



DPC: 25/30474647 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 15 July 2025

Origin: International

Latest date for receipt of comments: 07 September 2025

Project No. 2023/01132

Responsible committee: IST/33/1 Information Security Management Systems

Interested committees:

Title: Draft BS EN ISO/IEC 27000 Information security, cybersecurity and privacy protection — Information security management systems — Overview.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 07 September 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 27000

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

ICS: 35.030; 01.040.35

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2025-07-15

Voting terminates on:
2025-10-07

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 27000:2025(en)

Full document details: 25/30474647 DC

© ISO/IEC 2025  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

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	v
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 Risks are constantly changing	3
4.1.5 Risk treatment plan	4
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 Successful ISMS implementation	5
4.2.3 Determining information security requirements	6
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	6
5.3.1 ISO/IEC 27002 (Information security controls)	6
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	7
5.5.1 ISO/IEC 27013 (Integrated implementation with ISO/IEC 20000-1)	7
5.5.2 ISO/IEC 27014 (Governance of information security)	8
5.5.3 ISO/IEC TR 27016 (Organizational economics)	8
5.5.4 ISO/IEC TR 27029 (ISO/IEC 27002 and ISO and IEC standards)	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 Conformity assessment	8
5.7.1 ISO/IEC 27006-1 (Requirements for bodies providing audit and certification)	8
5.8 Relationships between the standards	8
Bibliography	10

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 organizations, governmental and non-governmental, in liaison with ISO, 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 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 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).

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 Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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 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](#) contains definitions for those terms used in presenting the concepts and principles ISO/IEC 27000;
- ISO/IEC 27000 is no longer a terminology document.

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.