

INTERNATIONAL STANDARD

ISO/IEC 27007

First edition
2011-11-15

Information technology — Security techniques — Guidelines for information security management systems auditing

*Technologies de l'information — Techniques de sécurité — Lignes
directrices pour l'audit des systèmes de management de la sécurité de
l'information*

Reference number
ISO/IEC 27007:2011(E)





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

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	v
Introduction.....	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Principles of auditing	1
5 Managing an audit programme	1
5.1 General	1
5.1.1 IS 5.1 General	2
5.2 Establishing the audit programme objectives	2
5.2.1 IS 5.2 Establishing the audit programme objectives	2
5.3 Establishing the audit programme	2
5.3.1 Role and responsibilities of the person managing the audit programme	2
5.3.2 Competence of the person managing the audit programme	2
5.3.3 Determining the extent of the audit programme	2
5.3.4 Identifying and evaluating audit programme risks	3
5.3.5 Establishing procedures for the audit programme	3
5.3.6 Identifying audit programme resources	3
5.4 Implementing the audit programme	3
5.4.1 General	3
5.4.2 Defining the objectives, scope and criteria for an individual audit	3
5.4.3 Selecting the audit methods	4
5.4.4 Selecting the audit team members	4
5.4.5 Assigning responsibility for an individual audit to the audit team leader	5
5.4.6 Managing the audit programme outcome	5
5.4.7 Managing and maintaining audit programme records	5
5.5 Monitoring the audit programme	5
5.6 Reviewing and improving the audit programme	5
6 Performing an audit	5
6.1 General	5
6.2 Initiating the audit	5
6.2.1 General	5
6.2.2 Establishing initial contact with the auditee	5
6.2.3 Determining the feasibility of the audit	5
6.3 Preparing audit activities	6
6.3.1 Performing document review in preparation for the audit	6
6.3.2 Preparing the audit plan	6
6.3.3 Assigning work to the audit team	6
6.3.4 Preparing work documents	6
6.4 Conducting the audit activities	6
6.4.1 General	6
6.4.2 Conducting the opening meeting	6
6.4.3 Performing document review while conducting the audit	6
6.4.4 Communicating during the audit	6
6.4.5 Assigning roles and responsibilities of guides and observers	6
6.4.6 Collecting and verifying information	6
6.4.7 Generating audit findings	7
6.4.8 Preparing audit conclusions	7
6.4.9 Conducting the closing meeting	7

6.5	Preparing and distributing the audit report	7
6.5.1	Preparing the audit report.....	7
6.5.2	Distributing the audit report	7
6.6	Completing the audit	7
6.7	Conducting audit follow-up	7
7	Competence and evaluation of auditors	7
7.1	General.....	7
7.2	Determining auditor competence to fulfil the needs of the audit programme	7
7.2.1	General.....	7
7.2.2	Personal behaviour	8
7.2.3	Knowledge and skills	8
7.2.4	Achieving auditor competence	9
7.2.5	Audit team leader.....	9
7.3	Establishing the auditor evaluation criteria.....	9
7.4	Selecting the appropriate auditor evaluation method	9
7.5	Conducting auditor evaluation.....	9
7.6	Maintaining and improving auditor competence.....	9
Annex A (informative) Practice Guidance for ISMS Auditing		10
Bibliography.....		27

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 27007 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

This International Standard provides guidance on the management of an information security management system (ISMS) audit programme and the conduct of the internal or external audits in accordance with ISO/IEC 27001:2005, as well as guidance on the competence and evaluation of ISMS auditors, which should be used in conjunction with the guidance contained in ISO 19011. This International Standard does not state requirements.

This guidance is intended for all users, including small and medium sized organizations.

ISO 19011, *Guidelines for auditing management systems* provides guidance on the management of audit programmes, the conduct of internal or external audits of management systems, as well as on the competence and evaluation of management system auditors.

The text in this International Standard follows the structure of ISO 19011, and the additional ISMS-specific guidance on the application of ISO 19011 for ISMS audits is identified by the letters “IS”.

Information technology — Security techniques — Guidelines for information security management systems auditing

1 Scope

This International Standard provides guidance on managing an information security management system (ISMS) audit programme, on conducting the audits, and on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011.

This International Standard is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.

2 Normative references

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

ISO 19011:2011, *Guidelines for auditing management systems*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*