International Standard

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

Sixth edition
2026-07

Reference number
ISO/IEC 27000:2026(en)

Horizontal document

© 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 ... **iv**
Introduction ... **vi**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Concepts and principles ... **2**
4.1 Concepts ... 2
4.1.1 The need for information security ... 2
4.1.2 Information ... 3
4.1.3 Information security ... 3
4.1.4 Constantly changing risks ... 3
4.1.5 Risk treatment plan ... 3
4.1.6 Purpose of an information security management system (ISMS) ... 4
4.1.7 Importance of an ISMS ... 4
4.1.8 Process approach ... 5
4.1.9 Scope ... 5
4.2 Principles ... 5
4.2.1 Establishing, implementing, maintaining and improving an ISMS ... 5
4.2.2 Successfully implementing an ISMS ... 5
4.2.3 Determining information security requirements ... 5
4.2.4 Integration into business processes ... 6
5 Documents related to ISMS including ISO/IEC 27001 ... **6**
5.1 General ... 6
5.2 ISO/IEC 27001 (specification of an ISMS) ... 6
5.3 Candidate necessary information security controls ... 7
5.3.1 ISO/IEC 27002 (information security controls) ... 7
5.3.2 ISO/IEC 27010 (inter-sector and inter-organizational communications) ... 7
5.3.3 ISO/IEC 27011 (telecommunications organizations) ... 7
5.3.4 ISO/IEC 27017 (cloud services) ... 7
5.3.5 ISO/IEC 27019 (energy utility industry) ... 7
5.4 Fulfilment of ISMS requirements ... 7
5.4.1 ISO/IEC 27003 (ISMS guidance) ... 7
5.4.2 ISO/IEC 27004 (monitoring, measurement, analysis and evaluation) ... 7
5.4.3 ISO/IEC 27005 (guidance on managing information security risks) ... 7
5.4.4 ISO/IEC 27007 (ISMS auditing) ... 7
5.5 Use of ISMS ... 8
5.5.1 ISO/IEC 27013 (integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1) ... 8
5.5.2 ISO/IEC 27014 (governance of information security) ... 8
5.5.3 ISO/IEC TR 27016 (organizational economics) ... 8
5.6 Control assessment, attributes, processes and competence ... 8
5.6.1 ISO/IEC TS 27008 (assessment of information security controls) ... 8
5.6.2 ISO/IEC 27021 (competence requirements for ISMS professionals) ... 8
5.6.3 ISO/IEC TS 27022 (ISMS processes) ... 8
5.6.4 ISO/IEC 27028 (ISO/IEC 27002 attributes) ... 8
5.7 ISO/IEC 27006-1 (Conformity assessment) ... 8
5.8 Relationships between the standards ... 8
Bibliography ... **10**

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

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 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*, 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 sixth edition cancels and replaces the fifth edition (ISO/IEC 27000:2018), which has been technically revised.

The main changes are as follows:

— the title has been modified;

— 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;

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

— Clause 3 has been modified to only contain definitions for those terms used in presenting the concepts and principles described in this document;

— 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

© ISO/IEC 2026 – All rights reserved

Introduction

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

3.2
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

3.3
integrity
property of accuracy and completeness

3.4
availability
property of being accessible and usable on demand by an authorized entity

3.5
event
occurrence or change of a particular set of circumstances

[SOURCE: ISO/IEC 27005:2022, 3.1.11, modified — The two notes to entry have been omitted.]

3.6
likelihood
chance of something happening

[SOURCE: ISO/IEC 27005:2022, 3.1.13, modified — The two notes to entry have been omitted.]

© ISO/IEC 2026 – All rights reserved