INTERNATIONAL STANDARD

ISO/IEC 27007

Third edition
2020-01

Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

Sécurité de l'information, cybersécurité et protection des données privées — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

Reference number
ISO/IEC 27007:2020(E)

© ISO/IEC 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

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
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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
5.2 Establishing audit programme objectives 1
5.3 Determining and evaluating audit programme risks and opportunities 2
5.4 Establishing audit programme 2
5.4.1 Roles and responsibilities of the individual(s) managing audit programme 2
5.4.2 Competence of individual(s) managing audit programme 2
5.4.3 Establishing extent of the audit programme 2
5.4.4 Determining audit programme resources 3
5.5 Implementing audit programme 3
5.5.1 General 3
5.5.2 Defining the objectives, scope and criteria for an individual audit 3
5.5.3 Selecting and determining audit methods 4
5.5.4 Selecting audit team members 4
5.5.5 Assigning responsibility for an individual audit to the audit team leader 4
5.5.6 Managing audit programme results 4
5.5.7 Managing and maintaining audit programme records 4
5.6 Monitoring audit programme 5
5.7 Reviewing and improving audit programme 5
6 Conducting an audit **5**
6.1 General 5
6.2 Initiating audit 5
6.2.1 General 5
6.2.2 Establishing contact with auditee 5
6.2.3 Determining feasibility of audit 5
6.3 Preparing audit activities 5
6.3.1 Performing review of documented information 5
6.3.2 Audit planning 5
6.3.3 Assigning work to audit team 6
6.3.4 Preparing documented information for audit 6
6.4 Conducting audit activities 6
6.4.1 General 6
6.4.2 Assigning roles and responsibilities of guides and observers 6
6.4.3 Conducting opening meeting 6
6.4.4 Communicating during audit 6
6.4.5 Audit information availability and access 6
6.4.6 Reviewing document information while conducting audit 6
6.4.7 Collecting and verifying information 7
6.4.8 Generating audit findings 7
6.4.9 Determining audit conclusions 7
6.4.10 Conducting closing meeting 7
6.5 Preparing and distributing audit report 7
6.5.1 Preparing audit report 7
6.5.2 Distributing audit report 7
6.6 Completing audit 7
6.7 Conducting audit follow-up 7

© ISO/IEC 2020 – All rights reserved

7 Competence and evaluation of auditors **8**
7.1 General 8
7.2 Determining auditor competence 8
7.2.1 General 8
7.2.2 Personal behaviour 8
7.2.3 Knowledge and skills 8
7.2.4 Achieving auditor competence 9
7.2.5 Achieving audit team leader competence 9
7.3 Establishing auditor evaluation criteria 9
7.4 Selecting appropriate auditor evaluation method 9
7.5 Conducting auditor evaluation 9
7.6 Maintaining and improving auditor competence 9
Annex A (informative) **Guidance for ISMS auditing practice** **10**
Bibliography **39**

 © ISO/IEC 2020 – All rights reserved

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.

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 document 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 and IEC 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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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

For an explanation of 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 www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27007:2017), which has been technically revised.

The main changes compared to the previous edition are as follows:

— the document has been aligned with ISO 19011:2018;

— the Introduction has been reworded and expanded;

— in 5.1, the entire text has been removed;

— in 5.2.2, the former item d) has been removed;

— in 5.3, the entire text has been removed;

— in 5.5.2.2, the former item b) and a paragraph below has been removed;

— in 6.5.2.2, the first paragraph has been removed and the NOTE reworded.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2020 – All rights reserved

Introduction

An information security management system (ISMS) audit can be conducted against a range of audit criteria, separately or in combination, including but not limited to:

— requirements defined in ISO/IEC 27001:2013;

— policies and requirements specified by relevant interested parties;

— statutory and regulatory requirements;

— ISMS processes and controls defined by the organization or other parties;

— management system plan(s) relating to the provision of specific outputs of an ISMS (e.g. plans to address risks and opportunities when establishing ISMS, plans to achieve information security objectives, risk treatment plans, project plans).

This document provides guidance for all sizes and types of organizations and ISMS audits of varying scopes and scales, including those conducted by large audit teams, typically of larger organizations, and those by single auditors, whether in large or small organizations. This guidance should be adapted as appropriate to the scope, complexity and scale of the ISMS audit programme.

This document concentrates on ISMS internal audits (first party) and ISMS audits conducted by organizations on their external providers and other external interested parties (second party). This document can also be useful for ISMS external audits conducted for purposes other than third party management system certification. ISO/IEC 27006 provides requirements for auditing ISMS for third party certification; this document can provide useful additional guidance.

This document is to be used in conjunction with the guidance contained in ISO 19011:2018.

This document follows the structure of ISO 19011:2018.

ISO 19011:2018 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.

Annex A provides guidance for ISMS auditing practices along with requirements of ISO/IEC 27001:2013, Clauses 4 to 10.

© ISO/IEC 2020 – All rights reserved

Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

1 Scope

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

This document 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 documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 19011:2018, *Guidelines for auditing management systems*

ISO/IEC 27000:2018, *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 19011 and ISO/IEC 27000 apply.

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 http://www.electropedia.org/

4 Principles of auditing

The principles of auditing of ISO 19011:2018, Clause 4, apply.

5 Managing an audit programme

5.1 General

The guidelines of ISO 19011:2018, 5.1, apply.

5.2 Establishing audit programme objectives

5.2.1 The guidelines of ISO 19011:2018, 5.2, apply. In addition, the guidance in 5.2.2 applies.

© ISO/IEC 2020 – All rights reserved