

AS/NZS ISO/IEC 27005:2012

AS/NZS ISO/IEC 27005:2012

Australian/New Zealand Standard™

**Information technology—Security
techniques—Information security risk
management (ISO/IEC 27005:2011, MOD)**



AS/NZS ISO/IEC 27005:2012

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-012, Information Security. It was approved on behalf of the Council of Standards Australia on 13 June 2012 and on behalf of the Council of Standards New Zealand on 18 June 2012.

This Standard was published on 29 June 2012.

The following are represented on Committee IT-012:

Attorney General's Department
Australia Post
Australian Association of Permanent Building Societies
Australian Chamber of Commerce and Industry
Australian Government Information Management Office
Australian Industry Group
Australian Information Industry Association
Australian Payments Clearing Association
Certification Forum of Australia
Consumers Federation of Australia
Council of Small Business Organisations of Australia
Department of Defence
Department of Social Welfare, New Zealand
Government Communication Security Bureau, New Zealand
Internet Industry Association
National ICT Australia
New Zealand Defence Force
NSW Police Force
Reserve Bank of Australia

Keeping Standards up-to-date

Standards are living documents which 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 Standards may also be withdrawn.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 which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.saiglobal.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR AS/NZS ISO/IEC 27005.

AS/NZS ISO/IEC 27005:2012

Australian/New Zealand Standard™

**Information technology—Security
techniques—Information security risk
management (ISO/IEC 27005:2011, MOD)**

Originated as HB 231:2000.
Previous edition HB 231:2004.
Jointly revised and redesignated as AS/NZS ISO/IEC 27005:2012.

COPYRIGHT

© Standards Australia Limited/Standards New Zealand

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 (Australia) or the Copyright Act 1994 (New Zealand).

Jointly published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001 and by Standards New Zealand, Private Bag 2439, Wellington 6140.

ISBN 978 1 74342 192 5

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Security to supersede HB 231:2004, *Information security risk management guidelines*.

The objective of this Standard is to endorse this important Standard as applicable for Australian use.

This Standard is an adoption with national modifications and has been reproduced from ISO/IEC 27005:2011, *Information technology—Security techniques—Information security risk management* and has been varied as indicated to take account of Australian/New Zealand conditions. The modifications are specified in Appendix ZZ.

This Standard contains all the normative requirements of ISO/IEC 27005:2011. It differs from ISO/IEC 27005:2011 as follows:

- (a) Informative Annex E (Information security risk assessment approaches) has been removed from the source text because the Committee considers that it is potentially misleading. Appendix ZZ specifies a replacement Annex E in which more comprehensive guidance on the topic of risk assessment is indicated by reference to IEC/ISO 31010.
- (b) Consequential editorial changes have been made consistent with the deletion of Annex E.

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

- (i) Its number appears on the cover and title page while the International Standard number appears only on the cover.
- (ii) In the source text ‘this International Standard’ should read ‘this Australian/New Zealand Standard’.
- (iii) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

<i>Reference to International Standard</i>		<i>Australian/New Zealand Standard</i>	
ISO/IEC		AS/NZS ISO/IEC	
27000	Information technology—Security techniques—Information security management systems—Overview and vocabulary	—	
27001	Information technology—Security techniques—Information security management systems—Requirements	27001	Information technology—Security techniques—Information security management systems—Requirements

The terms ‘normative’ and ‘informative’ have been used in this Standard to define the application of the annex or appendix to which they apply. A ‘normative’ annex or appendix is an integral part of a Standard, whereas an ‘informative’ annex or appendix is only for information and guidance.

CONTENTS

1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Structure of this International Standard	5
5	Background.....	6
6	Overview of the information security risk management process	7
7	Context establishment	10
7.1	General considerations.....	10
7.2	Basic Criteria	10
7.2.1	Risk management approach	10
7.2.2	Risk evaluation criteria	10
7.2.3	Impact criteria	11
7.2.4	Risk acceptance criteria	11
7.3	Scope and boundaries	12
7.4	Organization for information security risk management	12
8	Information security risk assessment.....	13
8.1	General description of information security risk assessment	13
8.2	Risk identification.....	13
8.2.1	Introduction to risk identification	13
8.2.2	Identification of assets.....	14
8.2.3	Identification of threats	14
8.2.4	Identification of existing controls.....	15
8.2.5	Identification of vulnerabilities	15
8.2.6	Identification of consequences.....	16
8.3	Risk analysis	17
8.3.1	Risk analysis methodologies	17
8.3.2	Assessment of consequences	18
8.3.3	Assessment of incident likelihood	18
8.3.4	Level of risk determination.....	19
8.4	Risk evaluation	19
9	Information security risk treatment	20
9.1	General description of risk treatment	20

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
-