



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



AS ISO/IEC 27003:2017

This Australian Standard® was prepared by Committee IT-012, Information Systems, Security and Identification Technology. It was approved on behalf of the Council of Standards Australia on 13 September 2017.

This Standard was published on 26 September 2017.

The following are represented on Committee IT-012:

- Australian Association of Permanent Building Societies
- Australian Information Industry Association
- Department of Defence (Australian Government)
- Engineers Australia
- Office of the Commissioner for Privacy and Data Protection

This Standard was issued in draft form for comment as DR AS ISO/IEC 27003:2017.

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.saiglobal.com (sales and distribution)

Australian Standard®

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

First edition AS ISO/IEC 27003:2017.

COPYRIGHT

Standards Australia Ltd 2017

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).

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia.

Preface

This Standard was prepared by the Australian members of the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification Technology.

The objective of this Standard is to provide guidance on the requirements for an information security management system (ISMS) as specified in AS ISO/IEC 27001 and provides recommendations ('should'), possibilities ('can') and permissions ('may') in relation to them. It is not the intention of this document to provide general guidance on all aspects of information security.

This Standard is identical with, and has been reproduced from, ISO/IEC 27003:2017, *Information technology—Security techniques—Information security management systems—Guidance*.

As this document has been reproduced from an International Standard, the following applies:

- (a) In the source text 'ISO/IEC 27003' should read 'this Australian Standard'.
- (b) A full point substitutes for a coma 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.

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	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.....	4
4.3 Determining the scope of the information security management system.....	5
4.4 Information security management system.....	6
5 Leadership	7
5.1 Leadership and commitment.....	7
5.2 Policy.....	8
5.3 Organizational roles, responsibilities and authorities.....	10
6 Planning	11
6.1 Actions to address risks and opportunities.....	11
6.1.1 General.....	11
6.1.2 Information security risk assessment.....	13
6.1.3 Information security risk treatment.....	16
6.2 Information security objectives and planning to achieve them.....	19
7 Support	22
7.1 Resources.....	22
7.2 Competence.....	23
7.3 Awareness.....	24
7.4 Communication.....	25
7.5 Documented information.....	26
7.5.1 General.....	26
7.5.2 Creating and updating.....	28
7.5.3 Control of documented information.....	29
8 Operation	30
8.1 Operational planning and control.....	30
8.2 Information security risk assessment.....	32
8.3 Information security risk treatment.....	32
9 Performance evaluation	33
9.1 Monitoring, measurement, analysis and evaluation.....	33
9.2 Internal audit.....	34
9.3 Management review.....	37
10 Improvement	38
10.1 Nonconformity and corrective action.....	38
10.2 Continual improvement.....	41
Annex A (informative) Policy framework	43
Bibliography	46

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](#)
-