



# ISO/IEC TR 27024

  
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 TR 27024](#) — Technical report — ISO/IEC 27001 family of standards references list — **Use of ISO/IEC 27001 family of standards in Governmental / Regulatory requirements** [DRAFT]

### Abstract

*"[ISO/IEC TR 27024] provides a list of national regulations that reference ISO/IEC 27001 as a requirement."*

*[Source: ISO/IEC JTC 1/SC 27 Committee Doc 11 May 2025]*

### Introduction

This **Technical Report** is meant to help management determine which of the [ISO27k standards](#) are recommended or required of their organisations for national compliance reasons (without being construed as legal advice), and to facilitate or encourage global harmonisation of the laws, regulations *etc.* in the field of information security management.

### Scope of the standard

The draft standard:

- Identifies a number of national laws, regulations and guidelines that depend and build upon the [ISO27k standards](#);
- Explicitly concerns information security, privacy/data protection, and digitalization and electronic archiving;
- Does not (explicitly) concern other areas such as governance, contracts, product quality/fitness for purpose, cryptography, digital signatures, defence, official secrets, classified information, health and safety, financial data integrity, medical records, misinformation, and more.

### Content of the standard

The central chapter contains just 18 clauses, each listing a selection of relevant laws and regs from a different country or region (such as the EU).

### Status of the standard

A **Technical Report** is being developed from SC 27 **Standing Document 7** - an internal committee reference document.

Since SD7 is mature, the standard progressed rapidly to **Draft Technical Report** stage and was planned for

[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](#)

release back in 2023. Patently, however, compiling and checking details on relevant laws and regs around the globe, along with editorial changes required by ISO, have substantially delayed release.

The title may become "*Government and regulatory use of ISO/IEC 27001, ISO/IEC 27002 and other information security standards*". It entering **Committee Draft** stage and is now due to be published this year.

### Personal comments

If this remained as a **Standing Document** without the formalities of becoming a standard, it would be easier, quicker and cheaper to update it as the referenced standards and laws/regs change, with the bonus of being freely available to those who need the information ... but the committee decided to publish it as a **Technical Report**.

Taking a broad perspective, there are *loads* of laws and regs that have *some* relevance to the confidentiality, integrity or availability of information. In the extreme, virtually every law involves forensic evidence with strong **cia** implications. Laws and regs relating to human safety are important to protect the valuable knowledge and competencies in our heads, while those relating to mental health affect our information processing capabilities. Laws and regs on tax and financial reporting and corporate governance all have information security implications. The standard is unlikely even to mention these.

This project faces a similar conundrum to [ISO/IEC 27002](#). It would be wonderful if the standard was truly comprehensive and up-to-date, and could be relied upon as such, but ultimately that is infeasible. There is a risk that naive users may rely on the standard as definitive without seeking competent legal advice or researching which laws and regs are in fact applicable - hopefully not *you* though, having read this cautionary note!

< [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