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

Abstract

"[ISO/IEC 27001] specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. [ISO/IEC 27001] also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization ..."

[Source: ISO/IEC 27001:2022]

Summary podcast

Introduction

ISO/IEC 27001:2022 (known colloquially as "ISO 27001", "ISO27001", "27001" or "two seven double-oh one") formally specifies an **I**nformation **S**ecurity **M**anagement **S**ystem, a governance arrangement comprising a structured suite of organised activities with which to manage risks relating to the confidentiality, integrity and availability of information (called 'information security risks' in the standard).

According to the ISO directives part 1 annex SL, a management system is "a set of interrelated or interacting elements of an organisation to establish policies and objectives, as well as processes to achieve those objectives. A management system can address a single discipline or several disciplines. The management system elements include the organisation's structure, roles and responsibilities, planning and operation".

An ISMS is therefore **a set of interrelated or interacting elements of an organisation to establish policies and objectives relating to the security of information, as well as processes to achieve those objectives**.

An 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 appropriately designed and fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts. Adaptation is important in such a dynamic field, and a key advantage of ISO27k's flexible risk-driven approach as opposed to more prescriptive and rigid approaches such as PCI-DSS.

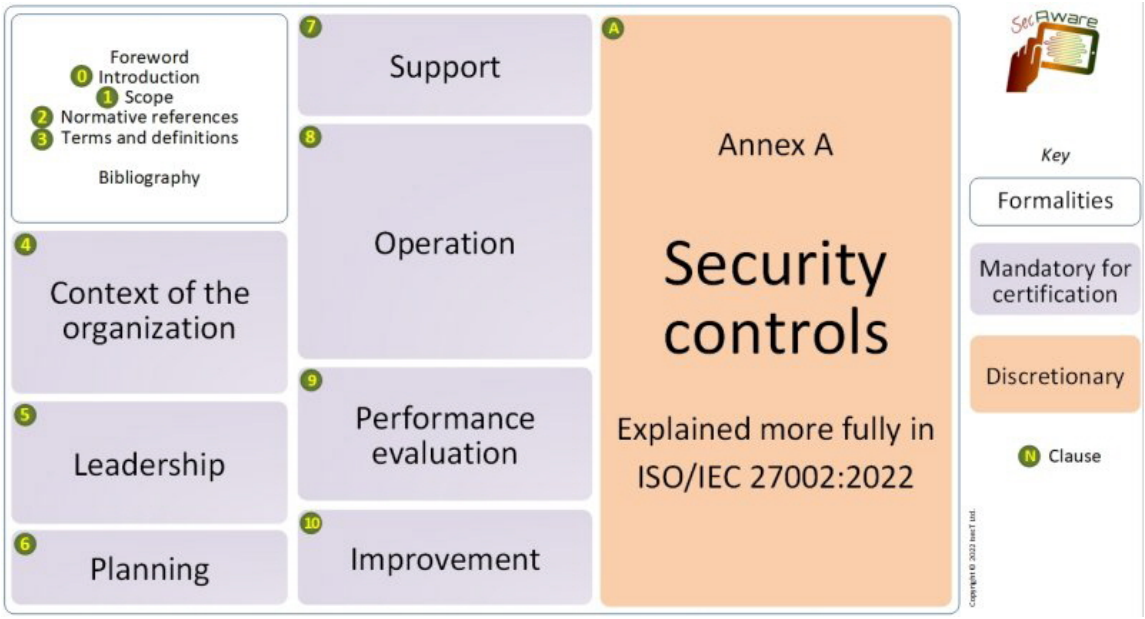
Flexibility allows the standard to apply to all types of organisations (*e.g.* commercial enterprises, government agencies, non-profits, clubs) of all sizes (from micro-businesses to sprawling multinationals) in all industries (*e.g.* retail, banking, defence, healthcare, education and government), worldwide. Given such a huge brief, the standard is necessarily generic, specifying the bare minimum.

ISO/IEC 27001 does *not* formally demand 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, perhaps but not necessarily drawing on those listed in the menu and potentially supplementing or replacing them with other *a la carte* options (sometimes known as extended or custom 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 and mandatory part of the ISMS.

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

Furthermore, management may elect to avoid, share or accept information risks rather than mitigate them through information security controls - a risk treatment decision within the specified risk management process. Appropriate governance arrangements and management controls are also appropriate to direct, control and oversee the ISMS: the standard gives fairly rudimentary and circumspect guidance in these areas.

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/business context, the needs and expectations of 'interested parties' and defining the scope of the ISMS. Section 4.4 coldly states that "The organisation shall establish, implement, maintain and continually improve" the ISMS, meaning that it must be operational, not 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, to clarify the *objectives* of information security, and to manage ISMS changes.
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 lots more detail on the security controls, including useful implementation guidance, and ISO/IEC 27005 to understand information risk management.

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.

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

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 for organisations that choose to implement it;
2. It can (optionally) be used as the basis for formal conformity assessment by certification auditors in order to certify organisations conformant.

The following 14 items of documentation 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** and the **Statement of Applicability** (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 risk assessment outputs *i.e.* the **assessed risks** (clause 8.2)
10. The **risk treatment decisions** (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 **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.

Although the standard does not specify precisely what form the documentation should take, 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.

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 and fully 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 covers "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. Under ISO/IEC 27001, the organisation's *management* decides what controls are necessary - not ISO/IEC, not the auditors, not its advisors

or consultants, not industry/trade bodies, not self-appointed experts on social media, not academics, not me ... but *management*.

Why adopt ISO/IEC 27001?

The benefits include:

- **Achieving and maintaining compliance:** satisfy information security-relevant laws and regulations.
- **Assurance and trust:** conformity tells a story worth telling, especially when competently certified.
- **Consistency:** fundamentally the same management system for all organisations, with the same structure and terms as other kinds of ISO management systems.
- **Enhancing resilience:** less disruption of critical business activities, supporting business continuity.
- **Focusing on priorities:** a cost-effective way to identify cost-effective controls.
- **Governance roadmap:** build an appropriate strategy and structure to manage information risks.
- **Proactive adaptation:** systematically monitor, measure and improve through regular management reviews, audits and feedback.
- **Proportional control:** implement security controls that are proportionate to the risks.
- **Protecting *and* exploiting valuable information:** secure proprietary and personal information while simultaneously permitting its use for authorised purposes.
- **Reducing losses:** sound information security means fewer, less damaging incidents.
- **Strengthening brands:** certification, in particular, enhances reputation, engendering trust.

If you are looking for an accepted way to apply best practices and improve your organisation's information security posture, ISO/IEC 27001 must be a candidate. It is a comprehensive, stable and well-respected standard that can help you protect valuable information *and* achieve business objectives.

Auditor practice notes

Although ISO deliberately steers clear of certification, in 2022, a select Auditing Practices Group within ISO/IEC JTC 1/SC 27 WG1 started preparing and publishing a series of notes for certification auditors. These are unofficial guidelines, explanatory and advisory (discretionary) in nature, not endorsed by ISO nor formally reviewed and approved by SC 27 member bodies in the same way as ISO27k standards. The notes concern various aspects of ISO27k of interest and concern to [certification] auditors and auditees, supplementing other ISO27k standards such as ISO/IEC 27003:

- Use of Annex A: explains the status, purpose and intended use of Annex A, and states what Annex A is *not* (*i.e.* a comprehensive set of required controls).
- Use of **S**tatement **o**f **A**pplicability: ~4 pages of explanation of how to prepare the SoA, covering terms such as 'applicability' and 'necessary controls', and what happens to the certificate if a certified organisation changes its SoA (*i.e.* nothing!).
- SC27 Journal (vol 3 issue 4, October 2023) carried versions of those articles and more:
  - What is Annex A?
  - Statement of Applicability
  - Auditor competence
  - How do I monitor, measure, analyse, and evaluate?
  - Risk management process

Thus far, the APNs might as well have been 'published' in a locked draw of a filing cabinet in a disused lavatory in the sub-basement of an ISO building, with "Beware the leopard!" on the door, somewhere under a Swiss mountain. It is always possible they may yet see the light of day, some day, maybe. Maybe not. That's the risk.

Metrics

While studiously avoiding the term "metrics", the standard requires the organisation to monitor and measure the performance and effectiveness of the ISMS and the 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 2023 ISO Survey, nearly 50,000 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 in **2005**.

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

The *third* edition, published in **2022**, has some wording changes to the main-body clauses to reflect the revised ISO directives part 1 annex SL common structure/boilerplate for all the ISO management systems standards, plus a completely restructured and revised Annex A reflecting ISO/IEC 27002:2022.

According to the International Accreditation Forum's Mandatory Document 26, all ISO/IEC 27001 accreditation bodies and certified organisations should have adopted or migrated to the *third* edition by **31 October 2025**.

An **amendment** to ISO/IEC 27001:2022 was published in February **2024**, formally clarifying that, in clauses 4.1 and 4.2, the 'relevance of climate change should be considered' - a timely reminder to think broadly when considering the context and purpose of the ISMS. SC 27 is considering whether to expand on that - conceivably through another ISO27k standard.

Personal comments

Whereas ISO/IEC 27001 does not use the word 'governance', a 'management system' combines a governance structure with a number of management controls to ensure management's strategic intent is put into effect, becoming an integral part of the organisation. In the case of an ISMS, the system enables management to direct, oversee, control and gain assurance in information risk, security, privacy and related areas. Other ISO management systems standards based on the same ISO boilerplate text presumably avoid the word 'governance' as well. This could be considered a systematic flaw in ISO's management systems approach. However, companion standards such as ISO/IEC 27014 provide guidance in that area.

Planning for updates to any certification standard is tricky because of the need to allow time for the accreditation and certification bodies to plan and enact their transition arrangements, although ISO deliberately and pointedly stays clear of accreditation and certification so, *in theory*, it should not really matter. *In practice*, it does, meaning a delicate and ambiguous relationship between standards and certification.

An ISMS documented almost *entirely* in the form of thought-provoking diagrams, mindmaps or motivational videos rather than the usual boring, wordy, static documents would be novel, radical, creative, perhaps even brilliant. If only I had the clients willing to give it a go ...

< Previous standard ^ Up a level ^ Next standard >