ISO/IEC 27002

Search

Search this site

ISO/IEC 27002:2013 — Information technology — Security techniques — **Code of practice for information security controls** *(second edition)*

Quick links

ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC TR 27019
ISO/IEC 27021
ISO/IEC 27022
ISO/IEC TR 27023
ISO/IEC 27030
ISO/IEC 27031
ISO/IEC 27032
ISO/IEC 27033
ISO/IEC 27034
ISO/IEC 27035
ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039

Introduction

ISO/IEC 27002 is a popular, internationally-recognized standard of good practice for information security. ISO/IEC 27002's lineage stretches back more than 30 years to the precursors of BS 7799.

Scope of the standard

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

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 and network security.

Relationship to ISO/IEC 27001

The **I**nformation **S**ecurity **M**anagement **S**ystem formally defined by ISO/IEC 27001 uses a summary of ISO/IEC 27002 in Annex A to suggest potential information security controls. However, organizations are free to select and implement other controls as they see fit. In practice, most organizations that adopt ISO/IEC 27001 also use ISO/IEC 27002 as a framework or starting point for their controls, making various changes as necessary to suit their information risk treatment requirements.

Structure and format of ISO/IEC 27002

ISO/IEC 27002 is a code of practice - a generic, advisory document, not a formal specification such as ISO/IEC 27001. It recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information. Organizations that adopt ISO/IEC 27002 assess their own information risks, clarify their control objectives and apply suitable controls (or indeed other forms of risk treatment) using the standard for guidance.

ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27101
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC TS 27570

The standard is structured logically around groups of related security controls. Many controls could have been put in several sections but, to avoid duplication and conflict, they were arbitrarily assigned to one and, in some cases, cross-referenced from elsewhere. For example, a card-access-control system for, say, a computer room or archive/vault is both an access control and a physical control that involves technology plus the associated management/administration and usage procedures and policies. This has resulted in a few oddities (such as section 6.2 on mobile devices and teleworking being part of section 6 on the organization of information security) but it is at least a reasonably comprehensive structure. It may not be perfect but it is good enough on the whole.

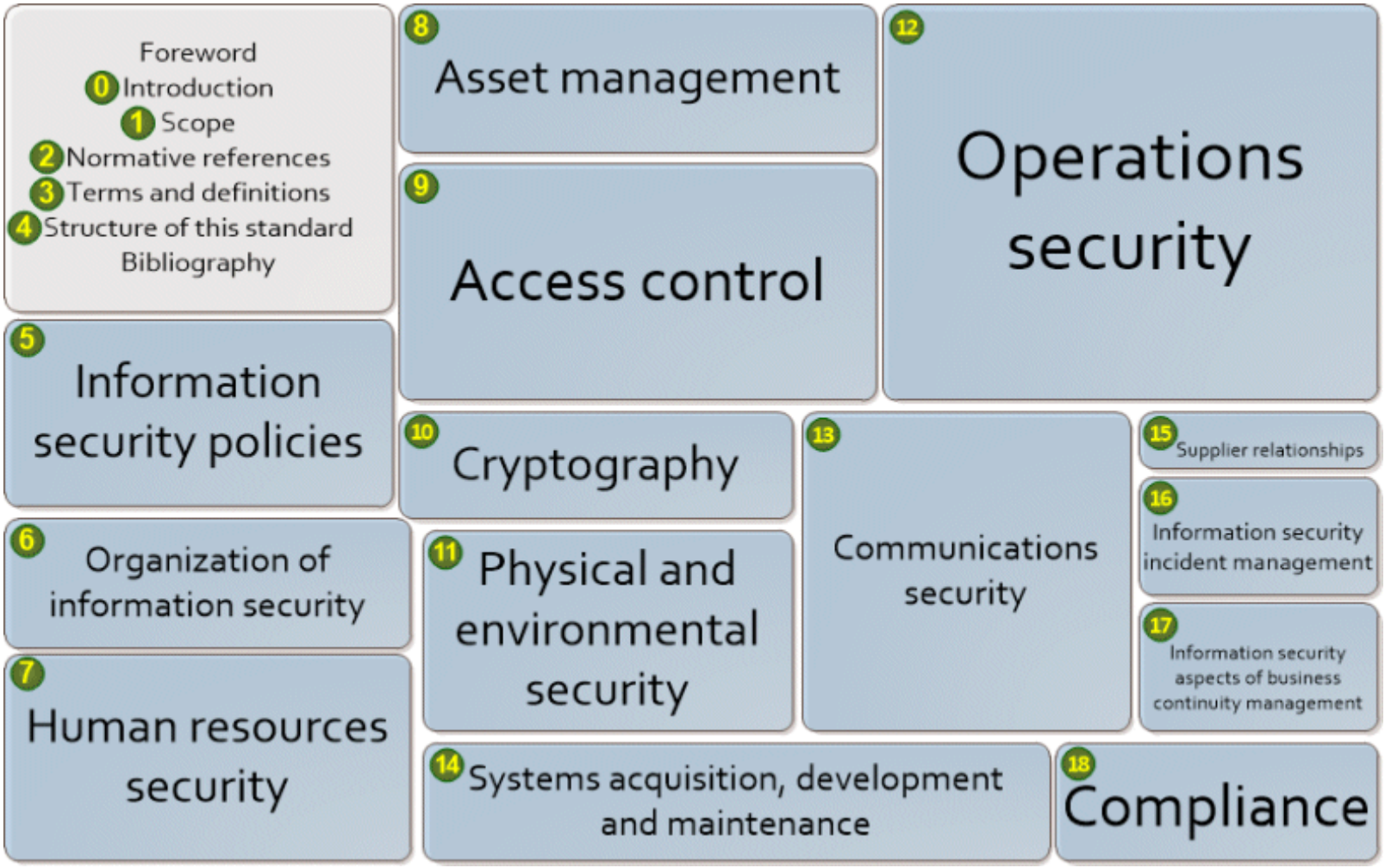
Contents of ISO/IEC 27002

In more detail, here is a breakdown summarizing the standard's 19 sections or chapters (21 if you include the unnumbered foreword and bibliography). The areas of the blocks roughly reflects the sizes of the sections. Click the diagram to jump to the relevant description.

ISO/IEC 27701

ISO 27799

Other ISO27k



Foreword

Briefly mentions ISO/IEC JTC1/SC 27, the committee that wrote the standard, and notes that this "second edition cancels and replaces the first edition (ISO/IEC 27002:2005), which has been technically and structurally revised".

Section 0: Introduction

This lays out the background, mentions three origins of information security requirements, notes that the standard offers generic and potentially incomplete guidance that should be interpreted in

the organization's context, mentions information and information system lifecycles, and points to ISO/IEC 27000 for the overall structure and glossary for ISO27k.

Section 1: Scope

The standard gives recommendations for those who are responsible for selecting, implementing and managing information security. It may or may not be used in support of an ISMS specified in ISO/IEC 27001.

Section 2: Normative references

ISO/IEC 27000 is the only standard considered absolutely indispensable for the use of ISO/IEC 27002. However, various other standards are mentioned in the standard, and there is a bibliography.

Section 3: Terms and definitions

All the specialist terms and definitions are now defined in ISO/IEC 27000 and most apply across the entire ISO27k family of standards.

Section 4: Structure of this standard

Security control clauses

Of the 21 sections or chapters of the standard, 14 specify control objectives and controls. These 14 are the 'security control clauses'.

There is a standard structure within each control clause: one or more first-level subsections, each one stating a control objective, and each control objective being supported in turn by one or more stated controls, each control followed by the associated implementation guidance and, in some cases, additional explanatory notes. The amount of detail is responsible for the standard being nearly 90 A4 pages in length.

35 control objectives

ISO/IEC 27002 specifies some 35 **control objectives** (one per 'security control category') concerning the need to protect the confidentiality, integrity and availability of information.

The control objectives are at a fairly high level and, in effect, comprise a generic functional requirements specification for an organization's information security management architecture.

Few professionals would seriously dispute the validity of the control objectives, or, to put that another way, it would be difficult to argue that an organization need *not* satisfy the stated control objectives in general. However, some control objectives are not applicable in every case and their generic wording is unlikely to reflect the precise requirements of every organization, especially given the very wide range of organizations and industries to which the standard applies. This is why ISO/IEC 27001 requires the SoA (Statement of Applicability), laying out unambiguously which information security controls are or are not required by the organization, as well as their implementation status.

114+++ controls

Each of the control objectives is supported by at least one **control**, giving a total of 114. However, the headline figure is somewhat misleading since the implementation guidance recommends *numerous* actual controls in the details.

The control objective relating to the relatively simple sub-subsection 9.4.2 "Secure log-on procedures", for instance, is supported by:

- Choosing, implementing and using suitable authentication techniques;
- Not disclosing sensitive information at log-on time;
- Data-entry validation;
- Protection against brute-force 'credential stuffing' attacks;
- Logging;
- Not transmitting passwords in clear over the network;
- Session inactivity timeouts;
- Access time restrictions ... plus many other controls such as policies and procedures, awareness and training, compliance assessment and enforcement, oversight, assurance and so on.

Whether you consider that to be one or several controls is up to you. It could be argued that ISO/IEC 27002 recommends literally *hundreds* of distinct information security controls, although some support multiple control objectives, in other words some controls have several purposes.

Furthermore, the wording throughout the standard clearly states or implies that this is not a totally comprehensive set. An organization may have slightly different or completely novel information security control objectives, requiring other controls (sometimes known as 'extended control sets') in place of or in addition to those stated in the standard. A hospital operating theater, for instance, is not the ideal place to be messing around with logins, passwords and all that jazz. Information risk and security is context-dependent.

Section 5: Information security policies

5.1 Management direction for information security

Management should define a set of policies to clarify their direction of, and support for, information security. At the top level, there should be an overall "information security policy" as specified in ISO/IEC 27001 section 5.2.

Section 6: Organization of information security

6.1 Internal organization

The organization should lay out the roles and responsibilities for information security, and allocate them to individuals. Where relevant, duties should be segregated across roles and individuals to avoid conflicts of interest and prevent inappropriate activities. There should be contacts with relevant external authorities (such as CERTs and special interest groups) on information security matters. Information security should be an integral part of the management of all types of project.

6.2 Mobile devices and teleworking

There should be security policies and controls for mobile devices (such as laptops, tablet PCs, wearable ICT devices, smartphones, USB gadgets and other Boys' Toys) and teleworking (such as telecommuting, working-from home, road-warriors, and remote/virtual workplaces). [I don't know how this ended up under section 6, but here it is.]

Section 7: Human resource security

7.1 Prior to employment

Information security responsibilities should be taken into account when recruiting permanent employees, contractors and temporary staff (*e.g*. through adequate job descriptions, pre-employment screening) and included in contracts (*e.g*. terms and conditions of employment and other signed agreements defining security roles and responsibilities, compliance obligations *etc.*).

7.2 During employment

Managers should ensure that employees and contractors are made aware of and motivated to comply with their information security obligations. A formal disciplinary process is necessary to handle information security incidents allegedly caused by workers.

7.3 Termination and change of employment

Security aspects of a person's departure from the organization, or significant changes of roles within it, should be managed, such as returning corporate information and equipment in their possession, updating their access rights, and reminding them of their ongoing obligations under privacy and intellectual property laws, contractual terms *etc.* plus ethical expectations.

Section 8: Asset management

8.1 Responsibility for assets

All information assets should be inventoried and owners should be identified to be held accountable for their security. 'Acceptable use' policies should be defined, and assets should be returned when people leave the organization.

8.2 Information classification

Information should be classified and labelled by its owners according to the security protection needed, and handled appropriately.

8.3 Media handling

Information storage media should be managed, controlled, moved and disposed of in such a way that the information content is not compromised.

Section 9: Access control

9.1 Business requirements of access control

The organization's requirements to control access to information assets should be clearly documented in an access control policy and procedures. Network access and connections should be restricted.

9.2 User access management

The allocation of access rights to users should be controlled from initial user registration through to removal of access rights when no longer required, including special restrictions for privileged access rights and the management of passwords (now called "secret authentication information") plus regular reviews and updates of access rights.

9.3 User responsibilities

Users should be made aware of their responsibilities towards maintaining effective access controls *e.g*. choosing strong passwords and keeping them confidential.

9.4 System and application access control

Information access should be restricted in accordance with the access control policy e.g. through secure log-on, password management, control over privileged utilities and restricted access to program source code.

Section 10: Cryptography

10.1 Cryptographic controls

There should be a policy on the use of encryption, plus cryptographic authentication and integrity controls such as digital signatures and message authentication codes, and cryptographic key management.

Section 11: Physical and environmental security

11.1 Secure areas

Defined physical perimeters and barriers, with physical entry controls and working procedures, should protect the premises, offices, rooms, delivery/loading areas *etc.* against unauthorized access. Specialist advice should be sought regarding protection against fires, floods, earthquakes, bombs *etc.*

11.2 Equipment

"Equipment" (meaning ICT equipment, mostly) plus supporting utilities (such as power and air conditioning) and cabling should be secured and maintained. Equipment and information should not be taken off-site unless authorized, and must be adequately protected both on and off-site. Information must be destroyed prior to storage media being disposed of or re-used. Unattended equipment must be secured and there should be a clear desk and clear screen policy.

Section 12: Operations security

12.1 Operational procedures and responsibilities

IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Capacity and performance should be managed. Development, test and operational systems should be separated.

12.2 Protection from malware

Malware controls are required, including user awareness.

12.3 Backup

Appropriate backups should be taken and retained in accordance with a backup policy.

12.4 Logging and monitoring

System user and administrator/operator activities, exceptions, faults and information security events should be logged and protected. Clocks should be synchronized.

12.5 Control of operational software

Software installation on operational systems should be controlled.

12.6 Technical vulnerability management

Technical vulnerabilities should be patched, and there should be rules in place governing software installation by users.

12.7 Information systems audit considerations

IT audits should be planned and controlled to minimize adverse effects on production systems, or inappropriate data access.

13 Communications security

13.1 Network security management

Networks and network services should be secured, for example by segregation.

13.2 Information transfer

There should be policies, procedures and agreements (*e.g.* non-disclosure agreements) concerning information transfer to/from third parties, including electronic messaging.

Section 14: System acquisition, development and maintenance

14.1 Security requirements of information systems

Security control requirements should be analyzed and specified, including web applications and transactions.

14.2 Security in development and support processes

Rules governing secure software/systems development should be defined as policy. Changes to systems (both applications and operating systems) should be controlled. Software packages should ideally not be modified, and secure system engineering principles should be followed. The development environment should be secured, and outsourced development should be controlled. System security should be tested and acceptance criteria defined to include security aspects.

Note: there is a typo in 14.2.8: the reference to section 14.1.9 should read 14.2.9. See the status update below, or technical corrigendum 2 for the official correction.

14.3 Test data

Test data should be carefully selected/generated and controlled.

15: Supplier relationships

15.1 Information security in supplier relationships

There should be policies, procedures, awareness *etc.* to protect the organization's information that is accessible to IT outsourcers and other external suppliers throughout the supply chain, agreed within the contracts or agreements.

15.2 Supplier service delivery management

Service delivery by external suppliers should be monitored, and reviewed/audited against the contracts/agreements. Service changes should be controlled. [Exactly the same point applies to services delivered by internal suppliers, by the way!]

Section 16: Information security incident management

16.1 Management of information security incidents and improvements

There should be responsibilities and procedures to manage (report, assess, respond to and learn from) information security events, incidents and weaknesses consistently and effectively, and to collect forensic evidence.

Section 17: Information security aspects of business continuity management

17.1 Information security continuity

The continuity of information security should be planned, implemented and reviewed as an integral part of the organization's business continuity management systems.

17.2 Redundancies

IT facilities should have sufficient redundancy to satisfy availability requirements.

Section 18: Compliance

18.1 Compliance with legal and contractual requirements

The organization must identify and document its obligations to external authorities and other third parties in relation to information security, including intellectual property, [business] records, privacy/personally identifiable information and cryptography.

18.2 Information security reviews

The organization's information security arrangements should be independently reviewed (audited) and reported to management. Managers should also routinely review employees' and systems' compliance with security policies, procedures *etc.* and initiate corrective actions where necessary.

Bibliography

The standard concludes with a reading list of 27 (!) relevant ISO/IEC standards, more than half of which are other ISO27k standards.

ISO/IEC 27002 ISMS implementation guidance

A collection of **ISMS implementation guidelines** and **sample documents** is available to download in the free ISO27k Toolkit, and **implementation tips** are sprinkled liberally throughout our 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 sector.

Status of the standard

The second edition of ISO/IEC 27002 was **published in 2013** at the same time as ISO/IEC 27001.

The decision to drop the definition of "information asset" from ISO/IEC 27000 rather than truly bottom out this issue may prove to have been a tactical error. A **technical corrigendum** published in **2014** made minor changes to the wording of ISO/IEC 27002:2013 supposedly to clarify that "information" is indeed an "asset".

A simple monodigit typo resulting in a reference from section 14.2.8 pointing back to 14.1.9 (there is no such section - shock! Horror!) instead of forward to 14.2.9 (the correct, intended reference to, yes, the very next section) was noted formally as a defect in the published standard, following the proper ISO/IEC procedures to the letter of course. Esteemed representatives of a number of national standards bodies met in person to discuss and consider this dreadful situation at some length and some cost to their respective taxpayers. What on Earth could be done about

it? During the plenary held in Kuching it was decided unanimously that this mistake should be fixed by simply replacing "see 14.1.1 and 14.1.9€" with "see 14.1.1 and 14.2.9." Remarkable! Unanimous agreement on a simple fix! What a relief! [/SARCASM] The second corrigendum was published in **2015.**

The standard is currently being revised to reflect changes in information security since the current edition was drafted - things such as BYOD, cloud computing, virtualization, crypto-ransomware, social networking, pocket ICT and IoT, for instance.

The standard will be renamed "Information security controls".

The third edition is due to be published at the end of 2021.

It is currently at 3rd **W**orking **D**raft stage.

Personal comments

ISO/IEC 27002 is a *massive* monolithic standard covering a deliberately broad range of information security controls. Some 237 pages of comments on WD2 were received and processed, reflecting the extent of interest across the globe. WD3 is about 150 pages long!

The controls are being categorized into quite broad 'themes':

- **Organizational controls** - controls involving management and the organization in general, other than those in '27001;
- **Technical controls** - controls involving or relating to technologies, IT in particular (implying "cybersecurity", perhaps, *if* so defined);
- **People controls** - controls involving or relating to behaviors, activities, roles and responsibilities *etc.*;
- **Physical controls** - tangible controls such as locks, and other means of environmental protection and control such as fire and intruder alarms and uninterruptible power supplies;
- **External party controls** - controls involving or relating to parties outside the scope of an ISMS (*e.g.* contracted cloud services, service level agreements with other parts of the organization, legal and regulatory obligations, privacy policies and other obligations to customers *etc.*). *Note: this group may be part of 'organizational controls'.*

Aside from the 'themes', the controls will also be 'tagged' according to other parameters or criteria so they can be grouped or selected in other ways too. This makes the standard, and the project,

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);
- Any given application may require 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*.);
- Many of the controls we commonly consider (*e.g*. backups) are not atomic, being composed of several elements or pieces (*e.g.* backups involve strategies, policies and procedures, software, hardware, testing, incident recovery, physical protection of backup media *etc.*).

At the end of the day, security controls will inevitably be allocated to themes and tagged arbitrarily in places: for example, a commercial card access lock on a building entrance may fall into any, perhaps all 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 categorized as a physical control, possibly with references to other elements.

While the restructured standard should be readable and usable on paper, the tagging and cross-linking strongly hints at the possibility of building database systems (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, "What physical security controls apply to privacy?" or "What preventive controls do not involve technology?". Given a suitable database application, the sequencing options are almost irrelevant, whereas the tagging and description of the controls is critical. 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 want the standard to cover *both* information security *and* cybersecurity controls, clearly suggesting 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? Let's start there, eh, SC27, before jumping aboard the bandwagon!

< Previous standard ^ Up a level ^ Next standard >