DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27006-2

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2023-07-18

Voting terminates on:
2023-10-10

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

ICS: 03.120.20; 35.030

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

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.

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.

Reference number
ISO/IEC DIS 27006-2:2023(E)

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

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

© ISO/IEC 2023 – All rights reserved

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 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 3
7.1.2 General considerations 4
7.1.3 Determination of competence criteria 4
7.2 Personnel involved in the certification activities 5
7.2.1 General 5
7.2.2 Demonstration of auditor knowledge and experience 5
7.3 Use of individual external auditors and external technical experts 6
7.4 Personnel records 6
7.5 Outsourcing 6
8 Information requirements **6**
8.1 Public information 6
8.2 Certification documents 6
8.2.1 General 6
8.2.2 PIMS Certification documents 6
8.3 Reference to certification and use of marks 7
8.4 Confidentiality 7
8.5 Information exchange between a certification body and its clients 7
9 Process requirements **7**
9.1 Pre-certification activities 7
9.1.1 Application 7
9.1.2 Application review 7
9.1.3 Audit programme 7
9.1.4 Determining audit time 8
9.1.5 Multi-site sampling 8
9.1.6 Multiple management systems 8
9.2 Planning audits 8
9.2.1 Determining audit objectives, scope and criteria 8
9.2.2 Audit team selection and assignments 8
9.2.3 Audit plan 8
9.3 Initial certification 9
9.4 Conducting audits 9
9.4.1 General 9
9.4.2 Specific elements of the ISMS audit 9
9.4.3 Audit report 9
9.5 Certification decision 9
9.5.1 General 9

© ISO/IEC 2023 – All rights reserved

9.5.2 Certification decision ... 9
9.6 Maintaining certification ... 9
9.6.1 General ... 9
9.6.2 Surveillance activities ... 9
9.6.3 Re-certification ... 9
9.6.4 Special audits ... 9
9.6.5 Suspending, withdrawing or reducing the scope of certification ... 10
9.7 Appeals ... 10
9.8 Complaints ... 10
9.9 Client records ... 10
10 Management system requirements for certification bodies ... 10
10.1 Options ... 10
10.2 Option A: General management system requirements ... 10
10.3 Option B: Management system requirements in accordance with ISO 9001 ... 10
Annex A (normative) **Audit time ... 11**
Annex B (informative) **Methods for audit time calculations ... 14**
Bibliography ... 18

© ISO/IEC 2023 – 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*.

This second edition cancels and replaces the first edition (ISO/IEC TS 27006-2:2021) which has been technically revised.

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

— this document has been changed from a Technical Specification to an International Standard;

— the previous edition was aligned with ISO/IEC 27006:2015. The new structure and contents have been aligned with ISO/IEC 27006-1:202x;

— Annex A has been created.

— Annex B has been created.

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 2023 – All rights reserved

Introduction

ISO/IEC 27006-1 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 27006-1 with the objective of auditing and certifying privacy information management systems (PIMS) in accordance with ISO/IEC 27701, some additional requirements and guidance to ISO/IEC 27006-1 are necessary. These are provided by this document. The text in this document follows the structure of ISO/IEC 27006-1.

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.

[Editors' note: The revision of ISO/IEC 27006-1 was initiated, and accordingly 1st CD of ISO/IEC 27006-1 has been circulated for ballot by 2021-09-03. Drafts of ISO/IEC 27006-2 will be updated to keep consistency with the revision of ISO/IEC 27006-1.]

© ISO/IEC 2023 – 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 27006-1.

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.

[Editors' note: The text of this revised edition of ISO/IEC 27006-2 (including its scope) will be kept under review by ISO/CASCO throughout the project life-cycle. All comments and feedback from CASCO and its members will be discussed and resolved at WG 5 meetings. Also please note that the scope is consistent with ISO/IEC 27006:2015 and the consistency with the revision of ISO/IEC 27006 (i.e. 27006-1) will be kept during the revision of ISO/IEC 27006-2.]

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 27006-1:202x, *Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems – Part 1: General*

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

3 Terms and definitions

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

3.1
certification documents
documents indicating that a client's ISMS conforms to specified ISMS standards and any supplementary documentation required under the system

Note 1 to entry: In the context of this standard, the ISMS can be understood to include the PIMS.

[SOURCE: ISO/IEC 27006-1:202x, 3.1]

© ISO/IEC 2023 – All rights reserved