ISO/IEC 27001

New **ISO/IEC 27001:2022** — Information security, cybersecurity and privacy protection — **Information security management systems — Requirements** *(third edition)*

Abstract

"This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization ..."

[Source: ISO/IEC 27001:2022]

Introduction

ISO/IEC 27001 formally specifies an **I**nformation **S**ecurity **M**anagement **S**ystem, a governance arrangement comprising a structured suite of activities with which to manage information risks (called 'information security risks' in the standard).

The ISMS is an overarching framework through which management identifies, evaluates and treats (addresses) the organisation's information risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts - an important aspect in such a dynamic field, and a key advantage of ISO27k's flexible risk-driven approach as compared to, say, PCI-DSS.

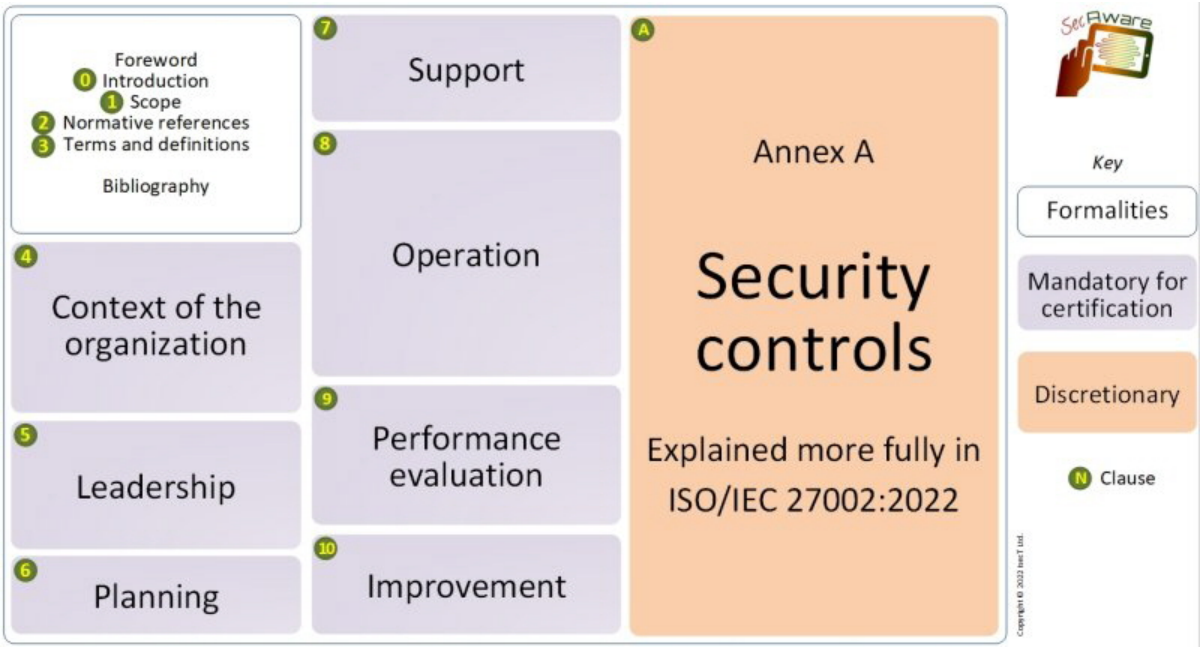
The standard covers all types of organisations (*e.g.* commercial enterprises, government agencies, non-profits) of all sizes (from micro-businesses to huge multinationals) in all industries (*e.g.* retail, banking, defense, healthcare, education and government). This is clearly a very wide brief.

ISO/IEC 27001 does *not* formally mandate specific information security controls since the controls that are required vary markedly across the wide range of organisations adopting the standard. The information security controls from ISO/IEC 27002:2022 are summarised in annex A to ISO/IEC 27001, rather like a menu. Organisations adopting ISO/IEC 27001 are free to choose whichever specific information security controls are applicable to their particular information risks, drawing on those listed in the menu and potentially supplementing them with other *a la carte* options (sometimes known as extended control sets). As with ISO/IEC 27002, the key to selecting applicable controls is to undertake a comprehensive assessment of the organisation's information risks, which is one vital part of the ISMS.

Furthermore, management may elect to avoid, share or accept information risks rather than mitigate them through controls - a risk treatment decision within the risk management process.

ISO/IEC 27035
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 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
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
ISO/IEC 27561

Structure of the standard



0 Introduction - the standard describes a process for systematically managing information risks.

1 Scope - it specifies generic ISMS requirements suitable for organisations of any type, size or nature.

2 Normative references - only ISO/IEC 27000 is considered absolutely essential reading for users of '27001.

3 Terms and definitions - see ISO/IEC 27000.

4 Context of the organisation - understanding the organisational context, the needs and expectations of 'interested parties' and defining the scope of the ISMS. Section 4.4 states very plainly that "The organisation shall establish, implement, maintain and continually improve" the ISMS, meaning that it must be operational, more than merely designed and documented.

5 Leadership - top management must demonstrate leadership and commitment to the ISMS, mandate policy, and assign information security roles, responsibilities and authorities.

6 Planning - outlines the process to identify, analyse and plan to treat information risks, and clarify the *objectives* of information security.

7 Support - adequate, competent resources must be assigned, awareness raised, documentation prepared and controlled.

8 Operation - more detail about assessing and treating information risks, managing changes, and documenting things (partly so that they can be audited by the certification auditors).

9 Performance evaluation - monitor, measure, analyse and evaluate/audit/review the information security controls, processes and management system, systematically improving things where necessary.

10 Improvement - address the findings of audits and reviews (*e.g.* nonconformities and corrective actions), systematically refining the ISMS.

Annex A Information security control reference - names the controls documented in ISO/IEC 27002:2022. The annex is 'normative' meaning that certified organisations are expected to use it to check their ISMS for completeness (according to clause 6.2), but that does *not* mean they are required to implement the controls: given their particular information risks, they may prefer other controls or risk treatments. Refer to ISO/IEC 27002 for detail on the security controls, including useful implementation guidance.

Bibliography - points readers to related standards, plus part 1 of the ISO/IEC directives, for more information. In addition, ISO/IEC 27000 is identified in the body of the standard as a normative (*i.e.* essential) standard and there are several references to ISO 31000 on risk management.

Mandatory requirements for certification

ISO/IEC 27001 is a formalised specification for an ISMS with two distinct purposes:

1. It lays out the design for an ISMS, describing the important parts at a fairly high level;

ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC TS 27570
ISO/IEC 27701
ISO 27799

2. It can (optionally) be used as the basis for formal conformity assessment by accredited certification auditors in order to certify an organisation conformant.

The following 14 items are explicitly required for certification:

1. ISMS scope (as per clause 4.3)
2. Information security policy (clause 5.2)
3. Information risk assessment *process* (clause 6.1.2)
4. Information risk treatment *process* (clause 6.1.3)
5. Information security objectives (clause 6.2)
6. Evidence of the competence of the people working in information security (clause 7.2)
7. Other ISMS-related documents deemed necessary by the organisation (clause 7.5.1b)
8. Operational planning and control documents (clause 8.1)
9. The *results* of the [information] risk assessments (clause 8.2)
10. The *decisions* regarding [information] risk treatment (clause 8.3)
11. Evidence of the monitoring and measurement of information security (clause 9.1)
12. The ISMS internal audit program and the results of audits conducted (clause 9.2).
13. Evidence of top management reviews of the ISMS (clause 9.3)
14. Evidence of nonconformities identified and corrective actions arising (clause 10.1)

Certification auditors check that the mandatory documentation is both present and fit for purpose, and may also check documentation relating to [an audit sample of] the discretionary controls.

The standard does not specify precisely what form the documentation should take, but clause 7.5.2 talks about aspects such as the titles, authors, formats, media, review and approval, while 7.5.3 concerns document control, implying a fairly formal ISO 9001-style approach. Electronic documentation (such as intranet pages) are just as good as paper documents, in fact better in the sense that they are easier to control and maintain. Diagrams are fine too, supplementing or replacing written words - an ISMS documented *entirely* as a set of diagrams or videos would be novel, perhaps brilliant!

ISMS scope and **S**tatement **o**f **A**pplicability **(SoA)**

Whereas the standard is *intended* to drive the implementation of an enterprise-wide ISMS, ensuring that all parts of the organisation benefit by addressing their information risks in an appropriate and systematically-managed manner, organisations can scope their ISMS as broadly or as narrowly as they wish - indeed scoping is a crucial decision for senior management (clause 4.3). A documented **ISMS scope** is one of the *mandatory* requirements for certification.

Although the **S**tatement **o**f **A**pplicability is not explicitly defined, it is a *mandatory* requirement of section 6.1.3. SoA refers to the output from the information risk assessments and, in particular, the decisions around treating those risks. The SoA may, for instance, take the form of a matrix identifying various types of information risks on one axis and risk treatment options on the other, showing how the risks are to be treated in the body, and perhaps who is accountable for them. It *usually* references the relevant controls from ISO/IEC 27002 but the organisation may use a completely different framework, catalogue, reference or source of controls such as NIST SP800-53, the ISF standard, BMIS and/or COBIT or a custom approach. The information security control objectives and controls from ISO/IEC 27002 are provided as a checklist at Annex A in order to avoid 'overlooking necessary controls' (controls that management determines are necessary to mitigate unacceptable information risks): they are not *mandatory* for all organisations.

The ISMS scope and SoA are crucial if a third party intends to attach any reliance to an organisation's ISO/IEC 27001 certificate. If an organisation's ISO/IEC 27001 scope only includes "Acme Ltd. Department X", for example, the associated certificate says nothing about the state of information security in "Acme Ltd. Department Y" or indeed "Acme Ltd." as a whole. Similarly, if for some reason management decides to accept malware risks without implementing conventional antivirus controls, the certification auditors may well challenge such a bold assertion but, *provided* the associated analyses and decisions were sound, that alone would not be justification to refuse to certify the organisation since antivirus controls are not in fact mandatory.

Metrics

In effect (without actually using the term "metrics"), the standard requires the use of metrics on the performance and effectiveness of the organisation's ISMS and information security controls. Section 9, "Performance evaluation", requires the organisation to determine and implement suitable security metrics ... but gives only high-level requirements.

ISO/IEC 27004 offers advice on *what* and *how* to measure in order to satisfy the requirement and evaluate the performance of the ISMS - an eminently sensible approach not dissimilar to that described in **PRAGMATIC** Security Metrics.

Certification

Certified conformity with ISO/IEC 27001 by an accredited and respected certification body is optional but is increasingly being demanded from suppliers and business partners by organisations that are (quite rightly!) concerned about the security of their information, and about information risks throughout the supply chain/network.

According to the 2021 ISO Survey, nearly 60,000 organisations worldwide held valid ISO/IEC 27001 conformity certificates, making this management system standard fourth in popularity behind ISO 9001 (quality assurance), ISO 14001 (environmental protection) and ISO 45001 (health and safety).

Certification brings a number of benefits above and beyond mere conformity, in much the same way that an ISO 9000-series certificate says more than just "We are a quality organisation". Independent assessment necessarily brings some rigor and formality to the implementation process (implying improvements to information security and all the benefits that brings through risk reduction), and invariably requires senior management approval (which is an advantage in security awareness terms, at least!).

The certificate has marketing potential and brand value, demonstrating that the organisation takes information security management seriously. However, as noted above, the assurance value of the certificate is highly dependent on the ISMS scope, RTP and SoA - in other words, **don't put *too much* faith in an organisation's ISO/IEC 27001 certificate if you are highly dependent on its information security.** In just the same way that certified PCI-DSS compliance does *not* mean "We guarantee to secure credit card data and other personal information", a valid ISO/IEC 27001 certificate is a positive sign but *not* a cast-iron guarantee about an organisation's information security. It says "We have a conformant ISMS in place", not "We secure your information", a subtle but important distinction.

Status of the standard

The *first* edition, based on BS 7799 Part 2 (**1999**), was published as ISO/IEC 27001 in **2005**.

The *second* edition, completely revised with substantial changes to align with other ISO management systems standards, was published in **2013**.

A technical corrigendum in **2014** clarified that *information* is an asset.

A second technical corrigendum in **2015** clarified that organisations are formally *required* to identify the implementation status of their information security controls in the SoA.

A **S**tudy **P**eriod looked at the value and purpose of Annex A in relation to the SoA, concluding that Annex A is a useful link to ISO/IEC 27002 but the main body wording should make it clear that **Annex A is discretionary**: organisations can adopt whatever set of controls (or indeed other risk treatments) they deem suitable to treat their information risks, *provided* the process of selecting, implementing, managing, monitoring and maintaining the risk treatments fulfils the (mandatory) main body requirements - in other words, the entire process falls within the ISMS.

New A *third* edition of the standard, published in **October 2022**, has some wording changes to the main-body clauses to reflect ISO's revised Annex SL common structure/boilerplate for all the management systems standards (see below), plus a completely revised Annex A reflecting ISO/IEC 27002:2022.

New The **I**nternational **A**ccreditation **F**orum's MD26:2022 is a **M**andatory **D**ocument providing advance guidance on the up-to-3-year transition arrangements for accreditation bodies, certification bodies and hence certified organisations. An update of MD26 is expected by the end of January 2023.

New During Q2/Q3 2023, SC 27 will review the future plans for '27001, deciding what to do next.

Personal comments

The 2022 edition of the ISO/IEC Directives, part 1 *"Consolidated ISO Supplement - Procedures for the technical work - Procedures specific to ISO"* Annex SL *"Harmonized approach for management system standards"* (previously known as "Draft Guide 83", sometimes "Annex L") appendix 2 (!)

formally specifies/mandates the boilerplate text and structure common to *all* the ISO and ISO/IEC management systems standards covering information security, quality assurance, environmental protection *etc.*

The idea is that people who are familiar with any one of the management systems will understand the basic principles underpinning all the others, and will find their structures and wording similar. Concepts such as certification, policy, conformity, document control, internal audits and management reviews are common to all the management systems standards, and the common policies, processes and governance arrangements can usefully be standardised within an organisation.

Annex SL appendix 2:

- Redefines risk as "effect of uncertainty" (dropping "of objectives" from the definition used in ISO/IEC 27000) with 4 notes (dropping the final 2 of 6 notes in the current definition). Whether that simplification helps, harms or has no effect on ISO27k remains to be seen.
- Replaces "outcomes" with "results" - a change made primarily for ease of translation.
- Includes "Planning of changes" *i.e.* any changes *to the management system* must be performed 'in a planned manner'. The new clause 6.3 is a single sentence .
- Replaces "outsourced" with "externally provided" to encompass outsourcing, contracting and conventional purchasing.
- Separately specifies general requirements for internal audits (9.2.1) *and* for the internal audit programme (9.2.2).
- Separately specifies general requirements for management reviews (9.3.1) *and* for their inputs (9.3.2) and outputs (9.3.3).
- Re-emphasises the need for proactive improvement of the management system in addition to reactive responses to shortcomings.
- Mandates a few boilerplate changes - such as dropping 'documented' from the definition of audit (the guidance says "This definition of "audit" differs slightly from the definition given in ISO 19011:2018 (Guidelines for auditing management systems), in that the definition in 3.18 does not specifically state that the audit process is to be "documented").

< Previous standard ^ Up a level ^ Next standard >