



**Information technology—Security
techniques—Information security
management—Monitoring,
measurement, analysis and evaluation**



AS ISO/IEC 27004:2018

This Australian Standard ® was prepared by IT-012, Information Systems, Security and Identification Technology. It was approved on behalf of the Council of Standards Australia on 18 December 2017.

This Standard was published on 22 February 2018.

The following are represented on Committee IT-012:

- Australian Information Industry Association
- Australian Payment Network
- Department of Defence (Australian Government)
- Department of Finance (Australian Government)
- Office of the Commissioner for Privacy and Data Protection, Vic.
- Certification Interests Australia

This Standard was issued in draft form for comment as DR AS ISO/IEC 27004:2017.

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)

ISBN 978 1 76035 976 8



Information technology—Security techniques—Information security management—Monitoring, measurement, analysis and evaluation

First published as AS ISO/IEC 27004:2018.

COPYRIGHT

© ISO/IEC 2018 — All rights reserved
© Standards Australia Limited 2018

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 guidelines intended to assist organizations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001:2013, Clause 9.1. This Standard establishes—

- (a) the monitoring and measurement of information security performance;
- (b) the monitoring and measurement of the effectiveness of an information security management system (ISMS) including its processes and controls; and
- (c) the analysis and evaluation of the results of monitoring and measurement.

This Standard is identical with, and has been reproduced from, ISO/IEC 27004:2016 *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*.

As this document has been reproduced from an International Standard, 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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Structure and overview	1
5 Rationale	2
5.1 The need for measurement	2
5.2 Fulfilling the ISO/IEC 27001 requirements	2
5.3 Validity of results	3
5.4 Benefits	3
6 Characteristics	4
6.1 General	4
6.2 What to monitor	4
6.3 What to measure	5
6.4 When to monitor, measure, analyse and evaluate	6
6.5 Who will monitor, measure, analyse and evaluate	6
7 Types of measures	7
7.1 General	7
7.2 Performance measures	7
7.3 Effectiveness measures	8
8 Processes	9
8.1 General	9
8.2 Identify information needs	10
8.3 Create and maintain measures	11
8.3.1 General	11
8.3.2 Identify current security practices that can support information needs	11
8.3.3 Develop or update measures	12
8.3.4 Document measures and prioritize for implementation	13
8.3.5 Keep management informed and engaged	13
8.4 Establish procedures	14
8.5 Monitor and measure	14
8.6 Analyse results	15
8.7 Evaluate information security performance and ISMS effectiveness	15
8.8 Review and improve monitoring, measurement, analysis and evaluation processes	15
8.9 Retain and communicate documented information	15
Annex A (informative) An information security measurement model	17
Annex B (informative) Measurement construct examples	19
Annex C (informative) An example of free-text form measurement construction	57
Bibliography	58

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](#)
-