring and indicators. The treatment plan should be revised to reflect:

— the outcomes of the information security risk treatment process;

— progressive implementation of the plan (e.g. a control is implemented as-specified, as-designed, as-built);

— identified difficulties in implementation of controls (e.g. technical or financial issues, inconsistencies with internal or external factors such as privacy considerations).

There are also cases where even if the residual risks are acceptable after the treatment plan is complete, the users will reject its use, or attempt to circumvent because these controls are not accepted by the users in terms of ease of use (e.g. not ergonomic, too complicated or too long).

The organization should review the effectiveness of the revised treatment plan.

10.8 Continual improvement

NOTE This subclause relates to ISO/IEC 27001:2022, 10.2

Input: All risk information obtained from the risk management activities.

Action: The information security risk management process should be continually monitored, reviewed and improved as necessary.

Trigger: Organization seeks to improve and mature from the lessons learnt during the information security risk management process.

Output: Continual relevance of the information security risk management process to the organization's business objectives or updating the process.

Implementation guidance:

Ongoing monitoring and review that the context, the outcome of the risk assessment and risk treatment, as well as management plans, remain relevant and appropriate to the circumstances is necessary to ensure that the information security risk management process is correct.

The organization should make sure that the information security risk management process and related activities remain appropriate in the present circumstances and are followed. Any agreed improvements to the process, or actions necessary to improve compliance with the process, should be notified to the responsible managers. These managers should be given assurance that no risk or risk element is overlooked or underestimated and that the necessary actions are taken and decisions are made to provide a realistic risk understanding and ability to respond.

It should be noted that the change management process should continually provide feedback to the risk management process in order to ensure that variations to information systems able to modify risks are promptly taken into account, even modifying risk assessment activities to properly evaluate them.

Additionally, the organization should regularly verify the criteria used to measure the risk. This verification should ensure that all elements are still valid and consistent with business objectives, strategies and policies, and that changes to the business context are taken into consideration adequately during the information security risk management process. This monitoring and review activity should address (but not be limited to):

— legal and environmental context;

— competition context;

— risk assessment approach;

— asset value and categories;

— consequence criteria;

— likelihood criteria;

— risk evaluation criteria;

— risk acceptance criteria;

— total cost of ownership;

— necessary resources.

The organization should ensure that risk assessment and risk treatment resources are continually available to review risk, to address new or changed threats or vulnerabilities, and to advise management accordingly.

Risk management monitoring can result in modifying or adding to the approach, methodology or tools used depending on:

— the organization's risk maturity;

— changes identified;

— risk assessment iteration;

— the aim of the information security risk management process (e.g. business continuity, resilience to incidents, compliance);

— the object of the information security risk management process (e.g. organization, business unit, information process, its technical implementation, application, connection to the internet).

The risk management cycles related to the scope of risk assessment and risk treatment are presented in 5.2.

Annex A
(informative)

Examples of techniques in support of the risk assessment process

A.1 Information security risk criteria

A.1.1 Criteria related to risk assessment

A.1.1.1 Risk assessment general considerations

In general, personal uncertainty dominates information risk assessment, and different analysts exhibit differing tendencies to uncertainty when interpreting points on likelihood and consequence scales. The reference scales should relate the consequence, likelihood and risk categories to common unambiguously specified objective values, possibly expressed in terms such as financial loss in monetary units and notional frequency of occurrence in a finite period which are specific for the quantitative approach.

Particularly where the qualitative approach is adopted, risk analysts should undergo training and periodic practice against an anchoring reference scale to maintain the calibration of their judgement.

A.1.1.2 Qualitative approach

A.1.1.2.1 Consequences scale

Table A.1 presents an example of consequence scale.

Table A.1 — Example of consequence scale

Consequences	Description
5 – Catastrophic	**Sector or regulatory consequences beyond the organization** Substantially impacted sector ecosystem(s), with consequences that can be long lasting. And/or: difficulty for the State, and even an incapacity, to ensure a regulatory function or one of its missions of vital importance. And/or: critical consequences on the safety of persons and property (health crisis, major environmental pollution, destruction of essential infrastructures, etc.).
4 – Critical	**Disastrous consequences for the organization** Incapacity for the organization to ensure all or a portion of its activity, with possible serious consequences on the safety of persons and property. The organization will most likely not overcome the situation (its survival is threatened), the activity sectors or state sectors in which it operates will likely be affected slightly, without any long-lasting consequences.
3 – Serious	**Substantial consequences for the organization** High degradation in the performance of the activity, with possible significant consequences on the safety of persons and property. The organization will overcome the situation with serious difficulties (operation in a highly degraded mode), without any sector or state impact.
2 – Significant	**Significant but limited consequences for the organization** Degradation in the performance of the activity with no consequences on the safety of persons and property. The organization will overcome the situation despite a few difficulties (operation in degraded mode).

Table A.1 *(continued)*

Consequences	Description
1 – Minor	**Negligible consequences for the organization** No consequences on operations or the performance of the activity or on the safety of persons and property. The organization will overcome the situation without too much difficulty (margins will be consumed).

A.1.1.2.2 Likelihood scale

Table A.2 and Table A.4 present examples of alternative ways to represent likelihood scales. Likelihood can be expressed either in probabilistic terms as in Table A.2 or in frequentist terms as in Table A.4. The probabilistic representation indicates the average likelihood of a risk event occurring in a specified period, whereas the frequentist representation indicates the number of times the risk event is expected to occur on average in a specified time period. As the two approaches merely express the same thing from two different perspectives, either representation can be used, depending on which the organization finds most convenient for a given category of risks.

However, if both approaches are used as alternatives within the same organization, it is important that each notionally equivalent rank on both scales represents the same actual likelihood. Otherwise, the results of assessment depend on which scale is used, rather than on the actual likelihood of the risk source being assessed. If both approaches are used, the probabilistic level for each notional rank should be calculated mathematically from the frequentist value of the equivalent rank or vice versa depending on which approach is used to define the primary scale.

If either of the two approaches alone is used, it is not necessary for the increments of the scale to be so closely defined, as prioritization of likelihoods can still be achieved regardless of the absolute values used. Although Table A.2 and Table A.4 use completely different increments and ranges of likelihood, depending on the organization's context and the category of risk being assessed, either can be equally effective for analysis if used exclusively. They would not, however, be usable safely as alternatives in the same context as the values attached to equivalent rankings do not correlate.

The categories and values used in Table A.2 and Table A.4 are only examples. The most appropriate value to assign to each level of likelihood depends on the risk profile and risk appetite of the organization.

Table A.2 — Example of likelihood scale

Likelihood	Description
5 – Almost certain	The risk source will most certainly reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very high.
4 – Very likely	The risk source will probably reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is high.
3 – Likely	The risk source is able to reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is significant.
2 – Rather unlikely	The risk source has relatively little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is low.
1 – Unlikely	The risk source has very little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very low.

Verbal labels such as “low”, “medium” and “high” can be attached to the rankings when using either approach to likelihood assessment. These can be useful when discussing levels of likelihood with

interested parties who are not risk specialists. However, they are subjective and therefore unavoidably ambiguous. Consequently, they should not be used as primary descriptors when performing or reporting assessments.

A.1.1.2.3 Level of risk

The utility of qualitative scales and the consistency of risk assessments that derive from them depend entirely on the consistency with which the category labels are interpreted by all interested parties. The levels of any qualitative scale should be unambiguous, its increments should be clearly defined, the qualitative descriptions for each level should be expressed in objective language and the categories should not overlap with each other.

Consequently, when using verbal descriptors of likelihood, consequence or risk, these should be formally referenced to unambiguous scales anchored to numerical (as in Table A.4) or ratiometric (as in Table A.2) reference points. All interested parties should be made aware of the reference scales to ensure that interpretation of qualitative assessment data and results is consistent.

Table A.3 presents an example of qualitative approach.

Table A.3 — Example of qualitative approach to risk criteria

Likelihood	Consequence				
	Catastrophic	**Critical**	**Serious**	**Significant**	**Minor**
Almost certain	Very high	Very high	High	High	Medium
Very likely	Very high	High	High	Medium	Low
Likely	High	High	Medium	Low	Low
Rather unlikely	Medium	Medium	Low	Low	Very low
Unlikely	Low	Low	Low	Very low	Very low

The design of a qualitative risk matrix should be guided by the organization's risk acceptance criteria (see 6.4.2 and A.1.2).

EXAMPLE An organization is sometimes more concerned about extreme consequences despite their unlikely occurrence, or primarily concerned about high frequency events with lesser consequences.

When designing a risk matrix, whether qualitative or quantitative, an organization's risk profile is normally asymmetrical. Trivial events are generally the most frequent and expected frequency typically reduces as consequences increase, culminating in very low likelihoods of extreme consequences. It is also uncommon for the business exposure represented by a high likelihood/low consequence event to be equivalent to that represented by a low likelihood/high consequence event. Although a risk matrix that is symmetrical about its low/low to high/high diagonal can seem easy to create and naively acceptable, it is unlikely to represent accurately any organization's real risk profile, and can therefore yield invalid results. To ensure that a risk matrix is realistic and can fulfil the requirement for continuous improvement (see ISO/IEC 27001:2022, 10.2), the reasoning both for allocating each category to the likelihood and consequence scales and the risk matrix, and regarding how the categories accord with the organization's risk profile, should be documented when the scales and matrix are defined or amended. As a minimum, the uncertainties intrinsic to using incremental scale matrices should be described with due cautions to their users.

The utility of qualitative scales and the consistency of risk assessments that derive from them depend entirely on the consistency with which the category labels are interpreted by all interested parties. The levels of any qualitative scale should be unambiguous, its increments should be clearly defined, the qualitative descriptions for each level should be expressed in objective language and the categories should not overlap with each other.

A.1.1.3 Quantitative approach

A.1.1.3.1 Finite scales

The level of risk can be calculated using any method and taking into account any relevant factors, but it is usually shown by multiplying the likelihood by the consequence.

Likelihood represents the probability or frequency of an event occurring within a given timeframe. This timeframe is typically annually (per year) but can be as large (e.g. per century) or little (e.g. per second) as the organization wants.

Likelihood scales should be defined in practical terms that reflect the context of the organization, so they help it to manage risk and are easy for all interested parties to understand. That primarily means setting realistic limits to the range of represented likelihoods. If the maximum and minimum limits of the scale are too far apart, each category within it includes an excessively wide range of likelihoods, making assessment uncertain.

EXAMPLE 1 The highest finite likelihood point on the scale can usefully be defined in terms of the time it typically takes for the organization to respond to events, and the lowest finite point in terms of the duration of the organization's long-term strategic planning.

Likelihoods above and below the defined limits of the scale can usefully be expressed as “greater than scale maximum” and “less than scale minimum”, clearly indicating thereby that likelihoods beyond the limits of the defined scale are extreme cases to be considered exceptionally (possibly using special “out of bounds” criteria). Outside these limits, the specific likelihood is less important than the fact of it being an exception in the given direction.

Usually, it is helpful to measure consequence using a financial figure, as this allows aggregation for reporting of risk.

EXAMPLE 2 Monetary consequence scales are typically based on factors of 10 (100 to 1 000; 1 000 to 10 000, etc.).

The widths of the categories of a likelihood scale should be selected with reference to those of the chosen consequence scale to avoid an excessive range of risk falling into each category.

EXAMPLE 3 If likelihood and consequence are represented by the indices of an exponential scale (i.e. the logarithms of the values on the scale), these should be summed.

The risk value can then be calculated as follows: antilog [log (likelihood value) + log (consequence value)].

Table A.4 — Example logarithmic likelihood scale

Approximate average frequency	Log expression	Scale value
Every hour	(approximately 10^5)	5
Every 8 hours	(approximately 10^4)	4
Twice a week	(approximately 10^3)	3
Once a month	(approximately 10^3)	2
Once a year	(10^1)	1
Once a decade	(10^0)	0

EXAMPLE 4 In Table A.4, an example of a high frequency event is a computer assisted event password attack or a distributed Denial-of-Service attack from a botnet. Indeed, attack frequencies can be much higher.

EXAMPLE 5 In Table A.4, an example of a low frequency event is volcanic eruptions. Even if an event is predicted to happen only once per century that does not mean it would not occur during the lifetime of an ISMS.

Table A.5 shows an example of logarithmic consequence scale. One purpose of considering frequency is to ensure that protective measures are strong enough to withstand high frequency attack sequences, even when the likelihood of such an attack sequence is low.

Table A.5 — Example logarithmic consequence scale

Consequence (a loss of)	Log expression	Scale value
£1 000 000	(10^6)	6
£100 000	(10^5)	5
£10 000	(10^4)	4
£1 000	(10^3)	3
£100	(10^2)	2
Less than £100	(10^1)	1

If both likelihood and consequence scales use a logarithmic base 10 to assign level, risk analysts can end up with too many risks on the same risk level and can be unable to make an appropriate prioritization or security investment decision. In that case, it can be useful to reduce the base and increase the number of considered levels. It should be noted that if different bases for likelihood and consequences are chosen, then a useful formula to sum up two factors cannot be applied.

EXAMPLE 6 If the likelihood is doubled when going from one level to the next, whereas the consequence is a factor of 10 more expensive, the formula will result in risks a) and b), where risk b) has a consequence level of 10 times more expensive than risk a) but only half the likelihood of risk a) ending up on the same risk level. This is economically incorrect.

Table A.4 and Table A.5 list ranges of likelihood and consequence that cover most eventualities across widely differing organizations. No single organization is likely to encounter the range of risk represented by the entirety of these example scales. The context of the organization and the scope of the ISMS should be used to define realistic upper and lower limits for both likelihoods and consequences, bearing in mind that quantifying ranges of risk in excess of 1 000 to 1 is likely to be of limited practical value.

A.1.2 Risk acceptance criteria

The criteria for the acceptance of risk can simply be a value above which the risks are deemed unacceptable.

EXAMPLE 1 In Table A.3, if the value medium is chosen, all risks with a value of very low, low or medium would be considered acceptable by the organization and all risks with a value of high or very high would be considered unacceptable.

By using a colour-coded risk matrix mirroring the scales for consequence and likelihood, organizations can present the risk distribution from one or several risk assessments graphically. Such a risk matrix may also be used for signalling the risk organization's attitude to the risk values and indicate whether a risk normally should be accepted or treated.

EXAMPLE 2 A risk matrix using three colours, e.g. red, amber and green can be applied to represent three risk evaluation grades, as presented in Table A.6.

It can be beneficial to choose other models using colours to a risk matrix.

EXAMPLE 3 If a risk matrix is used for comparing the results from an originally performed risk assessment with the results of a reassessment for the same risks, the risk reduction can be more easily presented if more colours are applied to present risk levels.

It is also possible to add determination of which level of management is authorized to accept a risk with a certain risk value to such a model.

Table A.6 presents an example of evaluation scale.

Table A.6 — Example of evaluation scale combined with three-colour risk matrix

Level of risk	Risk evaluation	Description
Low (green)	Acceptable as is	The risk can be accepted without further action.
Moderate (amber)	Tolerable under control	A follow-up in terms of risk management should be conducted and actions should be set up in the framework of continuous improvement over the medium and long term.
High (red)	Unacceptable	Measures for reducing the risk should absolutely be taken in the short-term. Otherwise, all or a portion of the activity should be refused.

A.2 Practical techniques

A.2.1 Information security risk components

When identifying and assessing information security risks, the following components should be taken into account:

— components related to the past:
  — security events and incidents (both inside the organization and outside);
  — risk sources;
  — exploited vulnerabilities;
  — measured consequences;
— components related to the future:
  — threats;
  — vulnerabilities;
  — consequences;
  — risk scenarios.

Relationships between information security risk components are presented in Figure A.1 and discussed in A.2.2 to A.2.7.

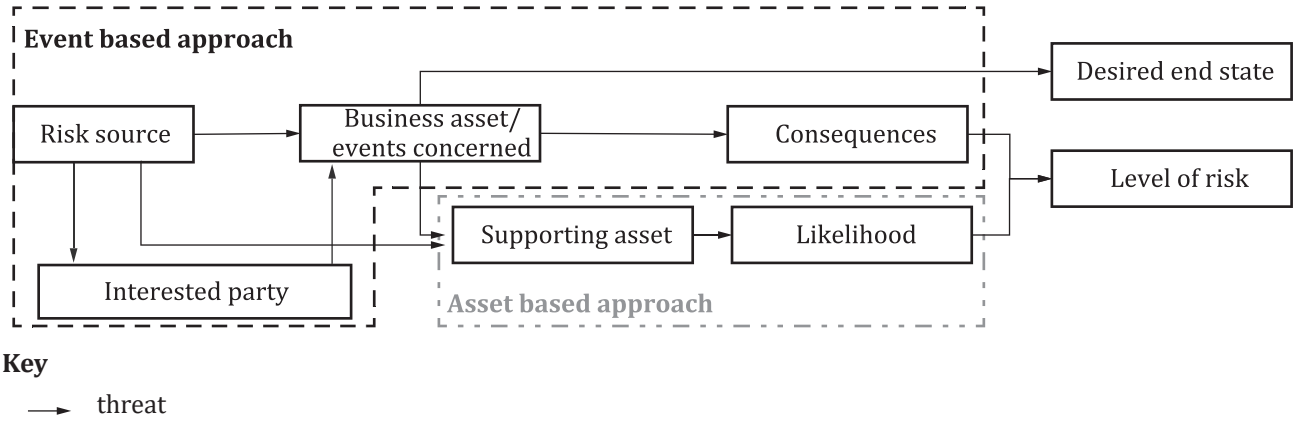


Figure A.1 — Information security risk assessment components

Details about "Desired end state" can be found in A.2.3 b).

A.2.2 Assets

When applying the asset-based approach to the risk identification, the assets should be identified.

In the risk assessment process, within the development of risk scenarios, the identification of events, consequences, threats, vulnerabilities, should be linked to assets.

In the risk treatment process, each control is applicable to a subset of the assets.

The assets can be divided into two categories:

— primary/business assets — information or processes of value for an organization;

— supporting assets — components of the information system on which one or several business assets are based.

The primary/business assets are often used in the event-based approach (identification of events and their consequences on business assets).

The supporting assets are often used in the asset-based approach (identification and analysis of vulnerabilities and threats on these assets) and in the risk treatment process (specification of the asset(s) to which each control should be applied).

Business and supporting assets are related, therefore risk sources identified for supporting assets can impact business assets.

For this reason, it is important to identify the relationships between the assets, and to understand their value to the organization. Misjudging the asset value can lead to a misjudgement of the consequences related to the risk but can also affect the understanding of the likelihood of threats under consideration.

EXAMPLE 1 A supporting asset is hosting a business asset (information in this case).

Data are protected by internal and external controls in order to prevent a risk source from achieving its objective related to the business asset by exploiting a vulnerability on the supporting asset. When distinguishing different types of assets, dependencies between assets should be documented and risk propagation assessed, so that it can be documented that the same risk is not assessed twice, once when it occurs on the supporting asset, and once when it affects the primary assets. Asset dependency graphs are useful tools to represent such dependencies and ensure that all dependencies have been considered.

EXAMPLE 2 The graph in Figure A.2 indicates dependent assets for the “showing order and invoice processing” business asset and can be read as follows:

— “Administrator” (type: human resource), who, if not properly trained, propagates a risk to the asset.

— “Maintain IT” (type: service), which propagates the risk to the asset.

— “Server” (type: hardware) or to the asset “Network” (type network connectivity). The server, if it stops operating or the misconfigured network causes the asset.

— “Web portal” (type: application), to stop running or to be unavailable.

Without “web portal”, the business process “showing order and invoice processing” does not offer the intended process to the customers.

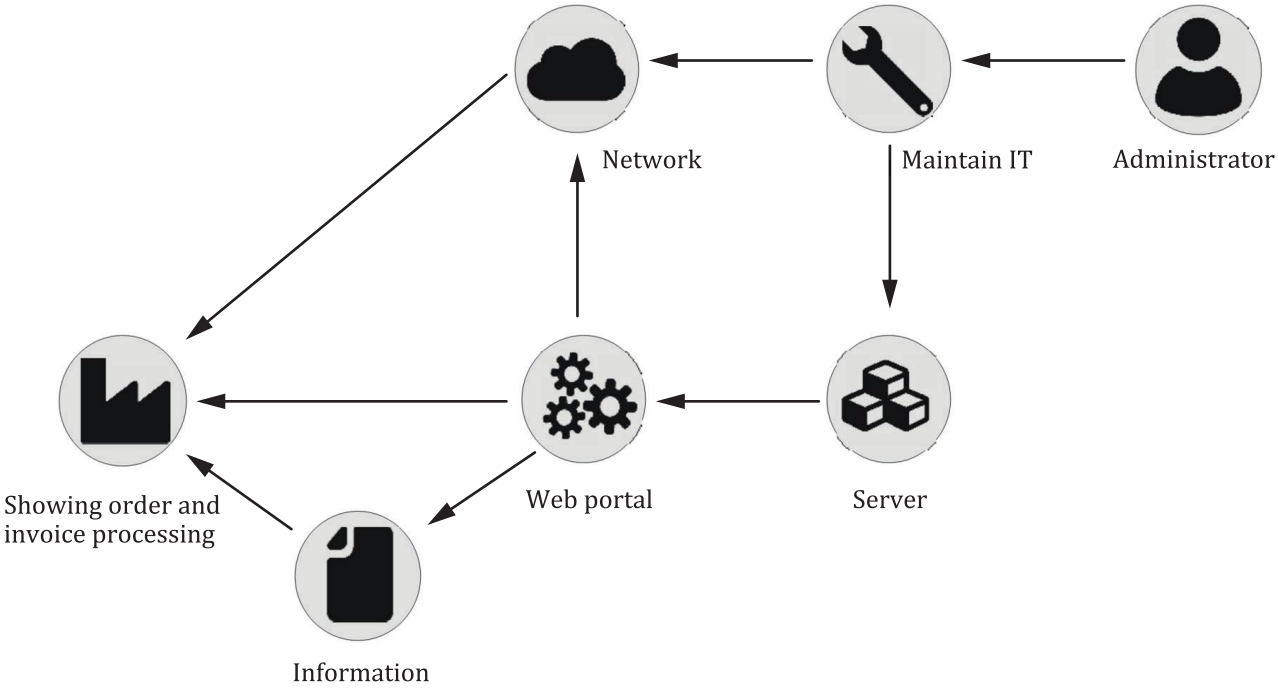


Figure A.2 — Example of an asset dependency graph

A.2.3 Risk sources and desired end state

This paragraph proposes to characterize this type of risk sources. Two main criteria structure this descriptive approach:

— the motivation;

— the ability to act.

a) Risk source identification

Table A.7 presents examples and usual methods of attack.

Table A.7 — Examples and usual methods of attack

Risk source	Examples and usual methods of attack
State-related	States, intelligence agencies Method: Attacks generally conducted by professionals, working under a calendar and a method of attack that are predefined. This attacker profile is characterized by its ability to carry out an offensive operation over a long period of time (stable resources, procedures) and to adapt its tools and methods to the topology of the target. By extension, these actors have the means of purchasing or discovering 0-Day vulnerabilities and some are able to infiltrate isolated networks and to conduct successive attacks in order to reach a target or targets (e.g. by means of an attack aimed at the supply chain).
Organized crime	Cybercriminal organizations (mafias, gangs, criminal outfits) Method: Online scams or in person, ransom request or attack via ransomware, use of bot-nets, etc. Due in particular to the proliferation of attack kits that are readily available online, cybercriminals are conducting increasingly sophisticated and organized operations for lucrative or fraudulent purposes. Some have the means of purchasing or discovering 0-Day vulnerabilities.

Table A.7 *(continued)*

Risk source	Examples and usual methods of attack
Terrorist	Cyber-terrorists, cyber-militias Method: Attacks that are usually not very sophisticated but which are conducted with determination for the purposes of destabilization and destruction: denial of service (aimed for example at making the emergency services of a hospital centre unavailable, untimely shutdowns of an energy production industrial system), exploitation of vulnerabilities of Internet sites and defacement.
Ideological activist	Cyber-hacktivists, interest groups, sects Method: The methods of attack and sophistication of the attacks are relatively similar to those of cyber-terrorists but are motivated by less destructive intentions. Some actors conduct these attacks in order to convey an ideology, a message (e.g. massive use of social networks as a sounding board).
Specialized outfits	"Cyber-mercenary" profile with IT capacities that are generally high from a technical standpoint. Because of this, it should be distinguished from script-kiddies with whom it shares however the spirit of a challenge and search for recognition but with a lucrative objective. Such groups can be organized as specialized outfits that propose veritable hacking services. Method: This type of experienced hacker is often at the origin of the designing and creating of attack kits and tools that are available online (possibly for a fee) which can then be used "turnkey" by other groups of attackers. There are no particular motivations other than financial gain.
Amateur	Profile of the script-kiddies hacker or who has good IT knowledge; motivated by the quest for social recognition, fun, challenge. Method: Basic attacks but with the capacity of use the attack kits that are available online.
Avenger	The motivations of this attacker profile are guided by a spirit of acute vengeance or a feeling of injustice (e.g. employee dismissed for serious fault, discontented service provider following a contract that was not renewed, etc.). Method: This attacker profile is characterized by its determination and its internal knowledge of the systems and organizational processes. This can make it formidable and provide it with substantial power to do harm.
Pathological attacker	The motivations of this attacker profile are of a pathological or opportunistic nature and are sometimes guided by the motive for a gain (e.g. unfair competitor, dishonest client, scammer, and fraudster). Method: Here, either attackers have a knowledge base in computing that leads them to attempt to compromise the IS of their target, or they use the attack kits available online, or decide to subcontract the IT attack by calling upon a specialized outfit. In certain cases, attackers can direct their attention to an internal source (discontented employee, unscrupulous service provider) and attempt to corrupt the latter.

b) Modelling a risk source's motivation — desired end state

There is a wide range of motivations; they can be political, financial, ideological, but also social or even represent a one-off or pathological psychological condition.

While it is not possible to directly express a motivation, it can be illustrated through the risk source's intention and expressed in the form of a desired end state (DES): the overall situation that the risk source wants to reach after the confrontation. A systematic classification of situations, associated with general categories of action, can guide the contextualized analysis.

Table A.8 presents an example classification of motivations to express the DES.

Table A.8 — Example classification of motivations to express the DES

Conquer	Long-term capture of resources or economic markets, gaining political power or imposing values
Acquire	Predatory approach, resolutely offensive, driven by capturing resources or benefits
Prevent	Offensive approach to limit the actions of a third party
Maintain	Efforts to maintain an ideological, political, economic or social situation
Defend	Adopting a strictly defensive fallback stance, or an explicitly threatening attitude (e.g. intimidation) in order to prevent the aggressive behaviour of a clearly designated opponent or prevent their action by slowing them down, etc.
Survive	Protecting an entity at all costs, which can lead to extremely aggressive actions

c) Target objectives

To reach the DES, the risk source focuses on one or several objectives impacting the business assets of the target system. These are the target objectives of the risk source.

Table A.9 presents examples of target objectives.

Table A.9 — Examples of target objectives

Target objective	Description
Spying	Intelligence operation (state-related, economic). In many cases, the attacker aims for a long-term installation in the information system and with total discretion. Weaponry, space, aeronautics, the pharmaceutical sector, energy and certain activities of the State (economics, finance, and foreign affairs) are privileged targets.
Strategic pre-positioning	Pre-positioning generally aimed at an attack over the long term, without the end purpose being clearly established (e.g. compromising telecom operator networks, infiltration of mass information internet sites in order to launch an operation of political or economic influence with a strong echo). Sudden and massive compromising of computers in order to form a botnet can be affiliated with this category.
Influence	Operation aimed at diffusing false information or at altering it, mobilizing opinion leaders on the social networks, destroying reputations, disclosing confidential information, degrading the image of an organization or of a State. The end purpose is generally to destabilize or modify perceptions.
Obstacle to functioning	Sabotage operation aimed for example at making an internet site unavailable, causing information saturation, preventing the use of a digital resource, making a physical installation unavailable. Industrial systems can be particularly exposed and vulnerable through IT networks with which they are interconnected (e.g. sending commands in order to generate hardware damage or a breakdown requiring extensive maintenance). Distributed Denial-of-Service attacks (DDoS) are commonly used techniques for neutralizing digital resources.
Lucrative	Operation aiming for a financial gain, either directly or indirectly. Generally linked to organized crime, mention can be made of: fraud on the internet, money laundering, extortion or embezzlement, financial market manipulation, forgery of administrative documents, identify theft, etc. Certain operations for profit can make use of a method of attack that is part of the categories hereinabove (e.g. spying and data theft, ransomware in order to neutralize an activity) but the end purpose remains financial.
Challenge, fun	Operation aimed at fulfilling an exploit for the purposes of social recognition, challenge or simply for fun. Although the objective is primarily for fun and without any particular desire to harm, this type of operation can have serious consequences for the victim.

The difference between a DES and a target objective can be illustrated by the example of a risk source whose aim is to win a deal (DES) that seeks to steal confidential information on negotiations from its competitor (strategic objective). Sometimes the target in question (the desired information) does not ultimately result in the DES.

It can be considered that the value of the target from the risk source's point of view is based on its contribution to the DES.

In very general terms, the risk source's target objectives are divided into two major classes:

— exploiting target resources for its own benefit, e.g. spying, theft, swindling, fraud, trafficking;

— preventing the target from using its resources (confrontation is always relative), e.g. war, terrorism, sabotage, subversion, destabilization.

A.2.4 Event-based approach

A.2.4.1 Ecosystem

In an event-based approach, scenarios should be built by analysing the different paths, relevant for interactions between the organization and interested parties, that all form an ecosystem that risk sources can use to reach the business assets and their DES.

An increasing number of methods of attack use the most vulnerable links in such an ecosystem in order to reach their targets.

The interested parties within the scope of the ISMS that should be taken into consideration when analysing risk scenarios can be of two types:

— external parties, including:

  — clients;

  — partners, co-contractors;

  — service providers (subcontractors, suppliers).

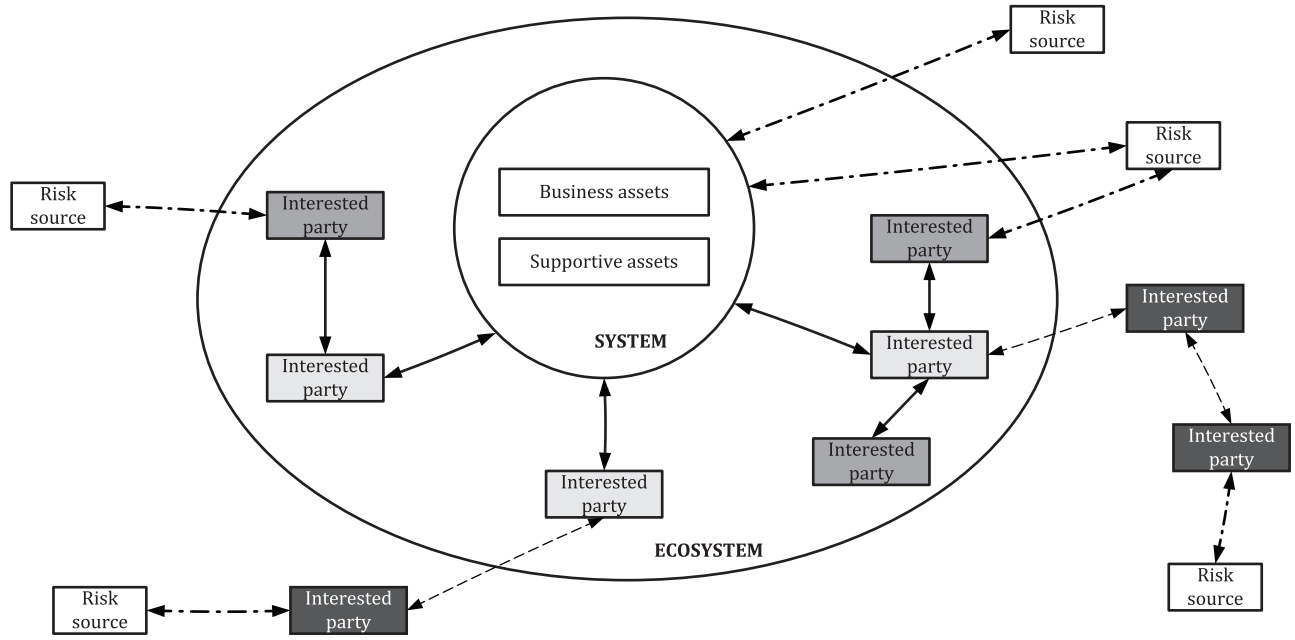
— internal parties, including:

  — technical related service providers (e.g. support services proposed by IT management);

  — business related service providers (e.g. commercial entity using business data);

  — subsidiaries (in particular, located in other countries).

The objective for identification of interested parties is to obtain a clear view of the ecosystem, in order to identify the most vulnerable ones. Ecosystem awareness should be addressed as a preliminary risk study. Figure A.3 shows the identification of interested parties of the ecosystem.



Key

relationship within the ecosystem

relationship that crosses the boundary of ecosystem

relationship within the risk source

internal/external interested party directly connected to the system (1st relationship level)

interested party connected to another interested party (2nd relationship level)

entity out of the ecosystem perimeter

Figure A.3 — Identification of the interested parties of the ecosystem

A.2.4.2 Strategic scenarios

Based on information on risk sources and events concerned, realistic high-level scenarios (strategic scenarios) can be imagined, indicating in what way a risk source can proceed to reach its DES. It can, for example, go through the ecosystem or divert some business processes. These scenarios are identified by deduction, starting from the risk sources and their DES: for each of them, the following questions can be asked, from the standpoint of the risk source:

— What are the organization's business assets that the risk sources must aim for in order to reach their DES?

— In order to make their attack possible or facilitate it, are they likely to attack the critical interested party of the ecosystem that have privileged access to the business assets?

Once the most exposed elements have been identified, the strategic scenario can be drawn, by describing the sequencing of the events generated by the risk source in order to reach its DES. Infringement on the business assets corresponds to ultimate events while the events regarding the ecosystem are intermediate events. The strategic scenario is reflecting a consequence assessment directly inherited from the events concerned.

Those scenarios can be represented in the shape of attack graphs or directly on the ecosystem view of the mapping of the information system by superposing the attack path(s).

Strategic scenarios require additional consideration of the likelihood of the events. The asset-based approach and the associated operational scenarios can be used to define the likelihood of events. The examples of threats presented in A.2.5.1 can be used to obtain necessary assessments.

A.2.5 Asset-based approach

A.2.5.1 Examples of threats

Table A.10 gives examples of typical threats. The list can be used during the threat assessment process. Threats considered as risk sources can be deliberate, accidental or environmental (natural) and can result, for example, in damage or loss of essential services. The list indicates for each threat type where D (deliberate), A (accidental), E (environmental) is relevant. D is used for all deliberate actions aimed at information and assets related to information, A is used for all human actions that can accidentally damage information and assets related to information, and E is used for all incidents that are not based on human actions. The groups of threats are not in priority order.

Controls can mitigate threats by deterring or preventing those threats from acting or occurring. Selection of controls to reduce risk also requires consideration of detective and responsive controls that identify, respond, contain and recover from events. Detective and responsive controls are associated with consequences rather than threats.

EXAMPLE Logging and monitoring enables security event identification and response.

Table A.10 — Examples of typical threats

Category	No.	Threat description	Type of risk source [a]
Physical threats	TP01	Fire	A, D, E
	TP02	Water	A, D, E
	TP03	Pollution, harmful radiation	A, D, E
	TP04	Major accident	A, D, E
	TP05	Explosion	A, D, E
	TP06	Dust, corrosion, freezing	A, D, E
Natural threats	TN01	Climatic phenomenon	E
	TN02	Seismic phenomenon	E
	TN03	Volcanic phenomenon	E
	TN04	Meteorological phenomenon	E
	TN05	Flood	E
	TN06	Pandemic/epidemic phenomenon	E
Infrastructure failures	TI01	Failure of a supply system	A, D
	TI02	Failure of cooling or ventilation system	A, D
	TI03	Loss of power supply	A, D, E
	TI04	Failure of a telecommunications network	A, D, E
	TI05	Failure of telecommunication equipment	A, D
	TI06	Electromagnetic radiation	A, D, E
	TI07	Thermal radiation	A, D, E
	TI08	Electromagnetic pulses	A, D, E
Technical failures	TT01	Failure of device or system	A
	TT02	Saturation of the information system	A, D
	TT03	Violation of information system maintainability	A, D
	TH01	Terror. attack, sabotage	D
	TH02	Social Engineering	D
	TH03	Interception of radiation of a device	D

[a] D = deliberate; A = accidental; E = environmental.

Table A.10 *(continued)*

Category	No.	Threat description	Type of risk source [a]
Human actions	TH04	Remote spying	D
	TH05	Eavesdropping	D
	TH06	Theft of media or documents	D
	TH07	Theft of equipment	D
	TH08	Theft of digital identity or credentials	D
	TH09	Retrieval of recycled or discarded media	D
	TH10	Disclosure of information	A, D
	TH11	Data input from untrustworthy sources	A, D
	TH12	Tampering with hardware	D
	TH13	Tampering with software	A, D
	TH14	Drive-by-exploits using web-based communication	D
	TH15	Replay attack, man-in-the-middle attack	D
	TH16	Unauthorized processing of personal data	A, D
	TH17	Unauthorized entry to facilities	D
	TH18	Unauthorized use of devices	D
	TH19	Incorrect use of devices	A, D
	TH20	Damaging devices or media	A, D
	TH21	Fraudulent copying of software	D
	TH22	Use of counterfeit or copied software	A, D
	TH23	Corruption of data	D
	TH24	Illegal processing of data	D
	TH25	Sending or distributing of malware	A, D, R
	TH26	Position detection	D
Compromise of functions or services	TC01	Error in use	A
	TC02	Abuse of rights or permissions	A, D
	TC03	Forging of rights or permissions	D
	TC04	Denial of actions	D
Organizational threats	TO01	Lack of staff	A, E
	TO02	Lack of resources	A, E
	TO03	Failure of service providers	A, E
	TO04	Violation of laws or regulations	A, D

[a] D = deliberate; A = accidental; E = environmental.

A.2.5.2 Examples of vulnerabilities

Table A.11 gives examples for vulnerabilities in various security areas, including examples of threats that can exploit these vulnerabilities. The lists can provide help during the assessment of threats and vulnerabilities, to determine relevant risk scenarios. In some cases, other threats can exploit these vulnerabilities as well.

Table A.11 — Examples of typical vulnerabilities

Category	No.	Examples of vulnerabilities
Hardware	VH01	Insufficient maintenance/faulty installation of storage media
	VH02	Insufficient periodic replacement schemes for equipment
	VH03	Susceptibility to humidity, dust, soiling
	VH04	Sensitivity to electromagnetic radiation
	VH05	Insufficient configuration change control
	VH06	Susceptibility to voltage variations
	VH07	Susceptibility to temperature variations
	VH08	Unprotected storage
	VH09	Lack of care at disposal
	VH10	Uncontrolled copying
Software	VS01	No or insufficient software testing
	VS02	Well-known flaws in the software
	VS03	No “logout” when leaving the workstation
	VS04	Disposal or reuse of storage media without proper erasure
	VS05	Insufficient configuration of logs for audit trail’s purposes
	VS06	Wrong allocation of access rights
	VS07	Widely-distributed software
	VS08	Applying application programs to the wrong data in terms of time
	VS09	Complicated user interface
	VS10	Insufficient or lack of documentation
	VS11	Incorrect parameter set up
	VS12	Incorrect dates
	VS13	Insufficient identification and authentication mechanisms (e.g. for user authentication)
	VS14	Unprotected password tables
	VS15	Poor password management
	VS16	Unnecessary services enabled
	VS17	Immature or new software
	VS18	Unclear or incomplete specifications for developers
	VS19	Ineffective change control
	VS20	Uncontrolled downloading and use of software
	VS21	Lack of or incomplete back-up copies
	VS22	Failure to produce management reports
Network	VN01	Insufficient mechanisms for the proof of sending or receiving a message
	VN02	Unprotected communication lines
	VN03	Unprotected sensitive traffic
	VN04	Poor joint cabling
	VN05	Single point of failure
	VN06	Ineffective or lack of mechanisms for identification and authentication of sender and receiver
	VN07	Insecure network architecture
	VN08	Transfer of passwords in clear
	VN09	Inadequate network management (resilience of routing)
	VN10	Unprotected public network connections

Table A.11 *(continued)*

Category	No.	Examples of vulnerabilities
Personnel	VP01	Absence of personnel
	VP02	Inadequate recruitment procedures
	VP03	Insufficient security training
	VP04	Incorrect use of software and hardware
	VP05	Poor security awareness
	VP06	Insufficient or lack of monitoring mechanisms
	VP07	Unsupervised work by outside or cleaning staff
	VP08	Ineffective or lack of policies for the correct use of telecommunications media and messaging
Site	VS01	Inadequate or careless use of physical access control to buildings and rooms
	VS02	Location in an area susceptible to flood
	VS03	Unstable power grid
	VS04	Insufficient physical protection of the building, doors and windows
Organization	VO01	Formal procedure for user registration and de-registration not developed, or its implementation is ineffective
	VO02	Formal process for access right review (supervision) not developed, or its implementation is ineffective
	VO03	Insufficient provisions (concerning security) in contracts with customers and/or third parties
	VO04	Procedure of monitoring of information processing facilities not developed, or its implementation is ineffective
	VO05	Audits (supervision) not conducted on a regular basis
	VO06	Procedures of risk identification and assessment not developed, or its implementation is ineffective
	VO07	Insufficient or lack of fault reports recorded in administrator and operator logs
	VO08	Inadequate service maintenance response
	VO09	Insufficient or lack of Service Level Agreement
	VO10	Change control procedure not developed, or its implementation is ineffective
	VO11	Formal procedure for ISMS documentation control not developed, or its implementation is ineffective
	VO12	Formal procedure for ISMS record supervision not developed, or its implementation is ineffective
	VO13	Formal process for authorization of publicly available information not developed, or its implementation is ineffective
	VO14	Improper allocation of information security responsibilities
	VO15	Continuity plans do not exist, or are incomplete, or are outdated
	VO16	E-mail usage policy not developed, or its implementation is ineffective
	VO17	Procedures for introducing software into operational systems not developed, or their implementation is ineffective
	VO18	Procedures for classified information handling not developed, or their implementation is ineffective
	VO19	Information security responsibilities are not present in job descriptions
	VO20	Insufficient or lack of provisions (concerning information security) in contracts with employees
	VO21	Disciplinary process in case of information security incident not defined, or not functioning properly
	VO22	Formal policy on mobile computer usage not developed, or its implementation is ineffective

Table A.11 *(continued)*

Category	No.	Examples of vulnerabilities
	VO23	Insufficient control of off-premise assets
	VO34	Insufficient or lack of "clear desk and clear screen" policy
	VO25	information processing facilities authorization not implemented or not functioning properly
	VO26	Monitoring mechanisms for security breaches not properly implemented
	VO27	Procedures for reporting security weaknesses not developed, or their implementation is ineffective
	VO28	Procedures of provisions compliance with intellectual rights not developed, or their implementation is ineffective

A.2.5.3 Methods for assessment of technical vulnerabilities

Proactive methods such as information system testing can be used to identify vulnerabilities depending on the criticality of the Information and Communications Technology (ICT) system and available resources (e.g. allocated funds, available technology, persons with the expertise to conduct the test). Test methods include:

— automated vulnerability scanning tool;

— security testing and evaluation;

— penetration testing;

— code review.

An automated vulnerability-scanning tool is used to scan a group of hosts or a network for known vulnerable services [e.g. system allows anonymous File Transfer Protocol (FTP), Sendmail relaying]. However, some of the potential vulnerabilities identified by the automated scanning tool do not necessarily represent real vulnerabilities in the context of the system environment (e.g. some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements). Some of the vulnerabilities flagged by the automated scanning software can actually not be vulnerable for a particular site but can be configured that way because their environment requires it. This test method can therefore produce false positives.

Security testing and evaluation (STE) is another technique that can be used in identifying ICT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g. test script, test procedures, and expected test results). The purpose of system security testing is to test the effectiveness of the security controls of an ICT system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.

Penetration testing can be used to complement the review of security controls and ensure that different facets of the ICT system are secured. Penetration testing, when used in the risk assessment process, can be used to assess an ICT system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the ICT system from the viewpoint of a threat source and to identify potential failures in the ICT system protection schemes.

Code review is the most thorough (but also most expensive) way of vulnerability assessment.

The results of these types of security testing help identify a system's vulnerabilities.

Penetration tools and techniques can give false results unless the vulnerability is successfully exploited. To exploit particular vulnerabilities, it is necessary to know the exact system/application/patches setup on the tested system. If those data are not known at the time of testing, it is not necessarily possible to exploit a particular vulnerability successfully (e.g. gaining remote reverse shell). However, it

is still possible to crash or restart a tested process or system. In such a case, the tested object should be considered vulnerable as well.

Methods can include the following activities:

— interview people and users;

— questionnaires;

— physical inspection;

— document analysis.

A.2.5.4 Operational scenarios

In an asset-based approach, operational scenarios can be built by analysing the different paths, within the supporting assets, that risk sources can use to reach the business assets and their DES.

Analysing those scenarios can help digging into the event-based approach.

A successful attack is often the result of exploiting several flaws. Intentional attacks generally follow a sequenced approach. The latter exploits in a coordinated manner several vulnerabilities of an IT, organizational or physical nature. Such an approach based on the simultaneous exploitation of separate flaws can have heavy consequences even though the exploited vulnerabilities can be insignificant when they are considered individually.

The analysed scenarios can be structured according to a typical attack sequence. Several models exist and can be used (e.g. the cyber kill chain model[1)]). The approach should allow identifying the critical supporting assets that can be used as vectors for entry or exploitation or as a propagation relay for the modelled attack.

These scenarios can be represented in the shape of graphs or attack diagrams, useful for representing the attacker's methods of attack.

A.2.6 Examples of scenarios applicable in both approaches

Risk scenarios can be built by using either an event-based approach, an asset-based approach, or both.

Figure A.4 shows risk assessment based on risk scenarios.

1) The cyber kill chain model is the trade name of a product supplied by Lockheed Martin. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named. Equivalent products may be used if they can be shown to lead to the same results.

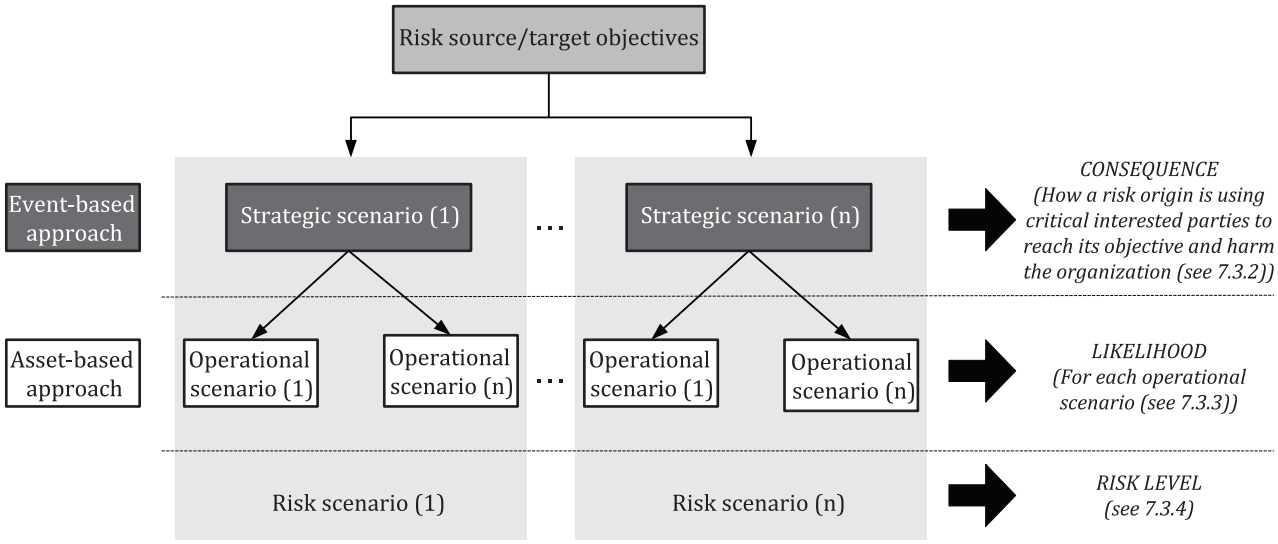


Figure A.4 — Risk assessment based on risk scenarios

Table A.12 shows examples of risk scenarios and the links with the asset/event-based approaches and risk sources.

Table A.12 — Examples of risk scenarios in both approaches

Risk source	**Target objective** **DES**	**Strategic risk scenario** (Event-based approach)	**Operational risk scenario** (Asset-based approach)
Authoritarian state	Acquiring a strategic attack vector	Subverting critical infrastructure	Deploying hidden and persistent malware in the supply chain
Organized crime	Development of illegal activities	Exploitation of port infrastructure	Infiltration of the dockers' union
			Taking control of a computerized flow management system
		Tax carousel fraud	Creating shell companies to carry out fake exchanges on the carbon tax market
		Extortion	Distributing ransomware
Aggressive business	Obtaining a market monopoly	Influencing the regulator	Corrupting a decision-maker
		Removing competitors	Defamation campaign on social networks

A.2.7 Monitoring risk-related events

Monitoring risk-related events is the identification of factors that can influence an information security risk scenario as defined in 10.5.2.

In this context, factors are identified as a set of elements allowing to detect an unexpected behaviour towards a given asset and that can be integrated into the monitoring capabilities and tools of the organization to determine the trigger of an information security risk scenario.

Monitoring risk-related events can be defined using several indicators coming from operational scenarios or strategic scenarios, both introduced in 7.2.1. They can be of different nature (technical, organizational, behavioural, results of audits, etc.). Events are monitored according to defined priorities such as magnitude of consequences and likelihood of the event.

Table A.13 provides an example of an information security risk scenario description with its associated monitoring risk-related events.

Table A.13 — Example of risk scenario and monitoring risk-related events relationship

Risk components	Examples		Events to monitor
Strategic scenario (event based)	Sensitive documents are destroyed by an administrator		
Events concerned	Loss of critical documents		
Severity of consequence	Descriptive measure: high		
Operational scenarios (asset based)	Usage of administrator rights to destroy the sensitive documents by directly accessing the database	- >	Detection of a direct access to the database outside of the normal working hours
	Root access in order to modify the system date/time		
	Malware infection of the administrator workstation with a propagation on the database	- >	Detection of operations impacting a large volume of data (Destruction)
Likelihood	Descriptive measure: medium		
Risk source	Administrator		
Target objective	Compromising of the sensitive document availability		
DES	Compromising of the system		
Security controls	Backup strategy implementation		
	Anti-malware solution		
	NTP implementation		
	OS Hardening		
	Access rights restriction on operational data		

The source-function-destination-trigger (SFDT) model allows to build monitoring risk-related events, where:

— source: indicates where the event/technique is coming from (who and why?) and can be associated to A.2.3 resources;

— function: indicates the type of which event/technique performed by the attacker (what?);

— destination: indicates on what the technique or event is performed (on which primary of support assets?);

— trigger: indicates which conditions allow to detect and identify the risk scenario (results of the attack).

An example of the SFDT model application is presented in Figure A.5.

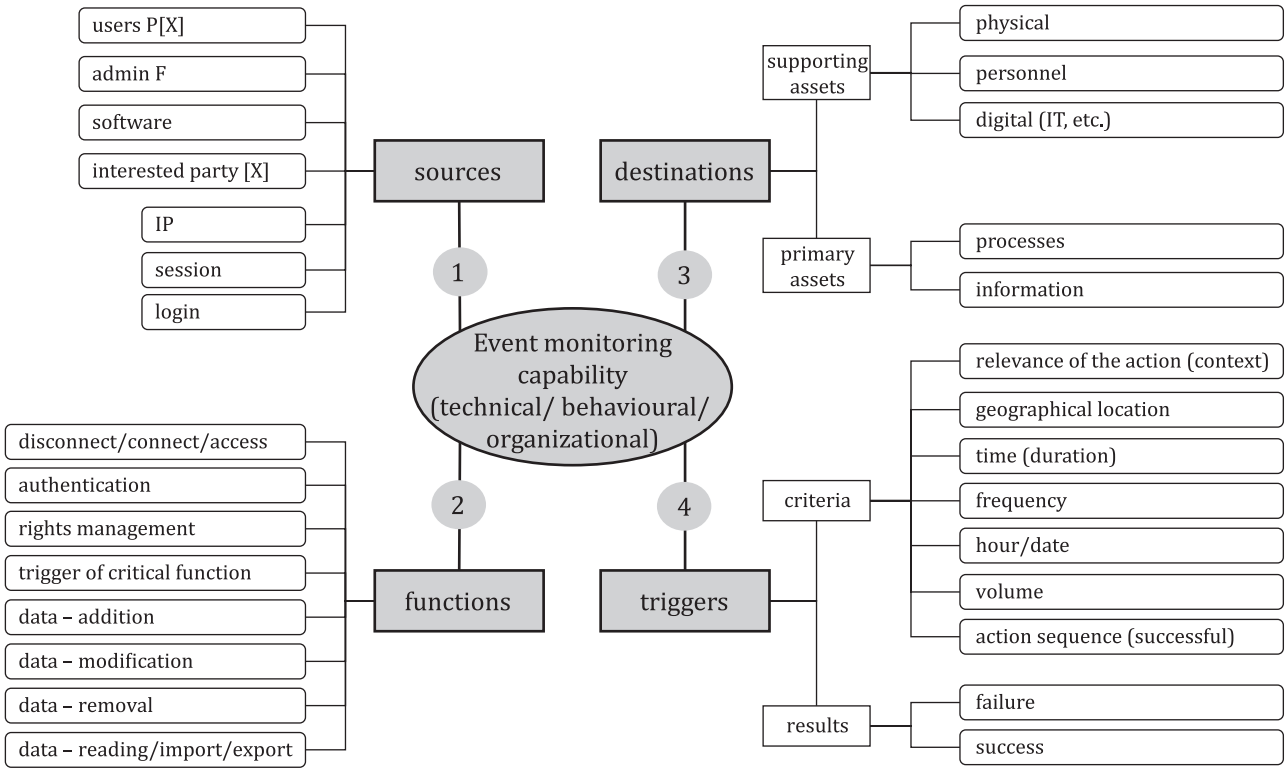


Figure A.5 — Example of SFDT model application

In order to ensure that a monitoring risk-related event is effective and efficient to monitor an information security risk scenario, it is necessary to determine its indicators.

Monitoring risk-related events indicators are:

— risk level of the risk scenario being monitored;

— effectiveness, capability of the risk-related events to monitor a risk scenario;

— efficiency, ratio between true positive alert and false positive, or the cost of the characterization.

Bibliography

[1] ISO 17666:2016, *Space systems — Risk management*

[2] ISO/IEC 27001:2022, *Information technology — Security techniques — Information security management systems — Requirements*

[3] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems — Guidance*

[4] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[5] ISO/IEC 27014, *Information security, cybersecurity and privacy protection — Governance of information security*

[6] ISO/IEC/TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*

[7] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[8] ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[9] ISO 31000:2018, *Risk management — Guidelines*

[10] IEC 31010:2019, *Risk management — Risk assessment techniques*

[11] ISO Guide 73:2009, *Risk management — Vocabulary*

ICS 35.030

Price based on 62 pages