TECHNICAL SPECIFICATION

ISO/IEC TS 27006-2

First edition
2021-02

Requirements for bodies providing audit and certification of information security management systems —

Part 2: Privacy information management systems

Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management des informations de sécurité —

Partie 2: Systèmes de management des informations de sécurité

Reference number
ISO/IEC TS 27006-2:2021(E)

© ISO/IEC 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

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
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 **2**
5 General requirements **2**
5.1 Legal and contractual matters 2
5.2 Management of impartiality 2
5.3 Liability and financing 2
6 Structural requirements **2**
7 Resource requirements **2**
7.1 Competence of personnel 2
7.1.1 PS 7.1.1 General considerations 2
7.1.2 PS 7.1.2 Determination of competence criteria 2
7.2 Personnel involved in the certification activities 3
7.2.1 PS 7.2 Demonstration of auditor knowledge and experience 4
7.2.2 PS 7.2.1.1 Selecting auditors 4
7.3 Use of individual external auditors and external technical experts 4
7.4 Personnel records 4
7.5 Outsourcing 4
8 Information requirements **4**
8.1 Public information 4
8.2 Certification documents 4
8.2.1 PS 8.2 PIMS Certification documents 4
8.3 Reference to certification and use of marks 5
8.4 Confidentiality 5
8.5 Information exchange between a certification body and its clients 5
9 Process requirements **5**
9.1 Pre-certification activities 5
9.1.1 Application 5
9.1.2 Application review 5
9.1.3 Audit programme 5
9.1.4 Determining audit time 6
9.1.5 Multi-site sampling 7
9.1.6 Multiple management systems 7
9.2 Planning audits 7
9.2.1 Determining audit objectives, scope and criteria 7
9.2.2 Audit team selection and assignments 7
9.2.3 Audit plan 7
9.3 Initial certification 7
9.4 Conducting audits 7
9.4.1 IS 9.4 General 7
9.4.2 IS 9.4 Specific elements of the ISMS audit 7
9.4.3 IS 9.4 Audit report 7
9.5 Certification decision 7
9.6 Maintaining certification 8
9.6.1 General 8
9.6.2 Surveillance activities 8
9.6.3 Re-certification 8
9.6.4 Special audits 8

© ISO/IEC 2021 – All rights reserved

9.6.5 Suspending, withdrawing or reducing the scope of certification ... 8
9.7 Appeals ... 8
9.8 Complaints ... 8
9.9 Client records ... 8
10 Management system requirements for certification bodies ... 8
10.1 Options ... 8
10.2 Option A: General management system requirements ... 8
10.3 Option B: Management system requirements in accordance with ISO 9001 ... 9

© ISO/IEC 2021 – 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 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/JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 27006 series can be found on the ISO website.

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 2021 – All rights reserved

Introduction

ISO/IEC 27006 sets out criteria for bodies providing audit and certification of information security management systems. If such bodies are also to be accredited as complying with ISO/IEC 27006 with the objective of auditing and certifying privacy information management systems (PIMS) in accordance with ISO/IEC 27701:2019, some additional requirements and guidance to ISO/IEC 27006 are necessary. These are provided by this document.

The text in this document follows the structure of ISO/IEC 27006 and the additional PIMS-specific requirements and guidance on the application of ISO/IEC 27006 for PIMS certification are identified by the letters “PS”.

The primary purpose of this document is to enable accreditation bodies to more effectively harmonize their application of the standards against which they are bound to assess certification bodies.

© ISO/IEC 2021 – All rights reserved

Requirements for bodies providing audit and certification of information security management systems —

Part 2:
Privacy information management systems

1 Scope

This document specifies requirements and provides guidance for bodies providing audit and certification of a privacy information management system (PIMS) according to ISO/IEC 27701 in combination with ISO/IEC 27001, in addition to the requirements contained within ISO/IEC 27006 and ISO/IEC 27701. It is primarily intended to support the accreditation of certification bodies providing PIMS certification.

The requirements contained in this document need to be demonstrated in terms of competence and reliability by anybody providing PIMS certification, and the guidance contained in this document provides additional interpretation of these requirements for any body providing PIMS certification.

NOTE This document can be used as a criteria document for accreditation, peer assessment or other audit processes.

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/IEC 17021-1, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

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

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

ISO/IEC 27006:2015, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17021-1, ISO/IEC 27000, ISO/IEC 27006 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/

© ISO/IEC 2021 – All rights reserved