ISO/IEC 27002

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 >

Hot ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — **Information security controls** *(third edition)*

Abstract

Summary podcast

"[ISO/IEC 27002] provides a reference set of generic information security controls including implementation guidance. [ISO/IEC 27002] is designed to be used by organisations: (a) within the context of an information security management system (ISMS) based on ISO/IEC27001; (b) for implementing information security controls based on internationally recognized best practices; [and] (c) for developing organisation-specific information security management guidelines."

[Source: ISO/IEC 27002:2022]

Introduction

ISO/IEC 27002 is a popular international standard describing a generic selection of 'good practice' information security controls, typically used to mitigate unacceptable risks to the confidentiality, integrity and availability of information.

Its lineage stretches back to BS 7799 in the mid-1990s.

ISO/IEC 27002 is an advisory document, a recommendation rather than a formal specification such as ISO/IEC 27001. Organisations are advised to identify and evaluate their own information risks, selecting and applying suitable information security controls to mitigate unacceptable risks using ISO/IEC 27002 and other relevant standards and sources for guidance.

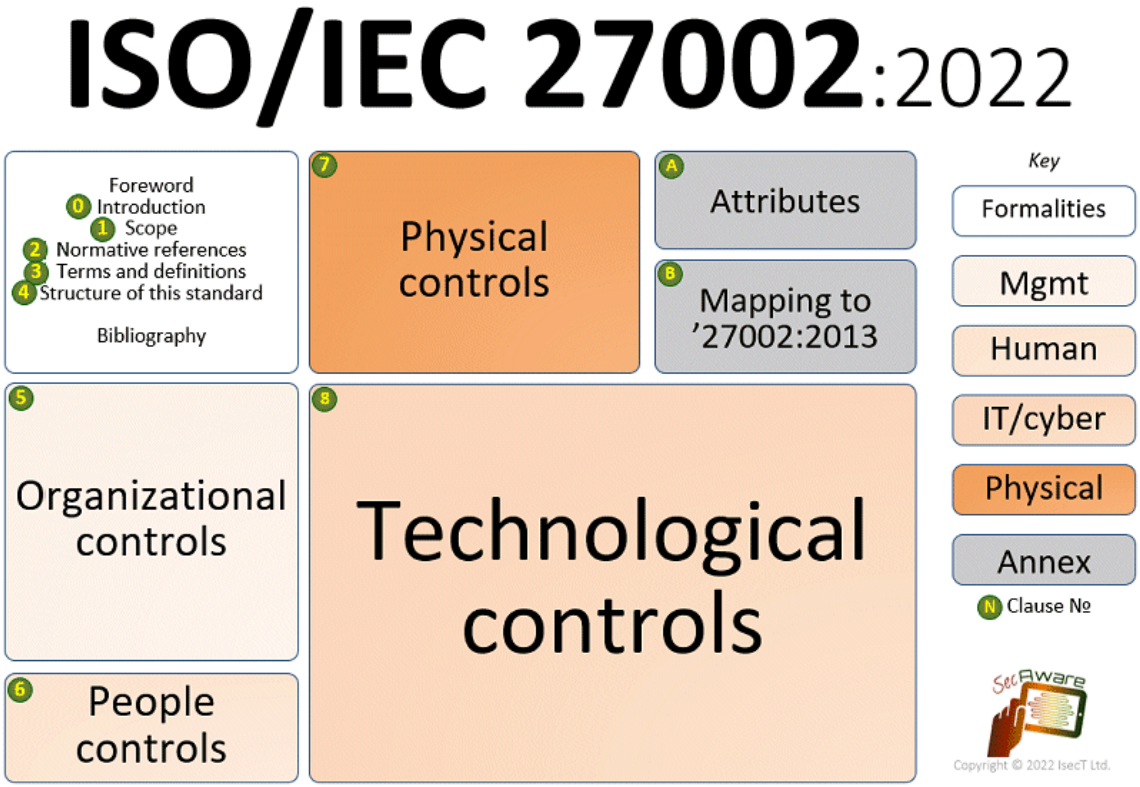
Scope

Like governance and risk management, information security management is a broad topic with ramifications for all organisations. Information security, and hence ISO/IEC 27002, is relevant to all types of organisation including commercial enterprises of all sizes (from one-man-bands up to multinational giants), not-for-profits, charities, clubs, government departments and quasi-autonomous bodies - in fact *any* organisation that handles and depends on information. The specific information risks and hence control requirements differ in detail but there is a lot of common ground, for instance most organisations need to address information risks relating to their employees plus contractors, consultants and third party suppliers of various information and IT services such as cloud computing.

IMPORTANT! The standard is explicitly concerned with *information* security, meaning the security of all forms of information (*e.g.* computer data, documentation, knowledge and intellectual property) and not just IT/systems/network/cyber security.

Structure

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



The standard lays out a 'reference set' of 93* generic information security controls and implementation guidance, categorised into 4 clauses based around these 'themes':

5. **Organisational controls** - a large and misleadingly-named catch-all group of 37* controls that don't fit neatly into the remaining themes;
6. **People controls** - 8* controls involving or relating to people *e.g.* individuals' behaviors, activities, roles and responsibilities, terms and conditions of employment *etc.*;
7. **Physical controls** - 14* tangible controls to secure tangible [information] assets;
8. **Technological controls** - 34* controls involving or relating to technologies, IT in particular.

The 93* controls are each tagged with one or more values from each of 5 'attributes' so they can be grouped, selected or filtered in other ways too:

- **Control type**: preventive, detective and/or corrective;
- **Information security properties**: confidentiality, integrity and/or availability;
- **Cybersecurity concepts**: identify, protect, detect, respond and/or recover;
- **Operational capabilities**: governance, asset management, information protection, human resource security, physical security, system and network security, application security, secure configuration, identity and access management, threat and vulnerability management, continuity, supplier relationships securit, legal and compliance, information security event management, and information security assurance.
- **Security domains**: governance and ecosystem, protection, defence and resilience.

This makes the standard even *more* complicated but reflects these complexities:

- A given control may have *several* applications (*e.g.* backups help protect against malware, hacks, bugs, accidents, mechanical breakdowns, fires *etc.*, and can include deputies and multi-skilled replacements for critical people, and alternative suppliers/sources of necessary information services, as well as data backups);
- An unacceptable risk typically requires *several* controls (*e.g.* malware can be mitigated using backups, awareness, antivirus, network access controls plus IDS/IPS, authentication, patching, testing, system integrity controls *etc.*, while avoiding infection can be a powerful approach if bolstered with controls such as policies and procedures, blacklisting etc.);
- Many of the 'controls' identified in the standard are not atomic, being composed of *several* smaller elements or pieces (*e.g.* backups involve strategies, policies and procedures, software, hardware, testing, incident recovery, physical protection of backup media *etc.*).

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

Some of the themes and attributes are arbitrarily assigned: for example, a commercial card access lock on a building entrance may fall into any, arguably *all four* of the themes listed above, but if it and other such controls were covered several times, the standard would become unwieldy. More likely, it would be categorised as a physical control, possibly with references to other elements.

Organisations can define their own attributes as well.

* **Note:** there are 21 fewer control clauses in the *third* edition than the *second* despite adding 11 new ones since several *second* edition control clauses were updated or merged. **Each clause is comprised of or incorporates numerous 'atomic' controls at a more detailed level of analysis. ISO/IEC 27002 notes or implies *hundreds* of detailed information security controls**, in fact, *way* more than the headline total of "93 controls" suggests.

Relationship to ISO/IEC 27001

An **I**nformation **S**ecurity **M**anagement **S**ystem as specified in ISO/IEC 27001 is a systematic approach to managing information risks, including the multitude of information security controls required to mitigate unacceptable risks *plus other risk treatments*: don't forget that risks may be avoided, shared or accepted. The ISMS is a framework for managing them all, consistently.

ISO/IEC 27001 Annex A briefly summarises/outlines the information security controls from [the second edition of] ISO/IEC 27002 on the basis that they are generally applicable good practices, worth considering. However, organisations are free to implement whichever controls they feel are appropriate and necessary to mitigate their unacceptable information risks. Variants of and extensions to the Annex A controls may well be better, and in some cases entirely different control suites (such as NIST's Cybersecurity Framework) or combinations (blending, say, GDPR or PCI-DSS controls with ISO/IEC 27002) would be more appropriate.

In practice, *most* organisations that adopt ISO/IEC 27001 also use Annex A and hence ISO/IEC 27002 as a general framework, basis or structure for their controls, making various changes as necessary to suit their specific information risks and risk treatment requirements.

Status of the standard

The *first* edition was published in **2005**.

The *second* edition was published in **2013**.

The completely restructured and updated *third* edition was published in **2022**.

ISO/IEC 27002 ISMS implementation guides

A collection of **ISMS implementation guidelines** and **sample documents** is available to download in the free ISO27k Toolkit.

ISMS implementation tips are sprinkled liberally throughout the ISO27k FAQ.

ISO/IEC 27003 provides generic ISMS implementation guidance, focusing on the management system rather than the security controls.

There are also a few 'sector-specific' ISMS implementation guidelines *i.e.* ISO/IEC 27011 for the telecomms sector, ISO 27799 for healthcare and ISO/IEC 27019 for the energy utilities.

Personal comments

In my considered opinion, one of the most distinctive, innovative and valuable features of the original Shell policy manual, the UK DTI Code of Practice/DISC standard PD003 and British Standard BS 7799 was that they explicitly addressed *information* security, recommending approaches and controls to secure *information* in any form - not just computer data, systems, apps, networks and technologies. The focus was clearly on protecting the intangible, vulnerable and valuable information content.

Over the years since ISO/IEC adopted it as an international standard, it has gradually evolved into a tech-centric IT, ICT or cyber-security standard. The third edition of '27002 continues along the same trajectory, as indicated by the relative proportions of the blobs on the diagram above.

The *third* edition misses numerous opportunities to encourage users to consider their **"information risks"** in order to determine whether various controls are even needed to avoid or mitigate the risks, and if so what controls are appropriate, taking account of their effectiveness, costs, value, reliability *etc*. It is as if the controls laid out in the standard are not merely good practices worth considering under various circumstances, but required or mandatory to the extent that not implementing them might perhaps be considered inept, unprofessional or bad practice. There is a subtle presumption that most if not all the controls *should* be employed by all organisations, regardless of the diversity of organisations in scope and their differing information risks. This is misleading, and has remained an issue for several years.

I miss the 'control objectives' from BS 7799: these succinctly explained what the controls were expected to

achieve, giving them a business-related purpose that was readily interpreted in the particular context of an individual organisation. If management accepted that an objective was valid, the controls were worth considering not in the sense of being obligatory or even recommended, so much as examples of the kinds of things that could be put in place to achieve the objective. In the third edition, the risk-based control objectives have become watered-down and often self-serving 'purposes', with little to no explicit reference to the organisation's information risks that the suggested controls are supposed to mitigate - a retrograde step as far as I'm concerned ... potentially presenting an opportunity to fill in the gaps (watch this space!). However, some experts complained of 'challenging conversations' between auditors and management: I suspect the underlying issue there was a failure to understand the true nature of information risk and risk treatment options.

While the restructured standard is readable and usable on paper, the tagging and cross-linking strongly of controls favours database applications (even something as simple as Excel) allowing users to filter or select and sort the controls by whatever criteria or questions they pose - for instance, "Which physical security controls are relevant to privacy?" or "What preventive controls do *not* involve technology?". Given a suitable database application, the sequence is almost irrelevant compared to the categorisation, tagging and description of the controls. It will be interesting to see how this turns out.

I am dismayed that the standard has been infected with the "cyber" virus, almost immediately creating problems of definition and interpretation. Some contributors wanted the standard to cover *both* information security *and* cybersecurity controls, implying that they consider those to be distinct domains, while others first want to understand the differences before classifying controls ... and I must say I'm in the second group. What is the meaning and scope of "cybersecurity", in fact?

Similarly, the committee hoped to resolve confusion over the meaning of "policy" in the *second* edition by distinguishing three variants or hierarchical levels in the *third* edition:

- "Information security policy" refers to the overall, high-level corporate policy at the peak of the classical policy pyramid, approved by 'top management'. 'Strategy' might have been a better term for this, at the risk of creating yet more confusion;
- "Topic-specific policy" refers to mid-level policies *e.g.* topic-specific policies on access control and clear desk and clear screen" (the latter sounds, to me, more like a rule than a mid-level policy ... and indeed, as expressed by the project team, the topic-specific policy concept includes guidelines and rules, making this layer a blend, transition or link between the upper and lower levels). These are aligned with and support the high level policy, approved by 'the appropriate management level', and [within reason] may be adapted/ interpreted locally by departments, business units *etc*. where their specific contexts (information risks, security requirements, business situations, locations *etc*.) differ from the overall corporate context;
- "Rule" is the lowest, most detailed/specific level, defined as an "accepted principle or instruction that states the organisation's expectations on what should be done, what is allowed or not allowed" (I'm not sure an organisation, *per se*, can 'expect' anything, or should have expectations *on* rather than *of* something: in a corporate context, rules are generally imposed by management on behalf of the organisation and its stakeholders ... but this definition was a bone of contention within SC 27 so a compromise is needed).

< Previous standard ^ Up a level ^ Next standard >