AS ISO/IEC 27002:2015
ISO/IEC 27002:2013
ISO/IEC 27002:2013/Cor 1:2014
A1 | ISO/IEC 27002:2013/Cor 2:2015
(Incorporating Amendment No. 1)

AS ISO/IEC 27002:2015

Information technology—Security techniques—Code of practice for information security controls

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

The following are represented on Committee IT-012:

- Australia and New Zealand Banking Group
- Attorney General's Department
- Microsoft
- Pacific Research
- Transport for NSW
- Veridity

This Standard was issued in draft form for comment as DR AS/NZS ISO/IEC 27002:2014.

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Standards may also be withdrawn.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.

AS ISO/IEC 27002:2015
(Incorporating Amendment No. 1)

Australian Standard®

Information technology—Security techniques—Code of practice for information security controls

Originated as part of AS/NZS 4444:1996.
Previous edition AS/NZS ISO/IEC 27002:2006.
Revised and designated as AS ISO/IEC 27002:2015.
Reissued incorporating Amendment No. 1 (May 2016).

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

ISBN 978 1 76035 030 7

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 27002:2006.

This Standard incorporates Amendment No. 1 (May 2016). The changes required by the Amendment are indicated in the text by a marginal bar and amendment number against the clause, note, table, figure or part thereof affected.

The objective of this Standard is to provide guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

This Standard is designed to be used by organizations that intend to—

(a) select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;

(b) implement commonly accepted information security controls; and

(c) develop their own information security management guidelines.

A1 This Standard is identical with, and has been reproduced from ISO/IEC 27002:2013, *Information technology—Security techniques—Code of practice for information security controls*, and its Corrigendum 1 (2014) and Corrigendum 2 (2015) which are added following the source text.

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

(i) In the source text ‘this International Standard’ should read ‘this Australian Standard’.

(ii) 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.

CONTENTS

Page

INTRODUCTION

0.1 Background and context

This International Standard is designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001[10] or as a guidance document for organizations implementing commonly accepted information security controls. This standard is also intended for use in developing industry- and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s).

Organizations of all types and sizes (including public and private sector, commercial and non-profit) collect, process, store and transmit information in many forms including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond the written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business and consequently deserve or require protection against various hazards.

Assets are subject to both deliberate and accidental threats while the related processes, systems, networks and people have inherent vulnerabilities. Changes to business processes and systems or other external changes (such as new laws and regulations) may create new information security risks. Therefore, given the multitude of ways in which threats could take advantage of vulnerabilities to harm the organization, information security risks are always present. Effective information security reduces these risks by protecting the organization against threats and vulnerabilities, and then reduces impacts to its assets.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. An ISMS such as that specified in ISO/IEC 27001[10] takes a holistic, coordinated view of the organization's information security risks in order to implement a comprehensive suite of information security controls under the overall framework of a coherent management system.

Many information systems have not been designed to be secure in the sense of ISO/IEC 27001[10] and this standard. The security that can be achieved through technical means is limited and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. A successful ISMS requires support by all employees in the organization. It can also require participation from shareholders, suppliers or other external parties. Specialist advice from external parties can also be needed.

In a more general sense, effective information security also assures management and other stakeholders that the organization's assets are reasonably safe and protected against harm, thereby acting as a business enabler.

0.2 Information security requirements

It is essential that an organization identifies its security requirements. There are three main sources of security requirements:

a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;

b) the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural environment;

c) the set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organization has developed to support its operations.

Resources employed in implementing controls need to be balanced against the business harm likely to result from security issues in the absence of those controls. The results of a risk assessment will help guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

ISO/IEC 27005[11] provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

0.3 Selecting controls

Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate.

The selection of controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations. Control selection also depends on the manner in which controls interact to provide defence in depth.

Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations. The controls are explained in more detail below along with implementation guidance. More information about selecting controls and other risk treatment options can be found in ISO/IEC 27005.[11]

0.4 Developing your own guidelines

This International Standard may be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

0.5 Lifecycle considerations

Information has a natural lifecycle, from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. The value of, and risks to, assets may vary during their lifetime (e.g. unauthorized disclosure or theft of a company's financial accounts is far less significant after they have been formally published) but information security remains important to some extent at all stages.

Information systems have lifecycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be taken into account at every stage. New system developments and changes to existing systems present opportunities for organizations to update and improve security controls, taking actual incidents and current and projected information security risks into account.

0.6 Related standards

While this standard offers guidance on a broad range of information security controls that are commonly applied in many different organizations, the remaining standards in the ISO/IEC 27000 family provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to ISO/IEC 27000 for a general introduction to both ISMSs and the family of standards. ISO/IEC 27000 provides a glossary, formally defining most of the terms used throughout the ISO/IEC 27000 family of standards, and describes the scope and objectives for each member of the family.

AUSTRALIAN STANDARD

Information technology—Security techniques—Code of practice for information security controls

1 Scope

This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

This International Standard is designed to be used by organizations that intend to:

a) select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;[10]

b) implement commonly accepted information security controls;

c) develop their own information security management guidelines.

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 Structure of this standard

This standard contains 14 security control clauses collectively containing a total of 35 main security categories and 114 controls.

4.1 Clauses

Each clause defining security controls contains one or more main security categories.

The order of the clauses in this standard does not imply their importance. Depending on the circumstances, security controls from any or all clauses could be important, therefore each organization applying this standard should identify applicable controls, how important these are and their application to individual business processes. Furthermore, lists in this standard are not in priority order.

4.2 Control categories

Each main security control category contains:

a) a control objective stating what is to be achieved;

b) one or more controls that can be applied to achieve the control objective.

Control descriptions are structured as follows:

Control

Defines the specific control statement, to satisfy the control objective.

Implementation guidance

Provides more detailed information to support the implementation of the control and meeting the control objective. The guidance may not be entirely suitable or sufficient in all situations and may not fulfil the organization's specific control requirements. .

Other information

Provides further information that may need to be considered, for example legal considerations and references to other standards. If there is no other information to be provided this part is not shown.

5 Information security policies

5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Implementation guidance

At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.

Information security policies should address requirements created by:

a) business strategy;

b) regulations, legislation and contracts;

c) the current and projected information security threat environment.

The information security policy should contain statements concerning:

a) definition of information security, objectives and principles to guide all activities relating to information security;

b) assignment of general and specific responsibilities for information security management to defined roles;

c) processes for handling deviations and exceptions.

At a lower level, the information security policy should be supported by topic-specific policies, which further mandate the implementation of information security controls and are typically structured to address the needs of certain target groups within an organization or to cover certain topics.

Examples of such policy topics include:

a) access control (see Clause 9);

b) information classification (and handling) (see 8.2);

c) physical and environmental security (see Clause 11);

d) end user oriented topics such as:

   1) acceptable use of assets (see 8.1.3);

   2) clear desk and clear screen (see 11.2.9);

   3) information transfer (see 13.2.1);

   4) mobile devices and teleworking (see 6.2);

   5) restrictions on software installations and use (see 12.6.2);

e) backup (see 12.3);

f) information transfer (see 13.2);

g) protection from malware (see 12.2);

h) management of technical vulnerabilities (see 12.6.1);

i) cryptographic controls (see Clause 10);

j) communications security (see Clause 13);

k) privacy and protection of personally identifiable information (see 18.1.4);

l) supplier relationships (see Clause 15).

These policies should be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an "information security awareness, education and training programme" (see 7.2.2).

Other information

The need for internal policies for information security varies across organizations. Internal policies are especially useful in larger and more complex organizations where those defining and approving the expected levels of control are segregated from those implementing the controls or in situations where a policy applies to many different people or functions in the organization. Policies for information security can be issued in a single "information security policy" document or as a set of individual but related documents.

If any of the information security policies are distributed outside the organization, care should be taken not to disclose confidential information.

Some organizations use other terms for these policy documents, such as "Standards", "Directives" or "Rules".

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.