



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/27001:2015

AS ISO/IEC 27001:2015
ISO/IEC 27001:2013
ISO/IEC 27001:2013/Cor 1:2014

AS ISO/IEC 27001:2015



Information technology—Security techniques—Information security management systems—Requirements



This Australian Standard® was prepared by Committee IT-012, Information Technology Security Techniques. It was approved on behalf of the Council of Standards Australia on 26 March 2015.

This Standard was published on 29 April 2015.

The following are represented on Committee IT-012:

- Australian Association of Permanent Building Societies
 - Australian Bankers Association
 - Australian Industry Group
 - Australian Information Industry Association
 - Australian Payments Clearing Association
 - Department of Communications (Australian Government)
 - Department of Defence (Australian Government)
 - Department of Finance (Australian Government)
 - Engineers Australia
 - New Zealand Computer Society
 - Office of the Chief Information Officer, SA
 - Office of the Commissioner for Privacy and Data Protection
-

This Standard was issued in draft form for comment as DR AS/NZS ISO/IEC 27001:2014.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

AS ISO/IEC 27001:2015

Australian Standard[®]

**Information technology—Security
techniques—Information security
management systems—Requirements**

Originated as part of AS/NZS 4444:1996.
Previous edition AS/NZS ISO/IEC 27001:2006.
Revised and designated as AS ISO/IEC 27001:2015.

COPYRIGHT

© Standards Australia Limited

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.

ISBN 978 1 76035 029 1

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Technology Security Techniques, to supersede, AS/NZS ISO/IEC 27001:2006.

The objective of this Standard is to specify the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This International Standard 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 International Standard 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 Standard.

This Standard is identical with, and has been reproduced from ISO/IEC 27001:2013, *Information technology—Security techniques—Information security management systems—Requirements* and its Corrigendum 1 (2014) which is added following the source text.

As this Standard is reproduced from an International Standard, the following applies:

- (a) In the source text ‘this International Standard’ should read ‘this Australian Standard’.
- (b) A full point substitutes for a comma when referring to a decimal marker.

None of the normative references in the source document have been adopted as Australian or Australian/New Zealand Standards.

The term ‘normative’ has been used in this Standard to define the application of the annex to which it applies. A ‘normative’ annex is an integral part of a Standard.

CONTENTS

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	1
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
6.2	Information security objectives and planning to achieve them	5
7	Support	5
7.1	Resources	5
7.2	Competence	5
7.3	Awareness	5
7.4	Communication	6
7.5	Documented information	6
8	Operation	7
8.1	Operational planning and control	7
8.2	Information security risk assessment	7
8.3	Information security risk treatment	7
9	Performance evaluation	7
9.1	Monitoring, measurement, analysis and evaluation	7
9.2	Internal audit	8
9.3	Management review	8
10	Improvement	9
10.1	Nonconformity and corrective action	9
10.2	Continual improvement	9
	Annex A (normative) Reference control objectives and controls	10
	Bibliography	23

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
-