AS ISO/IEC 27004:2018
ISO/IEC 27004:2016

AS ISO/IEC 27004:2018

Australian STANDARD

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

STANDARDS Australia

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.

ISBN 978 1 76035 976 8

AS ISO/IEC 27004:2018
ISO/IEC 27004:2016

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

First published as AS ISO/IEC 27004:2018.

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