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 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

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*