ISO/IEC 27006

Search

Search this site

ISO/IEC [TS] **27006** — Information technology — Security techniques — **Requirements for bodies providing audit and certification of information security management systems** *(two parts)*

Part 1

ISO/IEC 27006-1:2024 — Information technology, cybersecurity and privacy protection — **Requirements for bodies providing audit and certification of information security management systems — Part 1: General**
(fourth edition)

Abstract

"[ISO/IEC 27006-1] specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021-1.

The requirements contained in [ISO/IEC 27006-1] are demonstrated in terms of competence and reliability by bodies providing ISMS certification. The guidance contained in [ISO/IEC 27006-1] provides additional interpretation of these requirements for bodies providing ISMS certification.

NOTE [ISO/IEC 27006-1] can be used as a criteria document for accreditation, peer assessment or

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

other audit processes."

[Source: ISO/IEC 27006-1:2024]

Introduction

Part 1 of ISO/IEC 27006 is the **accreditation standard** that guides certification bodies on the formal processes they must follow when auditing their clients' **I**nformation **S**ecurity **M**anagement **S**ystems against ISO/IEC 27001 in order to certify or register them. The accreditation processes laid out in the standard give **assurance** that ISO/IEC 27001 certificates issued by accredited organisations are valid and meaningful.

Scope and purpose

The scope is to "specify requirements and provide guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification."

Any properly-accredited body providing ISO/IEC 27001 certificates *must* fulfill the requirements in ISO/IEC 27006 plus ISO/IEC 17021-1 and ISO 19011 in terms of their competence, suitability and reliability to perform their work properly. This is necessary to ensure that issued ISO/IEC 27001 certificates are meaningful, and truly indicate that the organisation has fully satisfied the requirements of ISO/IEC 27001. Since literally anyone can issue certificates without necessarily following the certification processes specified in this standard, even substantially non-conformant organisations could conceivably buy their ISMS certificates or simply 'self-certify' (assert rather than demonstrate conformity), discrediting the whole certification structure.

Content

ISO/IEC 27006-1 specifies requirements and provides guidance for conformity auditing specifically in the context of ISMSs, *in addition to* the general accreditation requirements laid down by ISO/IEC 17021-1 and ISO 19011.

The certification process involves auditing the information security *management system* for conformity with ISO/IEC 27001. The information security control set is "not used for conformity assessment", merely to determine that controls were included or excluded in accordance with ISO/IEC 27001 clause 6.1.3 d. A note to clause 9.1.1 states:

> *"It is possible for an organization to design its own necessary controls or to select them from any source, therefore it is possible that an organization is certified to ISO/IEC 27001 even though none of its necessary controls are those specified in ISO/IEC 27001:2022, Annex A."*

The standard follows the structure of ISO/IEC 27021-1 clause-by-clause, adding guidance specific to ISMS certifications where applicable - for example, in order to remain independent and objective, the certification body cannot also provide information security reviews or internal audits of the client's ISMS. [Since no period is specified, this could be interpreted as a permanent or indefinite exclusion.]

Status of the standard

The *first* edition of ISO/IEC 27006 was published in **2007**, incorporating and superseding the EA7/03 guidance on accredited certification processes.

The *second* edition was published in **2011**, reflecting changes to ISO 17021.

Following revisions to ISO/IEC 27001, ISO 19011 and ISO/IEC 17021-1, the current *third* edition was substantially revised and published in **2015**.

Minor wording changes were published as an amendment to the *third* edition in **2020.**

A second part was published in 2021 (see below).

The *fourth* edition was published as **ISO/IEC 27006-1** in **2024**. It builds upon two normative references - ISO/IEC 27021-1:2015 and ISO/IEC 27001:2022.

Meanwhile, SC 27 is working on the structure of ISO/IEC 27006-1 and other issues, including concerns raised but not entirely resolved in exchanges with CASCO.

See also ISO/IEC 27007 for guidance on auditing the management system element of an ISMS and ISO/IEC 27008 for guidance on auditing information security controls.

Personal comments

Certification auditors have only a passing interest in the organisation's information risks and information security controls that are being managed, sufficient to confirm that the ISMS is operational. It is largely assumed that any

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799

organisation with an operational ISMS in conformity with the standard is, in fact, managing its information risks diligently.

ISO/IEC 27001 gives organisations latitude on how they design and document their ISMS, and hence certification auditors cannot simply follow a straightforward conformity checklist: they need to understand *both* management systems *and* information risk and security concepts. As far as I'm concerned, that's a good thing!

The requirement to specify the SoA on ISO/IEC 27001 certificates has the unfortunate side-effect of impeding updating or maintaining an ISMS where that would affect the SoA *e.g.* responding to newly-identified information risks or to incorporate additional controls. Since that hampers a fundamental principle or purpose of having a management system, it may constitute a substantive defect in ISO/IEC 27006 ... and perhaps other ISO management system standards too.

Part 2

ISO/IEC TS 27006-2:2021 — Information security, cybersecurity and privacy protection — **Requirements for bodies providing audit and certification of information security management systems — Part 2: Privacy information management systems**

Abstract

"[ISO/IEC TS 27006-2] 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 [ISO/IEC 27006-2] need to be demonstrated in terms of competence and reliability by anybody providing PIMS certification, and the guidance contained in [ISO/IEC 27006-2] provides additional interpretation of these requirements for any body providing PIMS certification.

NOTE [ISO/IEC 27006-2] can be used as a criteria document for accreditation, peer assessment or other audit processes."

[Source: ISO/IEC TS 27006-2:2021]

Introduction

This **accreditation standard** guides certification bodies on the formal processes they must follow when auditing their clients' **P**rivacy **I**nformation **M**anagement **S**ystems against ISO/IEC 27701 and ISO/IEC 27001 in order to certify or register them. The accreditation processes laid out in the standard give **assurance** that ISO/IEC 27701 certificates issued by accredited organisations are valid, comparable and meaningful.

Scope and purpose

The scope of ISO/IEC TS 27006-2 is to:

> *"specify requirements and provide 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."*

This standard may also be used for peer assessment or other PIMS audit processes such as internal audits.

Any properly-accredited body providing ISO/IEC 27701 certificates *must* fulfill the requirements in this standard plus the following normative standards (the latest editions unless dated):

- 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 [see 'Part 1' above]*
- ISO/IEC 27701 — *Information technology — 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 (a free download!)*

Their competence, suitability and reliability to perform their work properly is necessary to ensure that issued ISO/IEC 27701 certificates are meaningful: if literally anyone were able to issue PIMS certificates without necessarily following the certification processes specified by this standard, even substantially non-conformant organisations could conceivably buy their certificates or simply 'self-certify' (assert rather than demonstrate conformity). Accreditation is an assurance control.

Content

The standard specifies formal requirements and offers guidance for conformity auditing specifically in the context of PIMSs, *in addition to* the general accreditation requirements laid down by ISO/IEC 17021-1 and the other normative standards.

Part 2 follows the structure of part 1 i.e.

Preamble, introduction, scope, normative references, definitions ...

4. Principles
5. General requirements
6. Structural requirements
7. Resource requirements
8. Information requirements
9. Process requirements
10. Management system requirements for certification bodies

Each section mostly has statements of the form "The requirements of ISO/IEC 27006-1, [section number] apply." This avoids duplication. 27006-2 is based firmly on 27006-1.

For some sections, additional requirements and guidance apply. For example, PIMS certification auditors obviously *need* to be familiar with ISO/IEC 27701 whereas ISMS certification auditors don't.

As with part 1, the certification process involves auditing the *management system* (specifically) for conformity with ISO/IEC 27701. Certification auditors have only a passing interest in the actual privacy arrangements that are being managed by the management system, doing sufficient checks to confirm that the PIMS is operational. It is *presumed* that any organisation with a PIMS that conforms to the standard probably does in fact have suitable privacy controls in place, thanks to the operation of said PIMS. More subtly, the standard does not demand particular, detailed privacy arrangements that may be inappropriate or insufficient if implemented in practice, and hopefully reduces the possibility of assertive certification auditors seeking to second-guess or override informed management decisions about how the organisation is addressing its privacy risks. The auditors' job is simply to provide assurance by assessing conformity with the mandatory requirements of the standard.

Status of the standard

The *first* edition of part 2 was published in **2021**.

The *second* edition is currently being developed with a new number: ISO/IEC 27706.

Personal comments

As with ISO/IEC 27001 ISMS certification, ISO/IEC 27006-2 concerns the *management system.* For certification, an organisation is formally required to *manage* its privacy arrangements in accordance with all the mandatory requirements of ISO/IEC 27701 ... which is subtly different from actually having all the appropriate privacy arrangements in place. For compliance/conformity auditors, the challenge is that 'appropriate' is not formally specified in ISO/IEC 27701 but is determined by the organisation itself.

The audit time anticipated for PIMS auditing is specified as a proportion of that needed for ISMS certification audits, paving the way for dual-certification for PIMS and ISMS. Personally, however, I am dubious about the need for the standards to specify audit time at all. I would feel more comfortable if accredited certification bodies' auditors determined it for themselves, in negotiation with their management and clients, taking account of factors such as the size and complexity of the organisation, the scope of the PIMS, the amount of assurance required by third parties likely to rely on the certificates, the client and auditors' liabilities if privacy breaches occur, and so

forth. Perhaps I am naive to think that auditors will plan and conduct their assignments professionally and competently, without bowing to commercial pressure from the clients ...

< Previous standard ^ Up a level ^ Next standard >