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

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



This document is a preview generated by EMS



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Information security management systems	11
4.1 General	11
4.2 What is an ISMS?	11
4.2.1 Overview and principles	11
4.2.2 Information	12
4.2.3 Information security	12
4.2.4 Management	12
4.2.5 Management system	13
4.3 Process approach	13
4.4 Why an ISMS is important	13
4.5 Establishing, monitoring, maintaining and improving an ISMS	14
4.5.1 Overview	14
4.5.2 Identifying information security requirements	14
4.5.3 Assessing information security risks	15
4.5.4 Treating information security risks	15
4.5.5 Selecting and implementing controls	15
4.5.6 Monitor, maintain and improve the effectiveness of the ISMS	16
4.5.7 Continual improvement	16
4.6 ISMS critical success factors	17
4.7 Benefits of the ISMS family of standards	17
5 ISMS family of standards	18
5.1 General information	18
5.2 Standard describing an overview and terminology: ISO/IEC 27000 (this document)	19
5.3 Standards specifying requirements	19
5.3.1 ISO/IEC 27001	19
5.3.2 ISO/IEC 27006	20
5.3.3 ISO/IEC 27009	20
5.4 Standards describing general guidelines	20
5.4.1 ISO/IEC 27002	20
5.4.2 ISO/IEC 27003	20
5.4.3 ISO/IEC 27004	21
5.4.4 ISO/IEC 27005	21
5.4.5 ISO/IEC 27007	21
5.4.6 ISO/IEC TR 27008	21
5.4.7 ISO/IEC 27013	22
5.4.8 ISO/IEC 27014	22
5.4.9 ISO/IEC TR 27016	22
5.4.10 ISO/IEC 27021	22
5.5 Standards describing sector-specific guidelines	23
5.5.1 ISO/IEC 27010	23
5.5.2 ISO/IEC 27011	23
5.5.3 ISO/IEC 27017	23
5.5.4 ISO/IEC 27018	24
5.5.5 ISO/IEC 27019	24
5.5.6 ISO 27799	25
Bibliography	26

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

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

This fifth edition cancels and replaces the fourth edition (ISO/IEC 27000:2016), which has been technically revised. The main changes compared to the previous edition are as follows:

- the Introduction has been reworded;
- some terms and definitions have been removed;
- [Clause 3](#) has been aligned on the high-level structure for MSS;
- [Clause 5](#) has been updated to reflect the changes in the standards concerned;
- Annexes A and B have been deleted.

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, including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information.

0.2 Purpose of this document

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 process to establish, implement, maintain, and improve an ISMS;
- c) address sector-specific guidelines for ISMS; and
- d) address conformity assessment for ISMS.

0.3 Content of this document

In this document, the following verbal forms are used:

- “shall” indicates a requirement;
- “should” indicates a recommendation;
- “may” indicates a permission;
- “can” indicates a possibility or a capability.

Information marked as “NOTE” is for guidance in understanding or clarifying the associated requirement. “Notes to entry” used in Clause 3 provide additional information that supplements the terminological data and can contain provisions relating to the use of a term.

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

1 Scope

This document provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

The terms and definitions provided in this document

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

2 Normative references

There are no normative references in this document.

3 Terms and definitions

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

access control

means to ensure that access to assets is authorized and restricted based on business and security requirements (3.56)

3.2

attack

attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

3.3

audit

systematic, independent and documented *process* (3.54) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the organization itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.