BSI Standards Publication

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

National foreword

This British Standard is the UK implementation of EN ISO/IEC 27000:2026. It is identical to ISO/IEC 27000:2026. It supersedes BS EN ISO/IEC 27000:2020, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/1, Information Security Management Systems.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2026

ISBN 978 0 539 27184 3

ICS 01.040.35; 03.100.70; 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2026.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD **EN ISO/IEC 27000**

EUROPÄISCHE NORM

July 2026

ICS 35.030

Supersedes EN ISO/IEC 27000:2020

English version

Information security, cybersecurity and privacy protection - Information security management systems - Overview (ISO/IEC 27000:2026)

Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Vue d'ensemble (ISO/IEC 27000:2026)

Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Überblick und Terminologie (ISO/IEC 27000:2026)

This European Standard was approved by CEN on 2 July 2026.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

European foreword

This document (EN ISO/IEC 27000:2026) has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" in collaboration with Technical Committee CEN-CENELEC/ JTC 13 “Cybersecurity and Data Protection” the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by January 2028, and conflicting national standards shall be withdrawn at the latest by January 2028.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO/IEC 27000:2020.

Any feedback and questions on this document should be directed to the users’ national standards body/national committee. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27000 has been approved by CEN-CENELEC as EN ISO/IEC 27000:2026 without any modification.

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.

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.

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.]