

---

---

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

**Part 2:  
Privacy information management  
systems**

iTeh STANDARD PREVIEW

(standards.iteh.ai)  
*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*

[https://standards.iteh.ai/catalog/standards/sist/e2877d47-98ed-4300-b007-  
e158d439607f/iso-iec-prf-ts-27006-2](https://standards.iteh.ai/catalog/standards/sist/e2877d47-98ed-4300-b007-e158d439607f/iso-iec-prf-ts-27006-2)

**PROOF / ÉPREUVE**

---

---



## iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC PRF TS 27006-2](https://standards.iteh.ai/catalog/standards/sist/e2877d47-98ed-4300-b007-e158d439607f/iso-iec-prf-ts-27006-2)  
[https://standards.iteh.ai/catalog/standards/sist/e2877d47-98ed-4300-b007-  
e158d439607f/iso-iec-prf-ts-27006-2](https://standards.iteh.ai/catalog/standards/sist/e2877d47-98ed-4300-b007-e158d439607f/iso-iec-prf-ts-27006-2)



### **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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
Foreword .....	v
Introduction .....	vi
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Principles</b> .....	<b>2</b>
<b>5 General requirements</b> .....	<b>2</b>
5.1 Legal and contractual matters .....	2
5.2 Management of impartiality .....	2
5.3 Liability and financing .....	2
<b>6 Structural requirements</b> .....	<b>2</b>
<b>7 Resource requirements</b> .....	<b>2</b>
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
<b>8 Information requirements</b> .....	<b>4</b>
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
<b>9 Process requirements</b> .....	<b>5</b>
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

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
<b>10</b>	<b>Management system requirements for certification bodies .....</b>	<b>8</b>
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

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC PRF TS 27006-2](https://standards.iteh.ai/catalog/standards/sist/e2877d47-98ed-4300-b007-e158d439607f/iso-iec-prf-ts-27006-2)  
<https://standards.iteh.ai/catalog/standards/sist/e2877d47-98ed-4300-b007-e158d439607f/iso-iec-prf-ts-27006-2>

## 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](http://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](http://www.iso.org/patents)) or the IEC list of patent declarations received (see [patents.iec.ch](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](http://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](http://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.

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC PRF TS 27006-2](https://standards.iteh.ai/catalog/standards/sist/e2877d47-98ed-4300-b007-e158d439607f/iso-iec-prf-ts-27006-2)

<https://standards.iteh.ai/catalog/standards/sist/e2877d47-98ed-4300-b007-e158d439607f/iso-iec-prf-ts-27006-2>

# 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.