ISO/IEC 27021

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 27021:2017 — Information technology — Security techniques — **Competence requirements for information security management systems professionals** *(first edition)*

Abstract

"ISO/IEC 27021:2017 specifies the requirements of competence for ISMS professionals leading or involved in establishing, implementing, maintaining and continually improving one or more information security management system processes that conforms to ISO/IEC 27001."

[Source: ISO/IEC 27021:2017]

Introduction

In order to stabilise and standardise the market for training and certifying professionals for ISO27k implementation and audits, this standard lays out the competence expected of ISMS professionals.

Scope

The standard concerns the competences (meaning the combination of knowledge and skills) required or expected of professionals managing an ISMS in accordance with ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 and ISO/IEC 27007.

The standard does NOT specify a personal certification or qualification scheme as such, but in effect serves as a reference for the bodies that run such schemes.

The standard does NOT cover auditor competence.

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

Purpose and justification

Various training and certification organisations are already active in the field, several of which offer ISO27k-related courses and qualifications such as the ISO/IEC 27001 **Lead Auditor** and **Lead Implementer** designations. Prior to the release of this standard, they made up their own curricula and assessment criteria with no guidance from ISO/IEC except the other ISO27k standards.

ISO/IEC 27021 provides a degree of commonality and comparability between the various qualifications, giving recruiters and employers greater confidence in the quality, competence and suitability of qualified candidates and employees for ISMS roles.

Structure and content

The standard starts by explaining that an ISMS is just one form of Management System, requiring a combination of competences in general business management (*e.g.* leadership and communication, planning and budgeting) plus information security/ISMS management (*e.g.* scoping the ISMS).

The competences roughly mirror the clauses in the main body of ISO/IEC 27001, except that most of the general management competences are not directly related to specific clauses.

Each competence is described quite succinctly in four ways:

- Relevant ISO/IEC 27001 clause (where applicable)
- Intended outcome: what this part of the role entails and is expected to achieve
- Knowledge required: things the ISMS professional should know about
- Skills required: things the ISMS professional should be able to do

Status

The *first* edition was published in **2017**.

Additional references to ISO/IEC 27001 clauses were added to plug gaps in the competencies table through an amendment in 2021: *ISO/IEC 27021:2017/Amd1:2021 Information technology - Security techniques - Competence requirements for information security management systems professionals - Amendment 1: Addition of ISO/IEC 27001:2013 clauses or subclauses to competence requirements*.

Personal comments

Although the title of this standard includes the reserved word 'requirements', that should *not* be taken to imply this is a certifiable standard. A revision to the title should avoid any conflict with CASCO.

The four standards listed in the scope section above may be the 'core standards' but they represent just a fraction of the growing ISO27k suite. It could be argued that several others are nearly as important - ISO/IEC 27003 and ISO/IEC 27004 for examples - which begs questions about the breadth and depth of knowledge and competencies truly expected of information security managers.

Another aspect is that (ISO27k notwithstanding) information security management is materially different in different types/sizes of organisation, so perhaps there is a need for different levels or tiers of qualification (or practitioner maturity, you could say), from entry-level basics up to subject matter experts? A tiered scheme would also encourage career development and lifelong learning. Since the standard is intended to guide those developing courses and qualifications, it might make sense to incorporate or build the standard around a matrix listing the skills and competencies on one axis and the levels or tiers on another, indicating in the body of the matrix which items people at that level/tier are expected to know about and be competent to perform ... something like this perhaps:

Knowledge, skill or competency area	Entry level	Practitioner	Expert
Familiarity with the core ISO27k standards 27000, 27001, 27002 and 27005	Required	Required	Required
Familiarity with other ISO27k standards *e.g.* 27003, 27004, 27007 ...		Suggested	Required
Information risk and security management principles	Required	Required	Required

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

Information risk and security management methods, frameworks *etc.*		Suggested	Required
etc.			

The idea of a tiered scheme was agreed in principle by the project team, with e-CF and e-QF schemes (whatever they are!) being mentioned in comments: maybe this suggestion will be revisited when the standard is next revised.

The standard incorporates the idea of a **B**ody **o**f **K**nowledge defined in the standard to cover the core aspects of governing and managing an ISMS, but extendable by organisations to address their specific additional requirements in this area.

< Previous standard ^ Up a level ^ Next standard >