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Standards may also be withdrawn.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.

Australian Standard®

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

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

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

INTRODUCTION

0.1 General

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This International Standard applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

AUSTRALIAN STANDARD

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

1 Scope

This International Standard specifies 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 International Standard.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009[5].

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system; and

b) the requirements of these interested parties relevant to information security.

NOTE The requirements of interested parties may include legal and regulatory requirements and contractual obligations.

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.