Singapore Standards Council

SS ISO/IEC 27001 : 2019

ISO/IEC 27001:2013, IDT

(ICS 35.040)

SINGAPORE STANDARD

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

Published by

Enterprise Singapore

SS ISO/IEC 27001 : 2019
ISO/IEC 27001:2013, IDT
(ICS 35.040)

SINGAPORE STANDARD

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

ISBN 978-981-48-3571-8

This Singapore Standard was approved on 2 May 2019 by the Information Technology Standards Committee under the purview of the Singapore Standards Council.

First published, 2019

The Information Technology Standards Committee (ITSC), appointed by the Standards Council, consists of the following members:

		Name	Capacity
Chairman	:	Mr Yap Chee Yuen	*Individual Capacity*
Deputy Chairman	:	Mr Chak Kong Soon	*Singapore Computer Society*
Secretary	:	Mr Tao Yao Sing	*Infocomm Media Development Authority*
Members	:	Mr Chau Chee Chiang	*Government Technology Agency*
		Mr Cheong Tak Leong	*Enterprise Singapore*
		Assoc Prof Benjamin Gan Kok Siew	*Singapore Management University*
		Mr Hong Tse Min	*Infocomm Media Development Authority*
		Assoc Prof Huang Zhiyong	*National University of Singapore*
		Mr Kendrick Lee	*Information Technology Management Association*
		Mr Lim Soon Chia	*Cyber Security Agency of Singapore*
		Mr George Loh	*National Research Foundation*
		Mr Kelvin Ng	*Nanyang Polytechnic*
		Mr Harish Pillay	*Internet Society (Singapore Chapter)*
		Mr Tan Boon Yuen	*Singapore Polytechnic*
		Mr Victor Tan Hein Kiat	*Defence Science and Technology Agency*
		Mr Wong Wai Meng	*SGTech*

The Technical Committee on Security and Privacy, appointed by the ITSC and responsible for the preparation of this standard, consists of representatives from the following organisations:

		Name	Capacity
Chairman	:	Mr Joseph Gan	*Individual Capacity*
Secretary	:	Mr Er Chiang Kai	*Individual Capacity*
Members	:	Dr Khin Mi Mi Aung	*Institute for Infocomm Research*
		Mr Chan Kin Chong	*Individual Capacity*
		Mr Fong Kok Khuan	*Government Technology Agency*
		Dr Guo Jian	*Nanyang Technological University*
		Dr Kang Meng Chow	*Amazon Web Services*
		Dr Ryan Ko	*Individual Capacity*
		Mr Lau Soon Liang	*Individual Capacity*
		Mr Robert Lee	*Cyber Security Agency of Singapore*

Members	:	Dr Charles Lim	*National University of Singapore*
		Dr Lim Hoon Wei	*Trustwave Pte Ltd*
		Mr Lin Yih	*Digital Applied Research & Technology Pte Ltd*
		Dr Vishram Mishra	*Microsec Pte Ltd*
		Mr David Ng	*Assurity Trusted Solutions Pte Ltd*
		Mr Henry Tan	*Cyber Security Agency of Singapore*
		Mr Aruna Withane	*Google*
		Mr Wong Onn Chee	*Resolvo Systems Pte Ltd*
		Dr Yang Yanjiang	*Huawei Singapore*
		Mr You Cheng Hwee	*Maximus Consulting Pte Ltd*
		Dr Zhou Jianying	*Singapore University of Technology and Design*

(blank page)

Contents

National Foreword

This Singapore Standard was prepared by the Technical Committee on Security and Privacy under the purview of the IT Standards Committee.

This standard is identical with ISO/IEC 27001:2013, "Information technology – Security techniques – Information security management systems – Requirements", published by the International Organization for Standardization, and incorporates the Technical Corrigendum 1 (September 2014) and Technical Corrigendum 2 (December 2015)

Where appropriate, the words "International Standard" shall be read as "Singapore Standard" and the reference to "ISO/IEC 27002" shall be replaced "SS ISO/IEC 27002".

Attention is drawn to the possibility that some of the elements of this Singapore Standard may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions.*

2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR.*

3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27001 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 27001:2005), which has been technically revised.

0 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.

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*