

AS/NZS ISO/IEC 27001:2023
ISO/IEC 27001:2022
ISO/IEC 27001:2022/Amd 1:2024
(Incorporating Amendment No. 1)



Australian/New Zealand Standard™

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



Share your feedback
about this standard.
Scan the QR code on your
phone or click/ enter the
link to take the survey
feedback.standards.org.au/27001:2023

AS/NZS ISO/IEC 27001:2023

This Joint Australian/New Zealand Standard™ was prepared by Joint Technical Committee IT-012, Information security, cybersecurity and privacy protection. It was approved on behalf of the Council of Standards Australia on 04 August 2023 and by the New Zealand Standards Approval Board on 02 August 2023.

This Standard was published on 15 September 2023.

The following are represented on Committee IT-012:

- Australasian Society for Computers and Law
- Australian Industry Group
- Australian Information Industry Association
- Australian Information Security Association
- Australian Security Industry Association
- Business Continuity Institute Australasia
- Consumers Federation of Australia
- CSIRO Data 61
- Cyber Security Cooperative Research Centre
- Department of Defence (Australian Government)
- Department of Internal Affairs, NZ
- Energy Networks Australia
- Engineers Australia
- ISACA Melbourne
- Joint Accreditation System of Australia & New Zealand
- Monash University
- NZ Ministry of Business, Innovation and Employment (MBIE)
- Office of the Victorian Information Commissioner
- University of Waikato
- University of Wollongong

This Standard was issued in draft form for comment as DR AS/NZS ISO/IEC 27001:2023.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

www.standards.govt.nz

AS/NZS ISO/IEC 27001:2023
ISO/IEC 27001:2022
ISO/IEC 27001:2022/Amd 1:2024
(Incorporating Amendment No. 1)

Australian/New Zealand Standard™

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

Originated as part of AS/NZS 4444:1996.
Jointly revised and redesignated as AS/NZS ISO/IEC 27001:2006.
Revised and designated as AS ISO/IEC 27001:2015.
Jointly revised and redesignated as AS/NZS ISO/IEC 27001:2023.
Reissued incorporating Amendment No 1 (November 2024).

COPYRIGHT

© ISO/IEC 2024 — All rights reserved
© Standards Australia Limited/the Crown in right of New Zealand, administered by the New Zealand Standards Executive 2024

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth) or the Copyright Act 1994 (New Zealand).

Preface

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information security, cybersecurity and privacy protection, to supersede AS ISO/IEC 27001:2015, *Information technology—Security techniques—Information security management systems—Requirements*.

A1 Amendment 1 to this Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information security, cybersecurity and privacy protection. **A1**

A1 This Standard incorporates Amendment No. 1 (November 2024). The start and end of changes introduced by the Amendment are indicated in the text by tags including the Amendment number 1. **A1**

The objective of this document is to specify 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.

A1 This document is identical with, and has been reproduced from, ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* and its Amendment No. 1 (2024) which has been added at the end of the source text. **A1**

As this document has been reproduced from an International document, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents

Preface	ii
Foreword	v
Introduction	vi
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.....	2
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.....	10
10 Improvement	10
10.1 Continual improvement.....	10
10.2 Nonconformity and corrective action.....	10
Annex A (normative) Information security controls reference	11
Bibliography	18

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

-
- Looking for additional Standards? Visit Intertek Inform Infostore
 - Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation
-