International Standard

Redline version
compares Sixth edition
to Fifth edition



ISO/IEC 27000

Information security, cybersecurity and privacy protection — Information security management systems — Overview

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Vue d'ensemble

Reference number
ISO/IEC 27000:redline:2026(en)

© ISO/IEC 2026

INFORMATION ON THIS REDLINE VERSION

This document is a **Redline version** published for information purposes. It is intended to assist users in identifying the changes introduced in comparison with the previous edition of the standard.

Additions are highlighted in green. Deletions are indicated by red strikethrough.

For graphics, additions are identified by a green frame, and deletions are indicated by a red cross.

Clause and heading numbers that include modifications are highlighted in yellow in the Table of Contents.

This Redline version is not an official ISO Standard and does not replace the current published edition. Only the current edition of the International Standard is to be regarded as the official document.

Markup used in this Redline version

Text example 1	added text (green highlight)
~~Text example 2~~	deleted text (red strike through)
	added graphics (green frame)
	deleted graphics (red cross)
1.x ...	modified clause and heading numbers (yellow in the Table of Contents)



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 ... **vi**

Introduction ... **viii**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

~~**4 Information security management systems** ... **12**~~

~~4.1 General~~ ... 12

4 Concepts and principles ... **12**

~~4.2 What is an ISMS?~~ ... 12

4.1 Concepts ... 12

~~4.2.1 Overview and principles~~ ... 12

4.1.1 The need for information security ... 13

~~4.2.2~~ 4.1.2 Information ... 13

~~4.2.3~~ 4.1.3 Information security ... 14

~~4.2.4 Management~~ ... 14

4.1.4 Constantly changing risks ... 14

4.1.5 Risk treatment plan ... 14

~~4.2.5 Management system~~ ... 15

4.1.6 Purpose of an information security management system (ISMS) ... 15

4.1.7 Importance of an ISMS ... 15

4.1.8 Process approach ... 16

4.1.9 Scope ... 16

~~4.3 Process approach~~ ... 16

~~4.4 Why an ISMS is important~~ ... 16

~~4.5 Establishing, monitoring, maintaining and improving an ISMS~~ ... 17

4.2 Principles ... 17

~~4.5.1 Overview~~ ... 17

4.2.1 Establishing, implementing, maintaining and improving an ISMS ... 17

4.2.2 Successfully implementing an ISMS ... 18

~~4.5.2~~ 4.2.3 ~~Identifying~~ Determining information security requirements ... 18

~~4.5.3 Assessing information security risks~~ ... 18

~~4.5.4 Treating information security risks~~ ... 19

~~4.5.5 Selecting and implementing controls~~ ... 19

4.2.4 Integration into business processes ... 20

~~4.5.6 Monitor, maintain and improve the effectiveness of the ISMS~~ ... 20

~~4.5.7 Continual improvement~~ ... 20

© ISO/IEC 2026 – All rights reserved

4.6 ISMS critical success factors 21
4.7 Benefits of the ISMS family of standards 21

5 ISMS family of standards 22
5.1 General information 22
5.2 Standard describing an overview and terminology: ISO/IEC 27000 (this document) 22
5.3 Standards specifying requirements 23
5.3.1 ISO/IEC 27001 23
5.3.2 ISO/IEC 27006 23
5.3.3 ISO/IEC 27009 23

5 Documents related to ISMS including ISO/IEC 27001 26
5.4 Standards describing general guidelines 24
5.4.1 ISO/IEC 27002 24
5.4.2 ISO/IEC 27003 24
5.4.3 ISO/IEC 27004 24
5.4.4 ISO/IEC 27005 24
5.4.5 ISO/IEC 27007 24
5.4.6 ISO/IEC TR 27008 25
5.4.7 ISO/IEC 27013 25
5.4.8 ISO/IEC 27014 25
5.4.9 ISO/IEC TR 27016 25
5.4.10 ISO/IEC 27021 26
5.1 General 26
5.2 ISO/IEC 27001 (specification of an ISMS) 27
5.5 Standards describing sector-specific guidelines 27
5.3 Candidate necessary information security controls 27
5.3.1 ISO/IEC 27002 (information security controls) 27
5.5.1 5.3.2 ISO/IEC 27010 (inter-sector and inter-organizational communications) 27
5.5.2 5.3.3 ISO/IEC 27011 (telecommunications organizations) 27
5.5.3 5.3.4 ISO/IEC 27017 (cloud services) 28
5.5.4 ISO/IEC 27018 28
5.5.5 ISO/IEC 27019 28
5.5.6 ISO 27799 29
5.3.5 ISO/IEC 27019 (energy utility industry) 29
5.4 Fulfilment of ISMS requirements 29
5.4.1 ISO/IEC 27003 (ISMS guidance) 29
5.4.2 ISO/IEC 27004 (monitoring, measurement, analysis and evaluation) 29
5.4.3 ISO/IEC 27005 (guidance on managing information security risks) 29
5.4.4 ISO/IEC 27007 (ISMS auditing) 30

© ISO/IEC 2026 – All rights reserved

5.5 Use of ISMS 30
5.5.1 ISO/IEC 27013 (integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1) 30
5.5.2 ISO/IEC 27014 (governance of information security) 30
5.5.3 ISO/IEC TR 27016 (organizational economics) 30
5.6 Control assessment, attributes, processes and competence 30
5.6.1 ISO/IEC TS 27008 (assessment of information security controls) 30
5.6.2 ISO/IEC 27021 (competence requirements for ISMS professionals) 30
5.6.3 ISO/IEC TS 27022 (ISMS processes) 30
5.6.4 ISO/IEC 27028 (ISO/IEC 27002 attributes) 30
5.7 ISO/IEC 27006-1 (Conformity assessment) 30
5.8 Relationships between the standards 31

Bibliography 32

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) ~~is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International~~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. ~~ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.~~

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ~~ISO documents~~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 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).~~

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

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation ~~on~~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 ~~the following URL: www.iso.org/iso/foreword.html~~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~~ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, ~~*IT Security techniques*~~*Information security, cybersecurity and privacy protection*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13, *Cybersecurity and data protection*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This ~~fifth~~sixth edition cancels and replaces the ~~fourth~~fifth edition (ISO/IEC 27000:~~2016~~2018), which has been technically revised. ~~The main changes compared to the previous edition are as follows:~~

The main changes are as follows:

— the ~~Introduction~~title has been ~~reworded~~modified;

~~— some terms and definitions have been removed;~~

— the structure of the document has been changed to stress its primary role, which is to provide an overview of, and explain the relationships between, documents related to ISMS (information security management systems) including ISO/IEC 27001;

© ISO/IEC 2026 – All rights reserved

— text presenting the concepts and principles of information security and information security management systems has been added;

— Clause 3 has been ~~aligned on the high-level structure for MSS~~modified to only contain definitions for those terms used in presenting the concepts and principles described in this document;

~~— Clause 5 has been updated to reflect the changes in the standards concerned;~~

~~— Annexes A and B have been deleted.~~

— it is no longer a terminology document.

This document has been given the status of a horizontal document in accordance with the ISO/IEC Directives, Part 1.

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.

© ISO/IEC 2026 – All rights reserved

Introduction

0.1 Overview

International Standards for management systems provide a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art. ISO/IEC JTC 1/SC 27 maintains an expert committee dedicated to the development of international management systems standards for information security, otherwise known as the Information Security Management system (ISMS) family of standards.

Through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets, including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information.

0.2 Purpose of this document

The ISMS family of standards includes standards that:

a) define requirements for an ISMS and for those certifying such systems;

b) provide direct support, detailed guidance and/or interpretation for the overall process to establish, implement, maintain, and improve an ISMS;

c) address sector-specific guidelines for ISMS; and

d) address conformity assessment for ISMS.

0.3 Content of this document

In this document, the following verbal forms are used:

— "shall" indicates a requirement;

— "should" indicates a recommendation;

— "may" indicates a permission;

— "can" indicates a possibility or a capability.

Information marked as "NOTE" is for guidance in understanding or clarifying the associated requirement. "Notes to entry" used in Clause 3 provide additional information that supplements the terminological data and can contain provisions relating to the use of a term.

This document explains the concepts and principles that underpin information security and information security management systems. It provides an overview of all documents related to ISMS (information security management systems) including ISO/IEC 27001 and explains the relationship between them.

© ISO/IEC 2026 – All rights reserved

Information security, cybersecurity and privacy protection — Information security management systems — Overview

1 Scope

~~This document provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).~~

~~The terms and definitions provided in this document~~

~~— cover commonly used terms and definitions in the ISMS family of standards;~~

~~— do not cover all terms and definitions applied within the ISMS family of standards; and~~

~~— do not limit the ISMS family of standards in defining new terms for use.~~

This document gives an overview of the concepts and principles used in the documents related to information security management systems (ISMS), including ISO/IEC 27001.

This document is considered to be a horizontal document as it provides an explanation of the concepts and principles that underpin information security and ISMS.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain ~~terminological~~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**~~
~~**access control**~~
~~means to ensure that access to assets is authorized and restricted based on business and security *requirements* (3.56)~~

~~**3.2**~~
~~**attack**~~
~~attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset~~

© ISO/IEC 2026 – All rights reserved

~~3.3~~
3.1
~~audit~~
information security
~~systematic, independent and documented *process* (3.54) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled~~

~~Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).~~

~~Note 2 to entry: An internal audit is conducted by the organization itself, or by an external party on its behalf.~~

~~Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.~~

preservation of *confidentiality* (3.2), *integrity* (3.3) and *availability* (3.4) of information

~~3.4~~
~~audit scope~~
~~extent and boundaries of an *audit* (3.3)~~

~~[SOURCE: ISO 19011:2011, 3.14, modified — Note 1 to entry has been deleted.]~~

~~3.5~~
~~authentication~~
~~provision of assurance that a claimed characteristic of an entity is correct~~

~~3.6~~
~~authenticity~~
~~property that an entity is what it claims to be~~

~~3.7~~
~~availability~~
~~property of being accessible and usable on demand by an authorized entity~~

~~3.8~~
~~base measure~~
~~*measure* (3.42) defined in terms of an attribute and the method for quantifying it~~

~~Note 1 to entry: A base measure is functionally independent of other *measures*.~~

~~[SOURCE: ISO/IEC/IEEE 15939:2017, 3.3, modified — Note 2 to entry has been deleted.]~~

~~3.9~~
~~competence~~
~~ability to apply knowledge and skills to achieve intended results~~

~~3.10~~
3.2
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or ~~*processes* (3.54)~~ processes

~~3.11~~
3.3
~~conformity~~
integrity
~~fulfilment of a *requirement* (3.56)~~

property of accuracy and completeness

© ISO/IEC 2026 – All rights reserved

3.12
consequence
outcome of an *event* (3.21) affecting *objectives* (3.49)

Note 1 to entry: An event 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, 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 73:2009, 3.6.1.3, modified — Note 2 to entry has been changed after "and".]

3.13
continual improvement
recurring activity to enhance *performance* (3.52)

3.14
control
measure that is modifying *risk* (3.61)

Note 1 to entry: Controls include any *process* (3.54), *policy* (3.53), device, practice, or other actions which modify *risk* (3.61).

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

[SOURCE: ISO Guide 73:2009, 3.8.1.1 — Note 2 to entry has been changed.]

3.15
control objective
statement describing what is to be achieved as a result of implementing *controls* (3.14)

3.16
correction
action to eliminate a detected *nonconformity* (3.47)

3.17
corrective action
action to eliminate the cause of a *nonconformity* (3.47) and to prevent recurrence

3.18
derived measure
measure (3.42) that is defined as a function of two or more values of *base measures* (3.8)

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.8, modified — Note 1 to entry has been deleted.]

3.19
3.4
documented information
availability
information required to be controlled and maintained by an *organization* (3.50) 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* (3.41), including related *processes* (3.54);

— information created in order for the *organization* (3.50) to operate (documentation);

— evidence of results achieved (records).

© ISO/IEC 2026 – All rights reserved

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

~~**3.20**~~
~~**effectiveness**~~
~~extent to which planned activities are realized and planned results achieved~~

~~**3.21**~~
3.5
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".~~

[SOURCE: ISO ~~Guide 73:2009, 3.5.1.3~~ /IEC 27005:2022, 3.1.11, modified — ~~Note 4~~ The two notes to entry ~~has been deleted~~ have been omitted.]

~~**3.22**~~
~~**external context**~~
~~external environment in which the organization seeks to achieve its *objectives* (3.49)~~

~~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* of the *organization* (3.50);~~

~~— relationships with, and perceptions and values of, external *stakeholders* (3.37).~~

~~[SOURCE: ISO Guide 73:2009, 3.3.1.1]~~

~~**3.23**~~
~~**governance of information security**~~
~~system by which an *organization's* (3.50) *information security* (3.28) activities are directed and controlled~~

~~**3.24**~~
~~**governing body**~~
~~person or group of people who are accountable for the *performance* (3.52) and conformity of the *organization* (3.50)~~

~~Note 1 to entry: The governing body can, in some jurisdictions, be a board of directors.~~

~~**3.25**~~
~~**indicator**~~
~~*measure* (3.42) that provides an estimate or evaluation~~

~~**3.26**~~
~~**information need**~~
~~insight necessary to manage *objectives* (3.49), goals, risks and problems~~

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

~~**3.27**~~
~~**information processing facilities**~~
~~any information processing system, service or infrastructure, or the physical location housing it~~

© ISO/IEC 2026 – All rights reserved

3.28
information security
preservation of *confidentiality* (3.10), *integrity* (3.36) and *availability* (3.7) of information

Note 1 to entry: In addition, other properties, such as *authenticity* (3.6), accountability, *non-repudiation* (3.48), and *reliability* (3.55) can also be involved.

3.29
information security continuity
processes (3.54) and procedures for ensuring continued *information security* (3.28) operations

3.30
information security event
identified occurrence of a system, service or network state indicating a possible breach of *information security* (3.28) *policy* (3.53) or failure of *controls* (3.14), or a previously unknown situation that can be security relevant

3.31
information security incident
single or a series of unwanted or unexpected *information security events* (3.30) that have a significant probability of compromising business operations and threatening *information security* (3.28)

3.32
information security incident management
set of *processes* (3.54) for detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents* (3.31)

3.33
information security management system (ISMS) professional
person who establishes, implements, maintains and continuously improves one or more information security management system *processes* (3.54)

3.34
information sharing community
group of *organizations* (3.50) that agree to share information

Note 1 to entry: An organization can be an individual.

3.35
information system
set of applications, services, information technology assets, or other information-handling components

3.36
integrity
property of accuracy and completeness

3.37
interested party (preferred term)
stakeholder (admitted term)
person or *organization* (3.50) that can affect, be affected by, or perceive itself to be affected by a decision or activity

3.38
internal context
internal environment in which the *organization* (3.50) seeks to achieve its objectives

Note 1 to entry: Internal context can include:

— governance, organizational structure, roles and accountabilities;

— *policies* (3.53), *objectives* (3.49), and the strategies that are in place to achieve them;

© ISO/IEC 2026 – All rights reserved

— the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, *processes* (3.54), systems and technologies);

— *information systems* (3.35), information flows and decision-making *processes* (both formal and informal);

— relationships with, and perceptions and values of, internal *stakeholders* (3.37);

— the organization's culture;

— standards, guidelines and models adopted by the organization;

— form and extent of contractual relationships.

[SOURCE: ISO Guide 73:2009, 3.3.1.2]

3.39
level of risk
magnitude of a *risk* (3.61) expressed in terms of the combination of *consequences* (3.12) and their *likelihood* (3.40)

[SOURCE: ISO Guide 73:2009, 3.6.1.8, modified — "or combination of risks" has been deleted in the definition.]

3.40
3.6
likelihood
chance of something happening

[SOURCE: ISO Guide 73:2009, 3.6.1.1 /IEC 27005:2022, 3.1.13, modified — Notes 1 and 2 The two notes to entry have been deleted omitted.]

3.41
3.7
management system
consequence
set of interrelated or interacting elements of an *organization* (3.50) to establish *policies* (3.53) and *objectives* (3.49) and *processes* (3.54) 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'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, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

outcome of an *event* (3.5) affecting objectives

[SOURCE: ISO/IEC 27005:2022, 3.1.14, modified — The three notes to entry have been omitted.]

3.42
3.8
measure
risk
variable to which a value is assigned as the result of *measurement* (3.43)

effect of uncertainty on objectives

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.15 27005:2022, 3.1.3, modified — Note 2 The seven notes to entry has been deleted have been omitted.]

© ISO/IEC 2026 – All rights reserved

~~3.43~~
3.9
~~**measurement**~~
risk treatment
~~*process* (3.54) to determine a value~~

process to modify *risk* (3.8)

~~3.44~~
3.10
~~**measurement function**~~
control
~~algorithm or calculation performed to combine two or more *base measures* (3.8)~~

~~[SOURCE: ISO/IEC/IEEE 15939:2017, 3.20]~~

measure that maintains and/or modifies *risk* (3.8)

[SOURCE: ISO/IEC 27002:2022, 3.1.8, modified — The two notes to entry have been omitted.]

~~3.45~~
~~**measurement method**~~
~~logical sequence of operations, described generically, used in quantifying an attribute with respect to a specified scale~~

~~Note 1 to entry: The type of measurement method depends on the nature of the operations used to quantify an *attribute* (3.4). Two types can be distinguished:~~

~~— subjective: quantification involving human judgment, and~~

~~— objective: quantification based on numerical rules.~~

~~[SOURCE: ISO/IEC/IEEE 15939:2017, 3.21, modified — Note 2 to entry has been deleted.]~~

~~3.46~~
~~**monitoring**~~
~~determining the status of a system, a *process* (3.54) or an activity~~

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

~~3.47~~
~~**nonconformity**~~
~~non-fulfilment of a *requirement* (3.56)~~

~~3.48~~
~~**non-repudiation**~~
~~ability to prove the occurrence of a claimed *event* (3.21) or action and its originating entities~~

~~3.49~~
~~**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-wide, project, product and *process* (3.54)].~~

~~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 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 objectives are set by the organization, consistent with the information security policy, to achieve specific results.~~

© ISO/IEC 2026 – All rights reserved

3.50
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.49)

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.

3.51
outsource
make an arrangement where an external *organization* (3.50) performs part of an organization's function or *process* (3.54)

Note 1 to entry: An external organization is outside the scope of the *management system* (3.41), although the outsourced function or process is within the scope.

3.52
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* (3.54), products (including services), systems or *organizations* (3.50).

3.53
policy
intentions and direction of an *organization* (3.50), as formally expressed by its *top management* (3.75)

3.54
process
set of interrelated or interacting activities which transforms inputs into outputs

3.55
reliability
property of consistent intended behaviour and results

3.56
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 and interested parties 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.

3.57
residual risk
risk (3.61) remaining after *risk treatment* (3.72)

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

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

3.58
review
activity undertaken to determine the suitability, adequacy and *effectiveness* (3.20) of the subject matter to achieve established *objectives* (3.49)

[SOURCE: ISO Guide 73:2009, 3.8.2.2, modified — Note 1 to entry has been deleted.]

© ISO/IEC 2026 – All rights reserved

3.59
review object
specific item being reviewed

3.60
review objective
statement describing what is to be achieved as a result of a *review* (3.59)

3.61
risk
effect of uncertainty on *objectives* (3.49)

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, its consequence, or likelihood.

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.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (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 risks can be expressed as effect of uncertainty on information security objectives.

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

3.62
risk acceptance
informed decision to take a particular *risk* (3.61)

Note 1 to entry: Risk acceptance can occur without *risk treatment* (3.72) or during the *process* (3.54) of risk treatment.

Note 2 to entry: Accepted risks are subject to *monitoring* (3.46) and *review* (3.58).

[SOURCE: ISO Guide 73:2009, 3.7.1.6]

3.63
risk analysis
process (3.54) to comprehend the nature of *risk* (3.61) and to determine the *level of risk* (3.39)

Note 1 to entry: Risk analysis provides the basis for *risk evaluation* (3.67) and decisions about *risk treatment* (3.72).

Note 2 to entry: Risk analysis includes risk estimation.

[SOURCE: ISO Guide 73:2009, 3.6.1]

3.64
risk assessment
overall *process* (3.54) of *risk identification* (3.68), *risk analysis* (3.63) and *risk evaluation* (3.67)

[SOURCE: ISO Guide 73:2009, 3.4.1]

3.65
risk communication and consultation
set of continual and iterative *processes* (3.54) that an organization conducts to provide, share or obtain information, and to engage in dialogue with *stakeholders* (3.37) regarding the management of *risk* (3.61)

Note 1 to entry: The information can relate to the existence, nature, form, *likelihood* (3.41), significance, evaluation, acceptability and treatment of risk.

© ISO/IEC 2026 – All rights reserved

Note 2 to entry: Consultation is a two-way process of informed communication between an *organization* (3.50) and its stakeholders 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, and

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

3.66
risk criteria
terms of reference against which the significance of *risk* (3.61) is evaluated

Note 1 to entry: Risk criteria are based on organizational objectives, and *external context* (3.22) and *internal context* (3.38).

Note 2 to entry: Risk criteria can be derived from standards, laws, *policies* (3.53) and other *requirements* (3.56).

[SOURCE: ISO Guide 73:2009, 3.3.1.3]

3.67
risk evaluation
process (3.54) of comparing the results of *risk analysis* (3.63) with *risk criteria* (3.66) to determine whether the *risk* (3.61) and/or its magnitude is acceptable or tolerable

Note 1 to entry: Risk evaluation assists in the decision about *risk treatment* (3.72).

[SOURCE: ISO Guide 73:2009, 3.7.1]

3.68
risk identification
process (3.54) of finding, recognizing and describing *risks* (3.61)

Note 1 to entry: Risk identification involves the identification of risk sources, *events* (3.21), their causes and their potential *consequences* (3.12).

Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and *stakeholders'* (3.37) needs.

[SOURCE: ISO Guide 73:2009, 3.5.1]

3.69
risk management
coordinated activities to direct and control an *organization* (3.50) with regard to *risk* (3.61)

[SOURCE: ISO Guide 73:2009, 2.1]

3.70
3.11
risk management process **specified requirement**
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 and reviewing *risk* (3.61)

Note 1 to entry: ISO/IEC 27005 uses the term "*process*" (3.54) to describe risk management overall. The elements within the *risk management* (3.69) process are referred to as "activities".

need or expectation that is stated

[SOURCE: ISO Guide 73:2009, 3.1 /IEC 17000:2020, 4.1, modified — Note 1 The four notes to entry has been added have been omitted.]

© ISO/IEC 2026 – All rights reserved