SLOVENSKI STANDARD
oSIST prEN ISO/IEC 27006-2:2023

01-september-2023

Zahteve za organe, ki izvajajo presojanje in certificiranje sistemov upravljanja informacijske varnosti - 2. del: Sistemi za upravljanje informacij o zasebnosti (ISO/IEC/DIS 27006-2:2023)

Requirements for bodies providing audit and certification of information security management systems - Part 2: Privacy information management systems (ISO/IEC/DIS 27006-2:2023)

Anforderungen an Stellen, die Informationssicherheits-Managementsysteme auditieren und zertifizieren - Teil 2: Datenschutz-Managementsysteme (ISO/IEC/DIS 27006-2:2023)

Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information - Partie 2: Systèmes de management de la protection de la vie privée (ISO/IEC/DIS 27006-2:2023)

Ta slovenski standard je istoveten z: **prEN ISO/IEC 27006-2**

ICS:

03.120.20	Certificiranje proizvodov in podjetij. Ugotavljanje skladnosti	Product and company certification. Conformity assessment
35.030	Informacijska varnost	IT Security

oSIST prEN ISO/IEC 27006-2:2023 **en,fr,de**

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

Reference number
ISO/IEC DIS 27006-2:2023(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*.

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.

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.]

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]

3.2
personally identifiable information
PII
any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

Note 1 to entry: 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 identify that natural person.

[SOURCE: ISO/IEC 29100:2011, 2.9]

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

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

[SOURCE: ISO/IEC 29100:2011, 2.10]

3.4
PII principal
natural person to whom the personally identifiable information (PII) relates

Note 1 to entry: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2011, 2.11]

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

[SOURCE: ISO/IEC 29100:2011, 2.12]

3.6
privacy information management system
PIMS
information security management system which addresses the protection of privacy as potentially affected by the processing of PII

[SOURCE: ISO/IEC 27701:2019, 3.2]

3.7
privacy risk assessment
overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personally identifiable information (PII)

Note 1 to entry: This process is also known as a privacy impact assessment.

[SOURCE: ISO/IEC 29100:2011, 2.20]

3.8
privacy stakeholder
natural or legal person, public authority, agency or any other body that can affect, be affected by, or perceive themselves to be affected by a decision or activity related to personally identifiable information (PII) processing

[SOURCE: ISO/IEC 29100:2011, 2.22]

3.9
processing of PII
operation or set of operations performed upon personally identifiable information (PII)

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 29100:2011, 2.23]

4 Principles

The principles from ISO/IEC 27006-1:202x, Clause 4, apply.

5 General requirements

5.1 Legal and contractual matters

The requirements of ISO/IEC 27006-1:202x, 5.1 apply.

5.2 Management of impartiality

5.2.1 General

The requirements of ISO/IEC 27006-1:202x, 5.2.1, apply. In addition, the requirements and guidance in 5.2.2 apply.

5.2.2 Conflicts of interest

The certification body shall not provide management system consultancy related to PIMS (e.g. services as external data protection officer or the equivalent, consultations regarding management processes or data protection processes).

Arranging, or participating as a lecturer in, training courses related to personal information security management systems are not considered consultancy or having a potential conflict of interest, provided that the provisions of ISO/IEC 27006-1:202x, 5.2.2 a), are applied.

5.3 Liability and financing

The requirements of ISO/IEC 27006-1:202x, 5.3, apply.

6 Structural requirements

The requirements of ISO/IEC 27006-1:202x, Clause 6, apply.

7 Resource requirements

7.1 Competence of personnel

7.1.1 General

The requirements of ISO/IEC 27006-1:202x, 7.1.1, apply.