ISO/IEC 27003

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 27003:2017 — Information technology — Security techniques — **Information security management systems — Guidance** *(second edition)*

Abstract

Summary podcast

> *"ISO/IEC 27003:2017 provides explanation and guidance on ISO/IEC 27001:2013."*
>
> *[Source: ISO/IEC 27003:2017]*

Introduction

ISO/IEC 27003 provides guidance for those implementing the ISO27k standards, covering the *management system* aspects in particular, as opposed to the information security controls which are summarised in ISO/IEC 27001 Annex A and explained more fully in ISO/IEC 27002.

The standard supplements and builds upon other standards, particularly ISO/IEC 27000 and ISO/IEC 27001 plus ISO/IEC 27004, ISO/IEC 27005, ISO 31000 and ISO/IEC 27014.

Purpose of the standard

As a result of ISO's directive to make all the **M**anagement **S**ystems **S**tandards consistent in structure and form, and in order for it to be usable for ISMS certification purposes, the language of ISO/IEC 27001:2013 is inevitably rather formal, curt and stilted. In contrast, ISO/IEC 27003 offers *pragmatic* explanation with *plain-speaking* advice and guidance for implementers of ISO/IEC 27001 (at least, that was the intention: arguably, the 2017 release fell short).

Structure and content of the standard

For convenience, ISO/IEC 27003 mirrors the structure of ISO/IEC 27001, expanding clause-by-clause on ISO/IEC 27001. The main sections are:

- 4 Context of the organisation
- 5 Leadership
- 6 Planning
- 7 Support
- 8 Operation
- 9 Performance evaluation

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

- 10 Improvement
- Annex - Policy framework [NOTE: this annex does *not* reflect or expand on the information security controls listed in ISO/IEC 27001 Annex A, since ISO/IEC 27002 already does that]

For each ISO/IEC 27001 clause, this standard:

- Re-states the requirement/s;
- Explains the implications; and
- Offers practical guidance and supporting information including examples, to help implementers implement.

For example, this is what ISO/IEC 27001 says in section 4.1, 'Understanding the organisation and its context':

> *"The organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.*
>
> *NOTE Determining these issues refers to establishing the external and internal context of the organisation considered in Clause 5.3 of ISO 31000:2009[5]."*

Section 4.1 of ISO/IEC 27003 first succinctly re-states the 'required activity':

> *"The organisation determines external and internal issues relevant to its purpose and affecting its ability to achieve the intended outcome(s) of the information security management system (ISMS)."*

Then it expands on the reasons *why* it is appropriate to 'determine external and internal issues', providing a page of explanation to supplement the succinct and somewhat hard to understand text from ISO/IEC 27001. It explains, for instance, that the 'internal issues' include the organisation's culture; its policies, objectives, and the strategies to achieve them; its governance, organisational structure, roles and responsibilities; and list a further seven 'internal issues' to consider. It also identifies/cross-references other clauses that use this information.

That alone would be a valuable expansion on ISO/IEC 27001 section 4.1 but ISO/IEC 27003 doesn't stop there: it goes on to provide a further page of explanation, practical guidance and real-world examples in this area.

The end result is that the reader gains a better understanding of the formal requirements from the main body clauses of ISO/IEC 27001 and a clearer idea of how to go about satisfying them.

Status of the standard

The *first* edition was published in **2010**.

A substantially revised *second* edition was issued in **2017.**

Work is under way now on a *third* edition, a project with three phases:

1. Update references and realign to the 2022 versions of ISO/IEC 27001 and ISO/IEC 27002; consolidate guidance into the Guidance sections for each clause; clarify the wording to avoid even *hinting* at additional ISMS requirements beyond those in ISO/IEC 27001, following rumoured CASCO concerns about implied conformity aspects.
2. Adopt ISO's version of plain English meaning substantial wording changes throughout, and expand ISO/IEC 27003 to cover the whole main body of ISO/IEC 27001 (but not the Annex A controls which are covered by ISO/IEC 27002).
3. Expand the implementation guidance, including brief introductions and references to related standards such as ISO/IEC 27004 and ISO/IEC 27005.

The revision project is presently at **W**orking **D**raft stage approaching phase 2. It is due to be published in 2027.

New A second part to this standard is due to be proposed at the SC27 meeting in September 2025. If approved, ISO/IEC 27003-2 would provide practical guidance on actually implementing an ISMS, for example "setting up an implementation project, suitable top management involvement in the steering committee, setting a clear ambition level, appointment of a suitable project manager, etc.", rejuvenating and updating the implementation advice from the 2010 first edition that has since been eroded.

Personal comments

Hot It takes *years* to prepare and release each new edition. *Meanwhile*, in the ISO27k Toolkit you will find the **ISO27k ISMS implementation guideline**, a plain-English explanation of the requirements from ISO/IEC 27001 (drawing heavily on the ISO Directives concerning the wording and intent of the boilerplate text for ISO's management systems) with pragmatic guidance for implementers (based on actual experience). The guideline is *not* an ISO/IEC standard but, hey, it's free of charge ... and available *now*!

New To my eyes, the proposed ISO/IEC 27003-2 resembles phase 3 of the current revision project ... so it is *possible* that the revision might stop and release the third edition after completing phase 2's plain English rewording (which I suspect will involve a *lot* more work than was planned), deferring phase 3 to the new part 2 project. Maybe. We shall see.

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

Although excluded from the current revision project, the scope and purpose of ISO/IEC 27003 could - at some distant future point perhaps - usefully extend *beyond* the ISMS design, implementation and certification phase to offer pragmatic advice on the **operation, management, monitoring** and **systematic improvement** of the ISMS. Certification of an ISMS is, after all, merely a milestone on the never-ending journey towards security maturity. As information security becomes an integral and valuable part of the organisation's routine business/operational activities and management, changes are bound to occur. Potentially '27003 might distinguish, encourage and support beneficial ISMS changes while discouraging counterproductive or detrimental ones. Alternatively, developing a separate ISO27k standard in parallel with the ongoing revision of ISO/IEC 27003 might be a quicker (less glacial) option.

< Previous standard ^ Up a level ^ Next standard >