ISO/IEC 27003

Search

Search this site

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

Introduction

ISO/IEC 27003 provides guidance for those implementing the ISO27k standards, covering the *management system* aspects in particular.

Its scope is simply to "provide explanation and guidance on ISO/IEC 27001:2013."

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 intent to make all the management systems standards 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. ISO/IEC 27003 offers *pragmatic* explanation with *plain-speaking* advice and guidance for implementers of '27001.

Structure and content of the standard

ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC TR 27019
ISO/IEC 27021
ISO/IEC 27022
ISO/IEC TR 27023
ISO/IEC 27030
ISO/IEC 27031
ISO/IEC 27032
ISO/IEC 27033
ISO/IEC 27034
ISO/IEC 27035
ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039

For convenience, '27003 follows virtually the same structure as '27001, expanding clause-by-clause on '27001:

- Foreword
- Introduction
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Context of the organization
- 5 Leadership
- 6 Planning
- 7 Support
- 8 Operation
- 9 Performance evaluation
- 10 Improvement
- Annex - Policy framework
- Bibliography

For each '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 '27001 says in section 4.1, 'Understanding the organization and its context':

> *"The organization 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*

ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27101
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC TS 27570

> *management system.*
>
> *NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009[5].”*

Section 4.1 of ‘27003 first states the ‘required activity’ (not the note):

> *“The organization 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 ‘27001. It explains, for instance, that the ‘internal issues’ include the organization’s culture; its policies, objectives, and the strategies to achieve them; its governance, organizational structure, roles and responsibilities; and list a further seven ‘internal issues’ to consider. It also identifies other clauses that use this information.

That alone would be a valuable expansion on ‘27001 section 4.1 but ‘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 should have a much better understanding of the requirements from ‘27001 and a clearer idea of how to go about satisfying them.

Status of the standard

The standard was initially published in 2010, advising on how to plan an ISMS implementation project.

The standard was *substantially* revised and re-issued in **April 2017.** It now reflects and explains the structure and sequence of ISO/IEC 27001:2013. It no longer anticipates a particular ISMS implementation project structure or approach.

Personal comments

Unlike the previous version, the revised 2017 standard is an excellent guide, plugging a hole in the ISO27k suite. On the ISO27k Forum, we are frequently asked how to interpret and implement ‘27001. Along with our FAQ, ‘27003 goes a long way towards answering questions of that nature.

I am intrigued at the idea that ‘27003 might perhaps, in future revisions, extend *beyond* the ISMS design, implementation and certification part to offer pragmatic advice on the operation, management, monitoring and improvement of the ISMS in the years that follow. The point is that certification of an ISMS is merely the start of a long process of evolution and maturity as

information security gradually becomes an integral and valuable part of normal business operations and strategies.

< Previous standard ^ Up a level ^ Next standard >