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 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

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.

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.

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/

4 Principles

The principles from ISO/IEC 27006:2015, Clause 4, apply.

5 General requirements

5.1 Legal and contractual matters

The requirements of ISO/IEC 27006:2015, 5.1 apply. In addition, the following requirements and guidance apply.

PS 5.1 Normative basis for this document

All requirements from ISO/IEC 27006 apply unless otherwise specified in this document.

5.2 Management of impartiality

The requirements of ISO/IEC 27006:2015, 5.2, apply. In addition, the following requirements and guidance apply.

PS 5.2 Conflicts of interest

The certification body shall not provide management system consultancy related to PIMS (e.g. services as external data protection officer, process reviews or data protection reviews).

Arranging and participating as lecturer in training courses related to personal information security management systems is not considered consultancy or having a potential conflict of interest, provided that the provisions of ISO/IEC 27006:2015, 5.2.1 a), are applied.

5.3 Liability and financing

The requirements of ISO/IEC 27006:2015, 5.3, apply.

6 Structural requirements

The requirements of ISO/IEC 27006:2015, Clause 6, apply.

7 Resource requirements

7.1 Competence of personnel

7.1.1 PS 7.1.1 General considerations

The requirements of ISO/IEC 27006:2015, 7.1.1, apply.

7.1.2 PS 7.1.2 Determination of competence criteria

The requirements of ISO/IEC 27006:2015, 7.1.2, apply. In addition, the following requirements and guidance apply.

7.1.2.1 PS 7.1.2.1 Competence requirements for PIMS auditing

7.1.2.1.1 The auditors shall have knowledge of:

a) privacy information management including ISO/IEC 27701;

b) identification and handling of personally identifiable information (PII);

c) privacy by design and by default;

d) PIMS monitoring, measurement, analysis and evaluation;

e) information security risks related to privacy information management and processing of PII;

f) policies and business requirements for privacy information management.

7.1.2.1.2 Collectively, the members of the audit team shall have knowledge of:

a) privacy information management and processing of PII related tools, methods, techniques and their application;

b) tracing privacy incidents;

c) privacy information risk assessment, privacy impact assessment and the related methods and risk management;

d) processes applicable to PIMS;

e) the current technology where privacy may be relevant or an issue;

f) all controls contained in ISO/IEC 27701 and their implementation;

g) the legal requirements that apply to privacy information management and/or processing of PII (e.g. sector specific laws and local privacy laws);

NOTE Knowledge of legal and regulatory requirements does not imply a specific educational degree in judicial or related study programmes.

h) industry privacy good practices and privacy procedures.

7.1.2.2 PS 7.1.2.4 Competence requirements for reviewing audit reports and making certification decisions

The personnel reviewing audit reports and making certification decisions shall have knowledge of:

a) the privacy framework presented in ISO/IEC 29100;

b) ISO/IEC 27701;

c) legal and regulatory requirements relevant to privacy;

NOTE Knowledge of legal and regulatory requirements does not imply a specific educational degree in judicial or related study programmes.

d) scope definition for management systems according to ISO/IEC 27701 (in particular in terms of PII controllers and PII processors) to be able to verify the appropriateness of the scope as well as changes to the scope.

The personnel reviewing audit reports and making certification decisions shall have general understanding of:

a) privacy information risk assessment, privacy impact assessment and risk management;

b) processes applicable to PIMS.

7.2 Personnel involved in the certification activities

The requirements of ISO/IEC 27006:2015, 7.2, apply. In addition, the following requirements and guidance apply.

7.2.1 PS 7.2 Demonstration of auditor knowledge and experience

The certification body shall demonstrate that the auditors have necessary knowledge and experience through (where applicable):

a) recognized PIMS-specific qualifications;

b) participation in PIMS training courses and attainment of relevant personal credentials;

c) PIMS audits witnessed by another PIMS auditor.

7.2.2 PS 7.2.1.1 Selecting auditors

In addition to 7.1.2.1, the criteria for selecting PIMS auditors shall ensure that each auditor:

a) has at least four years full-time practical workplace experience in information technology, of which at least two years was in a role or function relating to privacy;

b) has completed at least one onsite audit in the field of PIMS;

NOTE If the auditors are qualified in the field of ISMS and PIMS, they meet the requirements of ISO/IEC 27006:2015, 7.2.1.1 d), through the audits within the two fields.

c) keep current knowledge and skills in privacy information management up to date through continual professional development.

Technical experts shall comply with a).

7.3 Use of individual external auditors and external technical experts

The requirements of ISO/IEC 27006:2015, 7.3, apply.

7.4 Personnel records

The requirements of ISO/IEC 27006:2015, 7.4, apply.

7.5 Outsourcing

The requirements of ISO/IEC 27006:2015, 7.5, apply.

8 Information requirements

8.1 Public information

The requirements of ISO/IEC 27006:2015, 8.1, apply.

8.2 Certification documents

The requirements of ISO/IEC 27006:2015, 8.2, apply. In addition, the following requirements and guidance apply.

8.2.1 PS 8.2 PIMS Certification documents

The certification documents shall identify that the organization is either or both a PII controller and a PII processor within the scope of the certification.

Certification documents for ISO/IEC 27701 shall identify the ISO/IEC 27001 certification on which the ISO/IEC 27701 certification is based and that the organization conforms to ISO/IEC 27701.

The version of the statement of applicability (SoA) for ISO/IEC 27001 and, if issued separately, the SoA for ISO/IEC 27701 shall be included in the certification documents.

NOTE The SoA for ISO/IEC 27701 can be integrated with the SoA for ISO/IEC 27001, or produced separately from the SoA for ISO/IEC 27001.

The effective date of ISO/IEC 27701 certification shall not exceed the date of the ISO/IEC 27001 certification on which it is based.

The certification according to ISO/IEC 27001 may be obtained prior or in parallel to the ISO/IEC 27701 certification.

Certification documents shall include:

a) the words privacy information management system;

b) the role of the organization for each activity, product or service in scope (i.e. if the organization acts as PII controller and/or PII processor);

NOTE 1 An organization can deliver email services acting as PII processor and file sharing services acting as PII controller.

c) the fact that the certified organization fulfils both ISO/IEC 27001 and ISO/IEC 27701.

NOTE 2 The fact that the certified organization fulfils ISO/IEC 27001 can be satisfied by the inclusion of the identification of ISO/IEC 27001 (e.g. certification number of ISO/IEC 27001) in the certificate.

8.3 Reference to certification and use of marks

The requirements of ISO/IEC 27006:2015, 8.3, apply.

8.4 Confidentiality

The requirements of ISO/IEC 27006:2015, 8.4, apply.

8.5 Information exchange between a certification body and its clients

The requirements of ISO/IEC 27006:2015, 8.5, apply.

9 Process requirements

9.1 Pre-certification activities

9.1.1 Application

The requirements of ISO/IEC 27006:2015, 9.1.1, apply.

9.1.2 Application review

The requirements of ISO/IEC 27006:2015, 9.1.2, apply.

9.1.3 Audit programme

The requirements of ISO/IEC 27006:2015, 9.1.3, apply (except 9.1.3.6). In addition, the following requirements and guidance apply.

9.1.3.1 PS 9.1.3 Scope of certification

9.1.3.1.1 Scope of certification

The certification body shall ensure that the scope of the ISO/IEC 27701 certification is within or identical to the scope of the ISO/IEC 27001 certification.

The certification body shall ensure that the scope of certification to ISO/IEC 27701 is included within boundaries of the activities of the client as defined in the scope of the PIMS.

9.1.3.1.2 Specific elements of the PIMS audit

The audit programme for an ISO/IEC 27701 audit shall identify the role of the client with regard to PII controllers and PII processors.

The certification body shall confirm, in the scope of the client PIMS, that the PII processing is in the scope (see ISO/IEC 27701:2019, 5.2.3).

Certification bodies shall ensure that the client's information security and privacy risk assessment and risk treatment properly reflect its activities and extend to the boundaries of its activities as defined in the scope of the PIMS. Certification bodies shall confirm that this is reflected in the client's scope of their PIMS and statement of applicability.

9.1.3.2 PS 9.1.3 Certification audit criteria

The criteria against which the PIMS of a client is audited shall be ISO/IEC 27001 extended by ISO/IEC 27701. Other documents may be required for certification relevant to the function(s) performed.

9.1.4 Determining audit time

The requirements of ISO/IEC 27006:2015, 9.1.4, apply. In addition, the following requirements and guidance apply.

PS 9.1.4 Audit time

In addition to ISO/IEC 27006:2015, 9.1.4.1, the certification body shall identify the additional audit time to be spent on the ISO/IEC 27701 certification audits (including initial certification, surveillance and re-certification).

The audit time needed for PIMS-specific aspects shall be at least;

— 30 % of the audit time (if the audit client is a PII controller);

— 20 % of the audit time (if the audit client is a PII processor); or

— 50 % of the audit time (if the audit client is both PII controller and processor);

calculated for the identical ISO/IEC 27001 certification scope, based on ISO/IEC 27006:2015, 9.1.4 and Annex B.

The additional audit time for an initial PIMS audit (stage 1 and stage 2) shall be at least 2,5 days for PII processors, 3 days for PII controllers or 3,5 days for both, if the values calculated from the previous sentence are lower.

In the case that the organization has already been certified to ISMS (ISO/IEC 27001) and a PIMS initial audit is conducted separately from ISMS audits (i.e. ISMS surveillance audit or ISMS recertification audit), at least 0,5 audit days shall be added to the audit time in order to verify if the ISMS (especially its management system aspects such as internal audit and management review) is extended to include PIMS perspectives as specified in ISO/IEC 27701.

Additional audit days shall be calculated for each audit (i.e. surveillance audit, re-certification audit).

