DRAFT International Standard

ISO/IEC DIS 27007

Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

Sécurité de l'information, cybersécurité et protection des données privées — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

ICS: 03.120.20; 35.030

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2026-06-30

Voting terminates on:
2026-09-22

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 27007:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ..... **v**
Introduction ..... **vii**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Principles of auditing **9**
5 Managing an audit programme **9**
5.1 General 9
5.2 Establishing audit programme objectives 9
5.3 Determining and evaluating audit programme risks and opportunities 10
5.4 Establishing audit programme 10
5.4.1 Roles and responsibilities of the individual(s) managing the audit programme 10
5.4.2 Competence of individual(s) managing audit programme 10
5.4.3 Establishing extent of audit programme 10
5.4.4 Determining audit programme resources 10
5.5 Implementing audit programme 11
5.5.1 General 11
5.5.2 Defining the objectives, scope and criteria for an individual audit 11
5.5.3 Selecting and determining audit methods 11
5.5.4 Selecting audit team members 12
5.5.5 Assigning responsibility for an individual audit to the audit team leader 12
5.5.6 Managing audit programme results 12
5.5.7 Managing and maintaining audit programme records 12
5.6 Monitoring audit programme 12
5.7 Reviewing and improving audit programme 12
6 Conducting an audit **12**
6.1 General 12
6.2 Initiating audit 12
6.2.1 General 12
6.2.2 Establishing contact with auditee 12
6.2.3 Determining feasibility of audit 12
6.3 Preparing audit activities 13
6.3.1 Performing review of documented information 13
6.3.2 Audit planning 13
6.3.3 Assigning work to audit team 13
6.3.4 Preparing documented information for audit 13
6.4 Conducting audit activities 13
6.4.1 General 13
6.4.2 Assigning roles and responsibilities of guides and observers 13
6.4.3 Conducting opening meeting 13
6.4.4 Communicating during audit 13
6.4.5 Audit information availability and access 14
6.4.6 Reviewing documented information while conducting audit 14
6.4.7 Collecting and verifying information 14
6.4.8 Generating audit findings 14
6.4.9 Determining audit conclusions 14
6.4.10 Conducting closing meeting 14
6.5 Preparing and distributing audit report 14
6.5.1 Preparing audit report 14
6.5.2 Distributing audit report 15
6.6 Completing audit 15
6.7 Conducting audit follow-up 15

© ISO/IEC 2026 – All rights reserved

7 Competence and evaluation of auditors **15**
7.1 General 15
7.2 Determining auditor competence 15
7.2.1 General 15
7.2.2 Personal behaviour 15
7.2.3 Knowledge and skills 15
7.2.4 Achieving auditor competence 16
7.2.5 Achieving audit team leader competence 16
7.3 Establishing auditor evaluation criteria 16
7.4 Selecting appropriate auditor evaluation method 16
7.5 Conducting auditor evaluation 16
7.6 Maintaining and improving auditor competence 16
Annex A (informative) **Guidance for ISMS auditing practice** **17**
Bibliography **48**

© ISO/IEC 2026 – All rights reserved

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).

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 http://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.

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 27007:2020), which has been technically revised.

The main changes compared to the previous edition are as follows:

— the document has been aligned with ISO/FDIS 19011 and ISO/IEC 27001:2022/Amd 1:2024 ;

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.

[Editor's Note: During preparation of the DIS draft, an exchange with the ISO editor regarding the reference to ISO/IEC 27001 vs. ISO/IEC 27001:2022 vs. ISO/IEC 27001:2022 Amd1 and regarding if this is a normative or bibliographic reference happend. As can be seen in ISO/IEC 27003 CD2, several references can be done in parallel.

If ISO/IEC 27001 is referenced in general, no year is given. If we reference explicit clauses except Clause 4, then a reference to ISO/IEC 27001:2022 is correct. Only if we reference Clause 4, we need to cite Amd1.

In the current draft, the first distinction (no year vs. year) is already implemented, the second one (citing the Amd1 version explicitly) will be implemented during the implementation of the FDIS draft, to enable NBs input, if necessary (see also 2nd issue). NBs are kindly requested to review if any undated clause should be dated and vice versa and report this in their DIS ballot. The Clause 4 reference (using Amd1) is mechancial and will performed by the Editors for the FDIS draft.

*The ISO editor also pointed out, that ISO/IEC 27007 is a guideline standard and that according to the **ISO/IEC Directives, Part 2, 15.5.3**: "Only references cited in the text in such a way that some or all of their content constitutes requirements of the document shall be listed in the Normative references clause." the refererences to ISO/IEC 27001 should in the bibliography. However, to use Annex A you cannot do without ISO/IEC 27001, it is "indispensable for use". And this is implemented in ISO/IEC 27003 as well. In light of this, NBs are kindly requrested to review where they think the reference should be pointed to. The Editors will then review this with the ISO editors and determine the final placement for the FDIS draft.*

© ISO/IEC 2026 – All rights reserved

Aditionally, the OSD internal reference is currently incorrect for both ISO/IEC 27001 and ISO 19011. This will be handled automatically by the Editors for the FDIS draft as well.]

© ISO/IEC 2026 – All rights reserved

Introduction

An information security management system (ISMS) audit can be conducted against a range of audit criteria, separately or in combination, including but not limited to:

— requirements defined in ISO/IEC 27001:2022/Amd 1:2024;

— policies and requirements specified by relevant interested parties;

— statutory and regulatory requirements;

— ISMS processes and controls defined by the organization or other parties;

— management system plan(s) relating to the provision of specific outputs of an ISMS (e.g. plans to address risks and opportunities when establishing ISMS, plans to achieve information security objectives, risk treatment plans, project plans).

This document provides guidance for all sizes and types of organizations and ISMS audits of varying scopes and scales, including those conducted by large audit teams, typically of larger organizations, and those by single auditors, whether in large or small organizations. This guidance should be adapted as appropriate to the scope, complexity and scale of the ISMS audit programme.

This document concentrates on ISMS internal audits (first party) and ISMS audits conducted by organizations on their external providers and other external interested parties (second party).

Some of the guidance in this document is not appropriate for a third-party management system certification audit. This is because the scope and audit criteria for such audits are typically limited to requirements defined in ISO/IEC 27001:2022.

Also, because a third-party management system certification is a conformity assessment, the requirements of ISO/IEC 27006-1 [1] and ISO/IEC 17021-1:2015 [2] apply to all third-party ISMS certification audits, particularly regarding the process for raising findings during certification audits.

Third-party audits are not limited to the requirements in ISO/IEC 27001:2022/Amd 1:2024 as the criteria include the organisations own ISMS requirements and often, contractually, some of the CABs rules (i.e. for use of logos and marks).

This document is to be used in conjunction with the guidance contained in ISO/FDIS 19011.

This document follows the structure of ISO/FDIS 19011.

ISO/FDIS 19011 provides guidance on the management of audit programmes, the conduct of internal or external audits of management systems, as well as on the competence and evaluation of management system auditors.

Annex A provides guidance for ISMS auditing practices along with requirements of ISO/IEC 27001:2022, Clauses 4 to 10.

© ISO/IEC 2026 – All rights reserved

Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

1 Scope

This document provides guidance on managing an information security management system (ISMS) audit programme, on conducting audits, and on the competence of ISMS auditors, in addition to the guidance contained in ISO/FDIS 19011.

This document is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.

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/FDIS 19011, *Guidelines for auditing management systems*

ISO/IEC 27001:2022/Amd 1:2024, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements — Amendment 1: Climate action changes*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/FDIS 19011 apply.

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

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

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

perfluous, as the term is used in its dictionary definition in this document.]

3.1
authenticity
property that an entity is what it claims to be

[SOURCE: ISO/IEC 27002:2022 [3], 3.1.5]

3.2
availability
property of being accessible and usable on demand by an authorized entity

3.3
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or *processes* (3.34)

© ISO/IEC 2026 – All rights reserved

3.4
consequence
outcome of an *event* (3.11) affecting *objectives* (3.29)

Note 1 to entry: An *event* (3.11) can lead to a range of consequences.

Note 2 to entry: A consequence can be certain or uncertain and, in the context of *information security* (3.14), is usually negative.

Note 3 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 4 to entry: Initial consequences can escalate through knock-on effects.

[SOURCE: ISO Guide 31000:2018, 3.6, modified — Note 1to entry has been added, Note 2 and 4 to entry have been modified.]

3.5
continual improvement
recurring activity to enhance *performance* (3.31)

3.6
control
measure (3.24) that is modifying *risk* (3.39)

Note 1 to entry: Controls include any *process* (3.34), *policy* (3.33), device, practice, or other actions which modify *risk* (3.39).

Note 2 to entry: It is possible that controls not always exert the intended or assumed modifying effect.

Note 3 to entry: The definition from ISO/IEC 27005 is wider than this definition.

[SOURCE: ISO/IEC 27000:2018, 3.14 — Note 3to entry has been added.]

3.7
correction
action to eliminate a detected nonconformity

3.8
corrective action
action to eliminate the cause of a nonconformity and to prevent recurrence

3.9
documented information
information required to be controlled and maintained by an *organization* (3.30) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media and from any source.

Note 2 to entry: Documented information can refer to

— the *management system* (3.24), including related *processes* (3.34);

— information created in order for the *organization* (3.30) to operate (documentation);

— evidence of results achieved (records).

3.10
event
occurrence or change of a particular set of circumstances

Note 1 to entry: An event can be one or more occurrences, and can have several causes.

Note 2 to entry: An event can consist of something not happening.

Note 3 to entry: An event can sometimes be referred to as an “incident” or “accident”.

© ISO/IEC 2026 – All rights reserved

Note 4 to entry: This definition aligns with the definition used in ISO/IEC 27001:2022.

[SOURCE: ISO/IEC 27005:2022, 3.1.11, modified - Notes to entry changed and Note 3 and 4 to entry added.]

3.11
external context
external environment in which the *organization* (3.30) seeks to achieve its *objectives* (3.29)

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

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

— key drivers and trends having impact on the *objectives* (3.29) of the *organization* (3.30);

— relationships with, and perceptions and values of, external *stakeholders* (3.19).

Note 2 to entry: This definition aligns with the definition used in ISO/IEC 27001:2022.

[SOURCE: ISO/IEC 27005:2022, 3.1.1 modified — Note 1 to entry has been modified, Note 2 to entry added]

3.12
information need
insight necessary to manage *objectives* (3.29), goals, *risks* (3.39) and problems

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.12]

3.13
information processing facility
any information processing system, service or infrastructure, or the physical location housing it

[SOURCE: ISO/IEC 27002:2022, 3.1.12]

3.14
information security
preservation of *confidentiality* (3.3), *integrity* (3.19) and *availability* (3.2) of information

Note 1 to entry: In addition, other properties, such as *authenticity* (3.1), accountability, *non-repudiation* (3.28), and *reliability* (3.35) can also be involved.

3.15
information security event
identified occurrence of a system, service or network state indicating a possible breach of *information security* (3.15)*policy* (3.33) or failure of *controls* (3.6), or a previously unknown situation that can be security relevant

3.16
information security incident
single or a series of unwanted or unexpected *information security events* (3.16) that have a significant probability of compromising business operations and threatening *information security* (3.15)

ISO/IEC 27005:2022, 3.1.12

3.17
information system
set of applications, services, information technology assets, or other information-handling components

[SOURCE: ISO/IEC 27002:2022 [3], 3.1.17]

3.18
integrity
property of accuracy and completeness

© ISO/IEC 2026 – All rights reserved

3.19
interested party (preferred term)
stakeholder (admitted term)
person or *organization* (3.30) that can affect, be affected by, or perceive itself to be affected by a decision or activity

[SOURCE: ISO/IEC 27002:2022 [3], 3.1.18]

3.20
internal context
internal environment in which the *organization* (3.30) seeks to achieve its *objectives* (3.29)

Note 1 to entry: Internal context can include:

— governance, organizational structure, roles and accountabilities;

— policies (3.32), *objectives* (3.29), and the strategies that are in place to achieve them;

— the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, *processes* (3.34), systems and technologies);

— *information systems* (3.18), information flows and decision-making *processes* (3.34) (both formal and informal);

— relationships with, and perceptions and values of, internal *stakeholders* (3.19);

— the *organization* (3.29)'s culture;

— standards, guidelines and models adopted by the *organization* (3.30);

— form and extent of contractual relationships.

Note 2 to entry: This definition aligns with the definition used in ISO/IEC 27001:2022.

[SOURCE: ISO/IEC 27005:2022, 3.1.2 modified — Note 1 to entry has been modified, Note 2 to entry added]

3.21
level of risk
magnitude of a *risk* (3.39) expressed in terms of the combination of *consequences* (3.4) and their *likelihood* (3.23)

Note 1 to entry: The definition from ISO/IEC 27005 replaces "magnitude" by "significance".

[SOURCE: ISO/IEC 27000:2018, 3.39, modified — Note 1 to entry added.]

3.22
likelihood
chance of something happening

Note 1 to entry: This definition aligns with the definition used in ISO/IEC 27001:2022.

[SOURCE: ISO/IEC 27005:2022, 3.1.13, modified — Notes to entry have been deleted, Note 1 to entry added.]

3.23
management system
set of interrelated or interacting elements of an *organization* (3.30) to establish policies (3.53) and *objectives* (3.29) and *processes* (3.34) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the *organization* (3.29)'s structure, roles and responsibilities, planning and operation.

Note 3 to entry: The scope of a management system may include the whole of the *organization* (3.30), specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

© ISO/IEC 2026 – All rights reserved

[Editor's Note: This is a modified version of the definition from Annex SL of the directives as presented in ISO/IEC 27000:2018. As ISO/IEC 27001:2022 uses this term, it is for now included here. Experts and national bodies are kindly requested to review the situation and provide input on how to handle this term, preferably including the current policy of terms (TMB resolution 68/2005) and noting, that ISO/IEC 27007 is a type B management system standard.]

3.24
measure
variable to which a value is assigned as the result of *measurement* (3.26)

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.15, modified — Note 2 to entry has been deleted.]

3.25
measurement
process (3.34) to determine a value

3.26
monitoring
determining the status of a system, a *process* (3.34) or an activity

Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.

3.27
non-repudiation
ability to prove the occurrence of a claimed *event* (3.11) or action and its originating entities

[SOURCE: ISO/IEC 27002:2022 [3], 3.1.19]

3.28
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels [such as strategic, *organization* (3.29)-wide, project, product and *process* (3.34)].

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an *information security* (3.14) objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of information security management systems, *information security* (3.14) objectives are set by the *organization* (3.30), consistent with the information security policy, to achieve specific results.

3.29
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.29)

Note 1 to entry: The concept of organization includes but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

3.30
outsource
make an arrangement where an external *organization* (3.30) performs part of an organization's function or *process* (3.34)

Note 1 to entry: An external *organization* (3.30) is outside the scope of the *management system* (3.24), although the outsourced function or *process* (3.34) is within the scope.

© ISO/IEC 2026 – All rights reserved

3.31
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the management of activities, *processes* (3.34), products (including services), systems or *organizations* (3.30).

3.32
policy
intentions and direction of an *organization* (3.30), as formally expressed by its *top management* (3.51)

[SOURCE: ISO/IEC 27002:2022 [3], 3.1.24]

3.33
process
set of interrelated or interacting activities which transforms inputs into outputs

3.34
reliability
property of consistent intended behaviour and results

[SOURCE: ISO/IEC 27002:2022 [3], 3.1.31]

3.35
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.30) and *interested parties* (3.20) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, for example in *documented information* (3.10).

3.36
residual risk
risk (3.39) remaining after *risk treatment* (3.49)

Note 1 to entry: Residual risk can contain unidentified *risk* (3.39).

Note 2 to entry: Residual risk can also be referred to as "retained risk".

[SOURCE: ISO/IEC 27005:2022, 3.1.17]

3.37
review
activity undertaken to determine the suitability, adequacy and effectiveness (3.19) of the subject matter to achieve established *objectives* (3.29)

[SOURCE: ISO/IEC 27000:2018, 3.58]

3.38
risk
effect of uncertainty on *objectives* (3.29)

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

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an *event* (3.11), its *consequence* (3.4), or *likelihood* (3.23).

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

© ISO/IEC 2026 – All rights reserved

Note 4 to entry: Risk is often expressed in terms of a combination of the *consequences* (3.4) of an *event* (3.11) (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

Note 5 to entry: In the context of information security management systems, *information security* (3.14) risks can be expressed as effect of uncertainty on information security objectives.

Note 6 to entry: *information security* (3.14) risk is associated with the potential that *threats* (3.50) will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an *organization* (3.30).

This definition aligns with the definition used in ISO/IEC 27001:2022.

[SOURCE: ISO/IEC 27005:2022, 3.1.3 - Notes to entry modified.]

3.39
risk acceptance
informed decision to take a particular *risk* (3.39)

Note 1 to entry: Risk acceptance can occur without *risk treatment* (3.49) or during the *process* (3.34) of *risk treatment* (3.48).

Note 2 to entry: Accepted *risks* (3.39) are subject to *monitoring* (3.27) and *review* (3.38).

[SOURCE: ISO/IEC 27005:2022, 3.2.8]

3.40
risk analysis
process (3.34) to comprehend the nature of *risk* (3.39) and to determine the *level of risk* (3.22)

Note 1 to entry: Risk analysis provides the basis for *risk evaluation* (3.44) and decisions about *risk treatment* (3.49).

Note 2 to entry: Risk analysis includes *risk* (3.38) estimation.

[SOURCE: ISO/IEC 27005:2022, 3.2.5]

3.41
risk assessment
overall *process* (3.34) of *risk identification* (3.45), *risk analysis* (3.41) and *risk evaluation* (3.44)

[SOURCE: ISO/IEC 27005:2022, 3.2.3]

3.42
risk criteria
terms of reference against which the significance of *risk* (3.39) is evaluated

Note 1 to entry: Risk criteria are based on organizational *objectives* (3.29), and *external context* (3.12) and *internal context* (3.21).

Note 2 to entry: Risk criteria can be derived from standards, laws, policies (3.53) and other *requirements* (3.36).

[SOURCE: ISO/IEC 27005:2022, 3.1.7]

3.43
risk evaluation
process (3.34) of comparing the results of *risk analysis* (3.41) with *risk criteria* (3.43) to determine whether the *risk* (3.39) and/or its magnitude is acceptable or tolerable

Note 1 to entry: Risk evaluation assists in the decision about *risk treatment* (3.49).

Note 2 to entry: This definition aligns with the definition used in ISO/IEC 27001:2022.

[SOURCE: ISO/IEC 27005:2022, 3.2.6 modified — "magnitude" has replaced "significance" and Note 2 to enry added.]

© ISO/IEC 2026 – All rights reserved

3.44
risk identification
process (3.34) of finding, recognizing and describing *risks* (3.39)

Note 1 to entry: Risk identification involves the identification of *risk* (3.38) sources, *events* (3.11), their causes and their potential *consequences* (3.4).

Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and *stakeholders* (3.19)' needs.

Note 3 to entry: This definition aligns with the definition used in ISO/IEC 27001:2022.

[SOURCE: ISO/IEC 27005:2022, 3.2.4 , modified — "stakeholder" has replaced "interested party" in Note 2 to entry and Note 3 to entry added.]

3.45
risk management
coordinated activities to direct and control an *organization* (3.30) with regard to *risk* (3.39)

[SOURCE: ISO/IEC 27000:2018, 3.69]

3.46
risk management process
systematic application of management policies (3.53), procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, *monitoring* (3.27) and reviewing *risk* (3.39)

Note 1 to entry: ISO/IEC 27005 [4] uses the term *"process"* (3.34) to describe *risk management* (3.46) overall. The elements within the risk management process are referred to as "activities".

[SOURCE: IISO/IEC 27000:2018, 3.70]

3.47
risk owner
person or entity with the accountability and authority to manage a *risk* (3.39)

[SOURCE: ISO/IEC 27005:2022, 3.1.5]

3.48
risk treatment
process (3.34) to modify *risk* (3.39)

Note 1 to entry: Risk treatment can involve:

— avoiding the *risk* (3.39) by deciding not to start or continue with the activity that gives rise to the risk;

— taking or increasing *risk* (3.39) in order to pursue an opportunity;

— removing the *risk* (3.38) source;

— changing the *likelihood* (3.23);

— changing the *consequences* (3.4);

— sharing the *risk* (3.39) with another party or parties (including contracts and *risk* (3.38) financing);

— retaining the *risk* (3.39) by informed choice.

Note 2 to entry: Risk treatment that deal with negative *consequences* (3.4) are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

Note 3 to entry: Risk treatment can create new *risks* (3.39) or modify existing risks.

Note 4 to entry: This definition aligns with the definition used in ISO/IEC 27001:2022.

© ISO/IEC 2026 – All rights reserved

[SOURCE: ISO/IEC 27005:2022, 3.2.7, modified — Note 2 to entry removed, Note 4 to entry added.]

3.49
threat
potential cause of an unwanted incident, which can result in harm to a system or *organization* (3.30)

Note 1 to entry: The definition in ISO/IEC 27005:2022 is slightly different.

[SOURCE: ISO/IEC 27002:2022 [3], 3.1.34 modified - Note to entry added]

3.50
top management
person or group of people who directs and controls an *organization* (3.30) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the *organization* (3.30).

Note 2 to entry: If the scope of the *management system* (3.24) covers only part of an *organization* (3.30), then top management refers to those who direct and control that part of the organization.

Note 3 to entry: Top management is sometimes called executive management and can include Chief Executive Officers, Chief Financial Officers, Chief Information Officers, and similar roles.

4 Principles of auditing

The principles of auditing of ISO 19011:202x, Clause 4, apply.

5 Managing an audit programme

5.1 General

The guidelines of ISO 19011:202x, 5.1, apply.

5.2 Establishing audit programme objectives

5.2.1 The guidelines of ISO 19011:202x, 5.2, apply. In addition, the guidance in 5.2.2 applies.

5.2.2 ISMS-specific considerations for determining audit[1)] programme objectives can include:

a) identified information security requirements;

b) requirements of ISO/IEC 27001:2022/Amd 1:2024 ;

c) auditee's level of performance, as reflected in the occurrence of information security events and incidents and effectiveness of the ISMS;

NOTE Further information about performance monitoring, measurement, analysis and evaluation can be found in ISO/IEC 27004 [5].

d) information security risks to the relevant parties, i.e. the auditee and audit client;

e) Any additional control frameworks used by the ISMS – for example, ISO/IEC 27017, ISO/IEC 27018 or regional or national standards.

Examples of ISMS-specific audit programme objectives include:

— demonstrate conformity with all relevant legal and contractual requirements and other requirements and their security implications;

1) For the purpose of this document, the term "audit" refers to ISMS audits.

© ISO/IEC 2026 – All rights reserved