ISO/IEC 27013

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 27013:2021 — Information security, cybersecurity and privacy protection — **Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1** *(third edition)*

Abstract

"[ISO/IEC 27013] gives guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for organisations intending to: (a) implement ISO/IEC 27001 when ISO/IEC 20000-1 is already implemented, or vice versa; (b) implement both ISO/IEC 27001 and ISO/IEC 20000-1 together; or (c) integrate existing management systems based on ISO/IEC 27001 and ISO/IEC 20000-1. [ISO/IEC 27013] focuses exclusively on the integrated implementation of an information security management system (ISMS) as specified in ISO/IEC 27001 and a service management system (SMS) as specified in ISO/IEC 20000-1."

[Source: ISO/IEC 27013:2021]

Introduction

This standard provides guidance on implementing an **integrated information security *and* IT service management system**, based on both ISO/IEC 27001:2005 (ISMS) and ISO/IEC 20000-1:2011 (IT service management specification, derived from ITIL).

The benefits include:

- Credible provision of effective and secure information/IT services.
- Cost reduction, quicker implementation, better communication, increased reliability and efficiency, and easier certification process due to integration and commonality.

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

- Mutual understanding by service management and information security personnel.

Scope and purpose

The standard advises users on the processes and supporting documentation required to implement an integrated dual management system, for example helping them to:

- Implement ISO/IEC 27001 when they have already adopted ISO/IEC 20000-1, or *vice versa*;
- Implement both ISO/IEC 27001 and ISO/IEC 20000-1 together from scratch (brave souls!); or
- Align and coordinate pre-existing ISO/IEC 27001 and ISO/IEC 20000-1 management systems.

The scope of this standard spans two ISO/IEC JTC 1 subcommittees. SC 27 and SC 7 collaborated to ensure that the information security and IT service management perspectives were both duly considered.

Content of the standard

The standard proposes a framework for organising and prioritising activities, offering advice on:

- Aligning the information security and service management and improvement objectives;
- Coordinating multidisciplinary activities, leading to a more integrated and aligned approach (*e.g.* both donor standards specify incident management activities, with differing scopes for the incidents but otherwise quite similar);
- A collective system of processes and supporting documents (policies, procedures *etc.*);
- A common vocabulary and shared vision;
- Combined business benefits to customers and service providers plus additional benefits arising from the integration of both management systems; and
- Combined auditing of both management systems at the same time, with the consequent reduction in audit costs (we hope!).

Two annexes compare the ISO/IEC 27001 and 20000 standards side-by-side.

Status of the standard

The *first* edition was published in **2012.**

It was revised for ISO/IEC 27001:2013 and the *second* edition was published in **2015**.

It was revised again for ISO/IEC 20000-1:2018. The *third* edition was published in **2021**.

A 4-page *amendment* to the *third* edition was published in December **2024**, updating references to the 2022 versions of ISO/IEC 27001 and 27002, with useful guidance in aspects such as the selection of information security controls for the **S**tatement **o**f **A**pplicability from Annex A or elsewhere (1 of the 4 pages!).

Personal comments

Write out 1,000 times: "*There is more to information security than securing IT. There is more to information security than securing IT. There is more to information security than securing IT. There is more to information security than securing IT ...*"

< 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