



BSI Standards Publication

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

This is a preview of "BS ISO/IEC 27001:202...". [Click here to purchase the full version from the ANSI store.](#)

National foreword

This British Standard is the UK implementation of ISO/IEC 27001:2022. It does not supersede BS EN ISO/IEC 27001:2017, which remains current until it is withdrawn on UK implementation of a European Standard that approves the text of ISO/IEC 27001:2022. BSI, as a member of CEN/CENELEC, is obliged to publish the European Standard.

BSI requested a derogation from CEN/CENELEC for its national standard to be identical to ISO/IEC 27001:2022. The request was granted by CEN/CENELEC on the condition that BSI aligns its national standard with any future European Standard that approves the text of ISO/IEC 27001:2022.

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.

© The British Standards Institution 2022
Published by BSI Standards Limited 2022

ISBN 978 0 539 22734 5

ICS 03.100.70; 35.030; 35.040

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 December 2022.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

This is a preview of "BS ISO/IEC 27001:202...". [Click here to purchase the full version from the ANSI store.](#)

Third edition
2022-10

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

*Sécurité de l'information, cybersécurité et protection de la vie
privée — Systèmes de management de la sécurité de l'information —
Exigences*



Reference number
ISO/IEC 27001:2022(E)

© ISO/IEC 2022

This is a preview of "BS ISO/IEC 27001:202...". Click here to purchase the full version from the ANSI store.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

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

This is a preview of "BS ISO/IEC 27001:202...". Click here to purchase the full version from the ANSI store.

Contents

	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Context of the organization	1
4.1 Understanding the organization and its context.....	1
4.2 Understanding the needs and expectations of interested parties.....	1
4.3 Determining the scope of the information security management system.....	2
4.4 Information security management system.....	2
5 Leadership	2
5.1 Leadership and commitment.....	2
5.2 Policy.....	3
5.3 Organizational roles, responsibilities and authorities.....	3
6 Planning	3
6.1 Actions to address risks and opportunities.....	3
6.1.1 General.....	3
6.1.2 Information security risk assessment.....	4
6.1.3 Information security risk treatment.....	4
6.2 Information security objectives and planning to achieve them.....	5
7 Support	6
7.1 Resources.....	6
7.2 Competence.....	6
7.3 Awareness.....	6
7.4 Communication.....	6
7.5 Documented information.....	6
7.5.1 General.....	6
7.5.2 Creating and updating.....	7
7.5.3 Control of documented information.....	7
8 Operation	7
8.1 Operational planning and control.....	7
8.2 Information security risk assessment.....	8
8.3 Information security risk treatment.....	8
9 Performance evaluation	8
9.1 Monitoring, measurement, analysis and evaluation.....	8
9.2 Internal audit.....	8
9.2.1 General.....	8
9.2.2 Internal audit programme.....	9
9.3 Management review.....	9
9.3.1 General.....	9
9.3.2 Management review inputs.....	9
9.3.3 Management review results.....	9
10 Improvement	10
10.1 Continual improvement.....	10
10.2 Nonconformity and corrective action.....	10
Annex A (normative) Information security controls reference	11
Bibliography	19

This is a preview of "BS ISO/IEC 27001:202...". Click here to purchase the full version from the ANSI store.

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).

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 <https://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. 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*.

This third edition cancels and replaces the second edition (ISO/IEC 27001:2013), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 27001:2013/Cor 1:2014 and ISO/IEC 27001:2013/Cor 2:2015.

The main changes are as follows:

— the text has been aligned with the harmonized structure for management system standards and ISO/IEC 27002:2022.

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 is a preview of "BS ISO/IEC 27001:202...". [Click here to purchase the full version from the ANSI store.](#)

Introduction

0.1 General

This document has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This document can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this document does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003^[2], ISO/IEC 27004^[3] and ISO/IEC 27005^[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This document applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

This is a preview of "BS ISO/IEC 27001:202...". [Click here to purchase the full version from the ANSI store.](#)

This is a preview of "BS ISO/IEC 27001:202...". Click here to purchase the full version from the ANSI store.

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

1 Scope

This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in [Clauses 4 to 10](#) is not acceptable when an organization claims conformity to this document.

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/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 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/>

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000:2018^[5].

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

- a) interested parties that are relevant to the information security management system;
- b) the relevant requirements of these interested parties;
- c) which of these requirements will be addressed through the information security management system.