ISO/IEC 27701

Search

● Search this site

Home | ISO27k standards | FREE ISO27k Forum | FREE ISO27k Toolkit | FREE ISO27k FAQ | DONATE!

ISO/IEC 27000
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27006
ISO/IEC 27007
ISO/IEC TS 27008
ISO/IEC 27010
ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC 27019
ISO/IEC 27021
ISO/IEC TS 27022
ISO/IEC TR 27024
ISO/IEC TS 27028
ISO/IEC TR 27029
ISO/IEC 27031
ISO/IEC 27032
ISO/IEC 27033
ISO/IEC 27034
ISO/IEC 27035

< Previous standard ^ Up a level ^ Next standard >

ISO/IEC 27701:2019 — Information technology — Security techniques — **Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy information management — Requirements and guidelines** *(first edition)*

Abstract

> *"[ISO/IEC 27701] specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organisation.*
>
> *[ISO/IEC 27701] specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.*
>
> *[ISO/IEC 27701] is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS."*
>
> *[Source: ISO/IEC 27701:2019]*

Introduction

Although the fields of information security and privacy management substantially overlap, both go further. This standard explains how to 'enhance' (adapt and extend) an ISO/IEC 27001 **I**nformation **S**ecurity **M**anagement **S**ystem and the associated ISO/IEC 27002 controls to manage privacy as well as information security.

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

Scope of the standard

The standard specifies a **P**rivacy **I**nformation **M**anagement **S**ystem based on ISO/IEC 27001(ISMS), ISO/IEC 27002 (security controls) and ISO/IEC 29100 (privacy framework). It is applicable to both controllers and processors of **P**ersonally **I**dentifiable **I**nformation.

ISO/IEC 27701 builds and depends upon ISO/IEC 27001: organisations need to have an ISMS certified compliant to ISO/IEC 27001 in order for their PIMS to be certified compliant to ISO/IEC 27701.

Essentially the phrase ‘information security’ in ISO/IEC 27001 becomes ‘information security and privacy’.

Content of the standard

In the style of a sector-specific variant of ISO/IEC 27001, the ~70 page standard elaborates on the PIMS-related *differences* to the ISO/IEC 27001 and ISO/IEC 27002 standards clause-by-clause.

For example:

> *“ISO/IEC 27001:2013, 6.1.3.c) is refined as follows:*
>
> *The controls determined in 6.1.3 b) of ISO/IEC 27001:2013 shall be compared with those in ISO/IEC 27001:2013, Annex A and/or Annex B of [ISO/IEC 27701] to verify that no necessary controls have been omitted.*
>
> *When assessing the applicability of control objectives and controls from ISO/IEC 27001:2013 Annex A for the treatment of risks, the control objectives and controls shall be considered in the context of both risks to information security as well as risks related to the processing of PII, including risks to PII principals.”*

Status

The *first* edition was published in **2019**.

The standard is currently being updated, with a new title: “*Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance*”.

New The standard has been re-cast to specify a discrete PIMS rather than incorporating privacy within an ISMS. You can get a rough idea of what to expect by replacing “information security” with “privacy” in the main body of ISO/IEC 27001:2022, replacing Annex A with a generic catalogue of privacy control objectives and controls, and adding a further annex with PIMS implementation guidance (similar to ISO/IEC 27003).

New The *second* edition is at **F**inal **D**raft **I**nternational **S**tandard stage, and is scheduled for release *soon* (August 2025) once the remaining minor editorial issues are resolved.

Personal comments

Practitioners familiar with ‘the ISO27k way’ should have little difficulty applying the usual information risk management principles to personal information *i.e.*:

1. Identify privacy-related risks;
2. Evaluate them;
3. Decide how to treat them (what, if anything, to do about them);
4. Treat them (implement the risk-treatment decisions);
5. Lather, rinse, repeat.

Thanks to the standard elaborating on the requirements, even others ought to be able to have a jolly good stab at it.

An accompanying accreditation standard directs certification auditors on how to audit a PIMS and issue meaningful certificates for conformity with ISO/IEC 27701 - see ISO/IEC TS 27006-2. Note that, as with ISO/IEC 27001 ISMS certification, the emphasis is on verifying that the *management system* fulfills all the mandatory requirements of ISO/IEC 27701 ... which is subtly different from actually having all the appropriate privacy arrangements in place. For implementers and certification auditors alike, the challenge is that ‘appropriate’ is not laid out in ISO/IEC 27701 but is determined by the organisation itself. It is context-dependent.

< Previous standard ^ Up a level ^ Next standard >

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