International Standard

ISO/IEC 27706

First edition
2025-10

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

Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la protection de la vie privée

Reference number
ISO/IEC 27706:2025(en)

COPYRIGHT PROTECTED DOCUMENT

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 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 27706 cancels and replaces ISO/IEC TS 27006-2:2021, which has been technically revised.

The main changes are as follows:

— the title has been modified;

— the clause numbering has been aligned to ISO/IEC 17021 rather than ISO/IEC 27006-1, in accordance with ISO/IEC 27701;

— Annexes A, B and C have been added.

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 security, 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 17021-1:2015, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

ISO/IEC 27701:2025, *Information security, cybersecurity and privacy protection—Privacy information management systems—Requirements and guidance*