TECHNICAL REPORT

ISO/IEC TR 27008

First edition
2011-10-15

Information technology — Security techniques — Guidelines for auditors on information security controls

Technologies de l'information — Techniques de sécurité — Lignes directrices pour les auditeurs des contrôles de sécurité de l'information

Reference number
ISO/IEC TR 27008:2011(E)

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.

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

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 TR 27008 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

This Technical Report supports the Information Security Management System (ISMS) risk management process defined within ISO/IEC 27001 and ISO/IEC 27005, and the controls included in ISO/IEC 27002.

This Technical Report provides guidance on reviewing an organization's information security controls, e.g. in the organization, business processes and system environment, including technical compliance checking.

Please refer to ISO/IEC 27007 for advice on auditing the management systems elements, and ISO/IEC 27006 regarding ISMS compliance reviewing for certification purposes.

Information technology — Security techniques — Guidelines for auditors on information security controls

1 Scope

This Technical Report provides guidance on reviewing the implementation and operation of controls, including technical compliance checking of information system controls, in compliance with an organization's established information security standards.

This Technical Report is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations conducting information security reviews and technical compliance checks. This Technical Report is not intended for management systems audits.

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

3.1
review object
specific item being reviewed

3.2
review objective
statement describing what is to be achieved as a result of a review

3.3
security implementation standard
document specifying authorized ways for realizing security

4 Structure of this Technical Report

This Technical Report contains a description of the information security control review process including technical compliance checking.

Background information is provided in Clause 5.