ISO 27001

Clauses

Issued 2026

Clause 1: Scope – This clause relates to the scope or coverage of the standard to help organisations achieve the intended outcomes of their Information Security Management System (ISMS).

Clause 2: Normative references – There are no normative references (for example, additional requirements in other standards) that have to be considered. The clause is retained in order to maintain the same numbering scheme as all the other management system standards.

Clause 3: Terms and definitions – At first sight, the listing of terms and definitions seems confusing as they are not in alphabetical order. Instead, the approach stipulated by ISO is that terms and definitions are in the order that they appear in the standard.

High-Level Structure (HLS)



The ten-clause Annex SL structure shared by ISO 27001 and other ISO management system standards

Clause 4: Context of the organisation

This clause establishes the context of the ISMS and how the business strategy supports this. “Context of the organisation” is the clause that underpins the rest of the standard. It gives an organisation the opportunity to identify and understand the factors and parties that can affect, either positively or negatively, the ISMS. Firstly, the organisation will need to determine external and internal issues that are relevant to its purpose – i.e. the relevant issues, both inside and out, that have an impact on or affect its ability to achieve the intended outcome(s) of the ISMS. Importantly, issues should include not only information security conditions that the organisation affects but also those that it is affected by.

Clause 4	Clause number
Understanding the organisation and its context	4.1
Understanding the needs and expectations of interested parties	4.2
Determining the scope of the information security management system	4.3
Information security management system	4.4

Clause 5: Leadership

This clause is all about the role of “top management”, the person or group of people who direct and control the organisation at the highest level. The purpose is to demonstrate leadership and commitment by integrating information security management into business processes. Top management must demonstrate a greater involvement in the management system and need to establish the information security policy, which can include commitments specific to an organisation’s context.

Clause 5	Clause number
Leadership (title only)	5
Leadership and commitment	5.1
Information security policy	5.2
Organisational roles, responsibilities and authorities	5.3

Clause 6: Planning

This clause focuses on how an organisation plans actions to address both the risks and opportunities which have been identified in Clause 4. It focuses the organisation on the development and use of a planning process, rather than a procedure, to address a range of factors and the risks associated with them. Another key area of this clause is the need to establish measurable information security objectives.

Clause 6	Clause number
Planning (title only)	6
Actions to address risks and opportunities	6.1
Information security objectives and planning to achieve them	6.2
Planning of changes	6.3

Clause 7: Support

This clause covers the resources needed to deliver the ISMS. Simply expressed, this is a very powerful requirement covering all ISMS resource needs. Organisations will need to determine the necessary competence of people doing work under their control that affects information security performance and the ability to fulfil compliance obligations, and ensure they receive the appropriate training. In addition, organisations need to ensure that all people doing work under the organisation's control are aware of the information security policy, how their work may impact it and the implications of not conforming with the ISMS. Finally, there are the requirements for "documented information", which relate to the creation, updating and control of specific data.

Clause 7	Clause number
Support (title only)	7
Resources	7.1
Competence	7.2
Awareness	7.3
Communication	7.4
Documented information	7.5

Clause 8: Operation

The organisation shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

- establishing criteria for the processes;
- implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organisation shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organisation shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

Clause 8	Clause number
Operational planning and control	8.1
Information security risk assessment	8.2
Information security risk treatment (Statement of Applicability)	8.3

Clause 9: Performance evaluation

This is all about measuring and evaluating your ISMS to ensure that it is effective, and it helps you to continually improve. You will need to consider what should be measured, the methods employed and when data should be analysed and reported on. As a general recommendation, organisations should determine what information they need to evaluate information security performance and effectiveness. Internal audits will need to be carried out, and there are certain “audit criteria” defined to ensure that the results of these audits are reported to relevant management. Finally, management reviews will need to be carried out and “documented information” must be kept as evidence.

Clause 9	Clause number
Performance evaluation (title only)	9
Monitoring, measurement, analysis and evaluation (KPIs)	9.1
Internal audit	9.2
Management review	9.3

Clause 10: Improvement

This clause requires organisations to determine and identify opportunities for continual improvement of the ISMS. The requirement for continual improvement has been extended to ensure that the suitability and adequacy of the ISMS – as well as its effectiveness – are considered in the light of enhanced information security performance.

There are some actions that are required that cover the handling of corrective actions. Firstly, organisations need to react to the nonconformities and take action. Secondly, they need to identify whether similar nonconformities exist or could potentially occur.

Clause 10	Clause number
Improvement (title only)	10
Continual improvement	10.1
Nonconformity and corrective action	10.2