QSP SOLUTIONS

ISO27001:2022 Clauses

Clause 1: Scope This clause relates to the scope or coverage of the standard to help organizations achieve the intended outcomes of its information Security Management System (ISMS).

Clause 2: Normative reference There are no normative references, for example other 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)

Clause 4: Context of the organization

This is a new clause that establishes the context of the ISMS and how the business strategy supports this. 'Context of the organization' is the clause that underpins the rest of the standard. It gives an organization the opportunity to identify and understand the factors and parties that can affect, either positively or negatively, the ISMS. Firstly, the organization will need to determine external and internal issues that are relevant to its purpose i.e. what are 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 organization affects but also those that it is affected by.

Clause 5: Leadership

This clause is all about the role of "top management" which is the person or group of people who directs and controls the organization 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 organization's context.

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

Clause 6: Planning

This clause focuses on how an organization plans actions to address both risks and opportunities which have been identified in Clause 4. It focuses the organization on the development and use of a planning process, rather than a procedure to address both a range of factors and the risk associated with such factors. 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

Clause 7: Support

This clause is all about the execution of the plans and processes that enable an organization to meet their ISMS requirements. Simply expressed, this is a very powerful requirement covering all ISMS resource needs. Organizations will need to determine the necessary competence of people doing work that, under its control, affects its Information Security performance, its ability to fulfil its compliance obligations and ensure they receive the appropriate training. In addition, organizations need to ensure that all people doing work under the organization's control are aware of the Information Security policy, how their work may impact this and 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 organization 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 organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization 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, organizations 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" that are 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 and evaluation (title only)	9
Monitoring measuring, analysis and evaluation (KPIs)	9.1
Internal Audit	9.2
Management review	9.3

Clause 10: Improvement

This clause requires organizations 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 handling of corrective actions. Firstly, organizations need to react to the nonconformities and take action.

Secondly, they need to identify whether similar nonconformities exist or could potentially occur. This clause requires organizations to determine and identify opportunities for continual improvement of the ISMS.

Clause 10	Clause number
Non-conformity and corrective action	10.1
Continual improvement	10.2