FINAL DRAFT
International Standard

ISO/IEC FDIS 27706

Information technology, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of privacy information management systems

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2024-12-27

Voting terminates on:
2025-02-21

ISO/CEN PARALLEL PROCESSING

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/IEC FDIS 27706:2024(en)

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 3
5 General requirements 3
5.1 Legal and contractual matters 3
5.2 Management of impartiality 3
5.2.1 General considerations 3
5.2.2 Conflicts of interest 3
5.3 Liability and financing 3
6 Structural requirements 3
7 Resource requirements 3
7.1 Competence of personnel 3
7.1.1 General considerations 3
7.1.2 Determination of competence criteria 4
7.1.3 Evaluation processes 4
7.1.4 Other considerations 5
7.2 Personnel involved in the certification activities 5
7.3 Use of individual auditors and external technical experts 5
7.4 Personnel records 5
7.5 Outsourcing 5
8 Information Requirements 5
8.1 Public information 5
8.2 Certification documents 5
8.2.1 General 5
8.2.2 PIMS certification documents 5
8.3 Reference to certification and use of marks 5
8.4 Confidentiality 6
8.4.1 General 6
8.4.2 Access to organizational records 6
8.5 Information exchange between a certification body and its clients 6
9 Process requirements 6
9.1 Pre-certification activities 6
9.1.1 Application 6
9.1.2 Application review 6
9.1.3 Audit programme 6
9.1.4 Determining audit time 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 8
9.3.1 General 8
9.3.2 Initial certification audit 8
9.4 Conducting audits 9
9.4.1 General 9
9.4.2 Specific elements of the PIMS audit 9
9.4.3 Audit report 9
9.5 Certification decision 10

9.6 Maintaining certification 10
9.6.1 General 10
9.6.2 Surveillance activities 10
9.7 Appeals 10
9.8 Complaints 10
9.9 Client records 11

10 Management system requirements for certification bodies 11
10.1 Options 11
10.2 Option A: General management system requirements 11
10.3 Option B: Management system requirements in accordance with ISO 9001 11

Annex A (normative) **Audit time 12**

Annex B (informative) **Methods for audit time calculations 17**

Annex C (normative) **Required knowledge and skills 22**

Bibliography 24

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13, *Cybersecurity and data protection*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This first edition of ISO/IEC 27006 cancels and replaces ISO/IEC TS 27006-2:2021, which has been technically revised.

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 and www.iec.ch/national-committees.

Introduction

This document sets out requirements for bodies providing audit and certification of privacy information management systems in accordance with ISO/IEC 27701.

This document is also intended to assist accreditation bodies and peer assessors in being able to assess the minimum requirements for personnel competence in certification bodies and the processes of certification in these certification bodies in an efficient and harmonized way.

Information technology, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of 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 addition to the requirements contained within ISO/IEC 17021-1.

The requirements contained in this document are demonstrated in terms of competence and reliability by bodies providing PIMS certification. The guidance contained in this document provides additional interpretation of these requirements for bodies 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 17000, *Conformity assessment — Vocabulary and general principles*

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

ISO/IEC 27701:—[1], *Information security, cybersecurity and privacy protection—Privacy information management systems—Requirements and guidance*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17000, ISO/IEC 17021-1, ISO/IEC 27701, and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1
certification document

document indicating that a client's privacy information management system conforms to ISO/IEC 27701 and any supplementary documentation required under the management system

Note 1 to entry: This definition does not limit the number of documents collectively known as certification documents.

[SOURCE: ISO/IEC 27006-1:2024, 3.1, modified — the references to "information security management system" have been changed to "privacy information management system" and ISO/IEC 27001 to ISO/IEC 27701.]

[1] Under development. Stage at the time of publication: ISO/IEC DIS 27701:2024.

3.2
personally identifiable information
PII
information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or might be directly or indirectly linked to a natural person

Note 1 to entry: The “natural person” in the definition is the *PII principal* (3.4). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2024, 3.7]

3.3
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.2) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others [e.g. *PII processors* (3.5)] to *process PII* (3.8) on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100:2024, 3.8]

3.4
PII principal
data subject
natural person to whom the *personally identifiable information (PII)* (3.2) relates

[SOURCE: ISO/IEC 29100:2024, 3.9]

3.5
PII processor
privacy stakeholder that processes *personally identifiable information (PII)* (3.2) on behalf of and in accordance with the instructions of a *PII controller* (3.3)

[SOURCE: ISO/IEC 29100:2024, 3.10]

3.6
privacy information management system
PIMS
management system which addresses the protection of privacy as potentially affected by the *processing of personally identifiable information* (3.8)

[SOURCE: ISO/IEC 27701:—, 3.23]

3.7
privacy impact assessment
privacy risk assessment
overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of *personally identifiable information* (3.2), framed within an organization’s broader risk management framework

[SOURCE: ISO/IEC 29100:2024, 3.18]

3.8
processing of PII
operation or set of operations performed upon *personally identifiable information (PII)* (3.7)

Note 1 to entry: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.

[SOURCE: ISO/IEC 29100: 2024, 3.21]

3.9
statement of applicability
documentation of all necessary controls and justification for the inclusion or exclusion of such controls

[SOURCE: ISO/IEC 27701:—, 3.25]

4 Principles

The principles from ISO/IEC 17021-1:2015, Clause 4 shall apply.

5 General requirements

5.1 Legal and contractual matters

The requirements of ISO/IEC 17021-1:2015, 5.1 shall apply.

5.2 Management of impartiality

5.2.1 General considerations

The requirements of ISO/IEC 17021-1:2015, 5.2 shall apply.

5.2.2 Conflicts of interest

In addition to the requirements of ISO/IEC 17021-1:2015, 5.2.5, certification bodies shall not provide consulting for management systems related to privacy, data protection (e.g. in the form of an external data protection officer or data protection check) or privacy risk management.

Certification bodies may carry out the following activities without them being considered as consultancy or having a potential conflict of interest:

a) providing only generic and publicly available information when arranging and participating as a lecturer in training courses related to privacy information management systems, management systems or auditing;

b) adding value during certification and surveillance audits, e.g. by identifying opportunities for improvement, as they become evident during the audit.

5.3 Liability and financing

The requirements of ISO/IEC 17021-1:2015, 5.3 shall apply.

6 Structural requirements

The requirements of ISO/IEC 17021-1:2015, Clause 6 shall apply.

7 Resource requirements

7.1 Competence of personnel

7.1.1 General considerations

The requirements of ISO/IEC 17021-1:2015, 7.1.1 shall apply.

7.1.2 Determination of competence criteria

7.1.2.1 General

The requirements of ISO/IEC 17021-1:2015, 7.1.2 shall apply.

7.1.2.2 Generic competence requirements

The certification body shall define the competence requirements for each certification function as referenced in ISO/IEC 17021-1:2015, Table A.1.

The certification body shall also take into account the requirements specified in Annex C, for the PIMS technical areas.

The certification body shall consider the competence requirements for an audit team in information security in accordance with the requirements in ISO/IEC 27701.

NOTE ISO/IEC 27006-1:2024, 7.1.3 provides competence requirements for information security.

7.1.3 Evaluation processes

7.1.3.1 General

The requirements of ISO/IEC 17021-1:2015, 7.1.3 shall apply.

7.1.3.2 Evaluating auditors

The certification body shall demonstrate that the auditors have the necessary knowledge and experience through at least one of the following:

a) recognized PIMS-specific qualifications;

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

c) up-to-date professional development records;

d) PIMS audits witnessed by another competent and authorized PIMS auditor.

NOTE The knowledge and skills in privacy can include completion of PIMS audits under the supervision of other qualified PIMS auditors, as well as specific knowledge and skills in privacy information management systems.

7.1.3.3 Selecting auditors

In addition to 7.1.3.1, the process for selecting auditors shall ensure that each auditor:

a) has practical workplace experience in privacy to act as auditor for PIMS;

b) has received training regarding PIMS audit and audit management, and demonstrated skills of auditing a PIMS in accordance with to ISO/IEC 27701;

c) maintains relevant and current knowledge and skills in privacy information management and auditing through continual professional development.

7.1.3.4 Selecting technical experts

The process for selecting technical experts shall ensure that each technical expert:

a) has practical workplace experience in privacy to act as a technical expert;

b) maintains relevant and current knowledge and skills in privacy information management through continual professional development.

7.1.4 Other considerations

The requirements of ISO/IEC 17021-1:2015, 7.1.4 shall apply.

7.2 Personnel involved in the certification activities

The requirements of ISO/IEC 17021-1:2015, 7.2 shall apply.

7.3 Use of individual auditors and external technical experts

The requirements of ISO/IEC 17021-1:2015, 7.3 shall apply.

7.4 Personnel records

The requirements of ISO/IEC 17021-1:2015, 7.4 shall apply.

7.5 Outsourcing

The requirements of ISO/IEC 17021-1:2015, 7.5 shall apply.

8 Information Requirements

8.1 Public information

The requirements of ISO/IEC 17021-1-2015, 8.1 shall apply.

8.2 Certification documents

8.2.1 General

The requirements of ISO/IEC 17021-1-2015, 8.2 shall apply.

8.2.2 PIMS certification documents

Certification documents shall include:

a) the phrase “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 or PII processor or both)

c) the PII principals whose data are being processed for each activity, product or service in scope (e.g. employees, customers);

d) the version of the statement of applicability (SoA) for the organization’s PIMS.

NOTE A change to the statement of applicability which does not change the coverage of the controls in the scope of certification does not require an update of the certification documents.

Where no activity of the organization within the scope of the certification is undertaken at a defined physical location at all, the certification document(s) shall state that all activities of the organization are conducted remotely.

8.3 Reference to certification and use of marks

The requirements of ISO/IEC 17021-1-2015, 8.3 shall apply.