
**Information technology — Security
techniques — Information security
management systems — Overview and
vocabulary**

*Technologies de l'information — Techniques de sécurité — Systèmes
de gestion de la sécurité des informations — Vue d'ensemble et
vocabulaire*

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
0 Introduction	v
1 Scope	1
2 Terms and definitions	1
3 Information security management systems	6
3.1 Introduction	6
3.2 What is an ISMS?	7
3.3 Process approach	8
3.4 Why an ISMS is important	9
3.5 Establishing, monitoring, maintaining and improving an ISMS	10
3.6 ISMS critical success factors	11
3.7 Benefits of the ISMS family of standards	11
4 ISMS family of standards	12
4.1 General information	12
4.2 Standards describing an overview and terminology	13
4.3 Standards specifying requirements	13
4.4 Standards describing general guidelines	14
4.5 Standards describing sector-specific guidelines	15
Annex A (informative) Verbal forms for the expression of provisions	16
Annex B (informative) Categorized terms	17
Bibliography	19

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 27000 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

0 Introduction

0.1 Overview

International Standards for management systems provide a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art. ISO/IEC JTC 1 SC 27 maintains an expert committee dedicated to the development of international management systems standards for information security, otherwise known as the Information Security Management System (ISMS) family of standards.

Through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets and prepare for an independent assessment of their ISMS applied to the protection of information, such as financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties.

0.2 ISMS family of standards

The ISMS family of standards¹⁾ is intended to assist organizations of all types and sizes to implement and operate an ISMS. The ISMS family of standards consists of the following International Standards, under the general title *Information technology — Security techniques*:

- ISO/IEC 27000:2009, *Information security management systems — Overview and vocabulary*
- ISO/IEC 27001:2005, *Information security management systems — Requirements*
- ISO/IEC 27002:2005, *Code of practice for information security management*
- ISO/IEC 27003, *Information security management system implementation guidance*
- ISO/IEC 27004, *Information security management — Measurement*
- ISO/IEC 27005:2008, *Information security risk management*
- ISO/IEC 27006:2007, *Requirements for bodies providing audit and certification of information security management systems*
- ISO/IEC 27007, *Guidelines for information security management systems auditing*
- ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

NOTE The general title “*Information technology — Security techniques*” indicates that these standards were prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

International Standards not under the same general title that are also part of the ISMS family of standards are as follows:

- ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

1) Standards identified throughout this subclause with no release year indicated are still under development.

0.3 Purpose of this International Standard

This International Standard provides an overview of information security management systems, which form the subject of the ISMS family of standards, and defines related terms.

NOTE Annex A provides clarification on how verbal forms are used to express requirements and/or guidance in the ISMS family of standards.

The ISMS family of standards includes standards that:

- a) define requirements for an ISMS and for those certifying such systems;
- b) provide direct support, detailed guidance and/or interpretation for the overall Plan-Do-Check-Act (PDCA) processes and requirements;
- c) address sector-specific guidelines for ISMS; and
- d) address conformity assessment for ISMS.

The terms and definitions provided in this International Standard:

- cover commonly used terms and definitions in the ISMS family of standards;
- will not cover all terms and definitions applied within the ISMS family of standards; and
- do not limit the ISMS family of standards in defining terms for own use.

Standards addressing only the implementation of controls, as opposed to addressing all controls, from ISO/IEC 27002 are excluded from the ISMS family of standards.

To reflect the changing status of the ISMS family of standards, this International Standard is expected to be continually updated on a more frequent basis than would normally be the case for other ISO/IEC standards.

Information technology — Security techniques — Information security management systems — Overview and vocabulary

1 Scope

This International Standard provides:

- a) an overview of the ISMS family of standards;
- b) an introduction to information security management systems (ISMS);
- c) a brief description of the Plan-Do-Check-Act (PDCA) process; and
- d) terms and definitions for use in the ISMS family of standards.

This International Standard is applicable to all types of organization (e.g. commercial enterprises, government agencies, non-profit organizations).