

ISO/IEC 27021



Search

Search this site

< Previous standard ^ Up a level ^ Next standard >

Chat w/ Online Experts 24/7

A Technician Will Answer Your Questions in Minutes. Chat Now.

<u>ISO/IEC 27021:2017</u> — 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 27002, ISO/IEC 270

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.

1 of 3 8/28/25, 21:29



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 <u>ISO/IEC 27001</u>, 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 <u>ISO/IEC 27001</u> 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

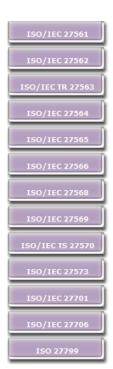
Although the title of this standard includes the reserved word 'requirements', that should *not* be taken to imply this is a certifiable standard. A revision to the title should avoid any conflict with <u>CASCO</u>.

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 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 |

2 of 3 8/28/25, 21:29



| Information risk and security management methods, frameworks <i>etc.</i> | 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 **of 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.

< <u>Previous standard</u> ^ <u>Up a level</u> ^ <u>Next standard</u> >

Copyright © 2025 IsecT Ltd. Contact us re Intellectual Property Rights

3 of 3 8/28/25, 21:29