Global Standards™

ISO 27001:2022

Information Security Management Systems Gap Analysis

gsc-co.com

ISO 27001:2022 Gap Analysis

If you're currently implementing an Information Security Management System (ISMS) and aiming for ISO 27001:2022 certification, this Gap Analysis will help you understand how compliant you are and where you need to do more work.

Note: If you're looking to implement the 2013 version of ISO 27001, please contact Global Standards. We can provide you with a Gap Analysis and guidance specifically for that version.

The ISO 27001 standard, like many ISO standards, includes some repetition and jumping from one clause to another. So, whilst this Gap Analysis is sequenced in the order of the clauses, some sections bring in elements from other clauses and some sub-clauses are skipped when they've been included elsewhere. The aim here is to help you audit in an organized way that largely reflects the standard but which is logical and understandable. It helps you look at the system as a whole - which is the way an Auditor will carry out the formal audit.

This document is not a complete checklist of everything that's covered in the ISO 27001 standard. Being able to tick 'Yes' to all the sections in here is no guarantee that you will achieve ISO 27001 certification. However, it's a very good starting point if you're new to ISO 27001 and it can help form the basis of your internal audits once your system is implemented.

The document starts with Clause 4 since the first three clauses do not contain auditable requirements.

Text in green italics indicates tips from the Global Standards Experts.

Please note that this document is for your own internal use only and has no officail standing.

Clause 4 - Context of the Organisation

This clause requires that you determine the relevant external and internal conditions that may affect your organisation's existence and strategy. The 'context' relates to the business environment in which you operate.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
4.1	Identified the external and internal issues that affect the organisation and the ISMS. *Possibly written down e.g. as a SWOT analysis. If not, must be able to explain your awareness to the Auditor. Don't forget to include 'legal requirements'. You might think this is simple but many companies find it's a very useful exercise to write this down.*						
4.2	Clear understanding of needs and expectations of interested parties, including customers, and other stakeholders. *'Other stakeholders' could include regulators, staff, suppliers, visitors. Remember to include legal and regulatory requirements of your customers.*						
4.3	Scope of the ISMS clearly determined. *The scope of your ISMS must be written down. It should describe the type of products and services you offer and justify if any require-ment of the standard is not applicable to you. Remember, an ISO 27001 system does NOT have to cover the whole organisation; you can ringfence areas. Take advice from Global Standards.*						
4.4	The ISMS is built and maintained in its entirety. You need to demonstrate an understanding of how you maintain and continually improve your system. (See also 9 and 10). *In the past, ISO was seen as an exercise in writing massive documents. That's not the case now but some documentation and organisation is required.*						

Clause 5 - Leadership and Commitment

Top management cannot delegate overall responsibility for the ISMS. They have to take ultimate responsibility and show real leadership, taking a proactive, hands-on role.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
5.1	Top management able to provide evidence that they take accountability for the ISMS. *Able to answer questions, perhaps show minutes of meetings, have awareness of any improvement actions required. Without top management leadership no initiatives will succeed. Support must be there and the Auditor will expect to have time to interview and discuss the system with them.*						
	Information Security Policy and objectives are aligned with the organisation's overall strategy and integrated into processes. *The policy is also your statement of intent.*						
	Evidence that top management actively promote the ISMS amongst staff. *Auditors might ask random staff for their comments.*						
	Resources (staff, time, budget etc.) are made available where necessary to support the functioning of the ISMS.						
	Ensuring that the ISMS supports continual improvement. *Evidence from Internal Audits, Management Reviews etc. will help support this.*						

Clause 5 - Leadership and Commitment

Top management cannot delegate overall responsibility for the EMS. They have to take ultimate responsibility and show real leadership, taking a proactive, hands-on role.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
5.2	The Information Security Policy, which contains your objectives, should be relevant to your organisation and what you're trying to achieve. Must contain commitment to continual improvement. Should be documented. *Also align it to any legislative requirements.*						
	The Information Security Policy is available to all interested parties and communicated to them. *Should be visible to staff on noticeboard/ intranet, for example, and people should be familiar with it.*						
5.3	Responsibilities and levels of authority for individuals relating to the ISMS must be understood. *A good way to check this is by random questioning of staff.*						
	Individual(s) with responsibility for ensuring the ISMS conforms to ISO 27001 are identified. *The identified individuals must understand their responsibilities. Formal ISO training such as 'Internal Auditing' is recommended. Auditors may question individuals to assess capability.*						
	Individual(s) with responsibility for reporting on the performance of the ISMS have been identified. *Possibly the same people as above. Internal Audit reports can satisfy this. See also 9.*						

Clause 6 - Planning

Risk-based thinking is one of the cornerstones of ISO 27001. This is all about ensuring that the expected results are achieved, and no unwanted incidents occur.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
6.1	With reference to 4.1 and 4.2, be sure that the ISMS can reduce / prevent undesirable effects and support continual improvement. Make sure you have actions identified to address these risks and opportunities and integrate them into your system. *This is one of the main purposes of an ISMS, supporting the aim of continual improvement.*						
	Systems to evaluate the effectiveness of actions you take. *This is connected to clause 9.*						
6.1.2	Develop an Information Security Risk Assessment that identifies criteria for risk acceptance and for performing the assessments. *This is one of the key parts of the standard. If you're unsure how to perform this, perhaps consider a **consultant.***						
	Can repeat the Information Security Risk Assessment and get consistent, valid, comparable results.						
	Identify the risks associated with loss of confidentiality, integrity and availability of information. Also identify who is responsible.						
	Risks analysed to determine: consequences of risk; likelihood of occurrence; the level of risk.						
	Evaluate the risks, comparing results of analysis with the criteria established and prioritise risks for treatment.						

Clause 6 - Planning

Risk-based thinking is one of the cornerstones of ISO 27001. This is all about ensuring that the expected results are achieved, and no unwanted incidents occur.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
6.1.3	Develop an Information Security Risk Treatment process based on results of 6.1.2. This should identify information security controls necessary. Also refer to Annex A of ISO 27001 to ensure nothing is missed. *You'll need a copy of the ISO 27001 standard for this.*						
	Publish a Statement of Applicability (SoA) that identifies controls and explains, where applicable, why controls have been omitted. *This can be quite a big piece of work despite being such a short sub-clause! The SoA summarises your position on each of the information security controls in Annex A. In essence, it outlines why you are tackling some risks and accepting other risks.*						
	Develop an Information Security Risk Treatment Plan. *Again, this can be quite a big piece of work despite this being such a short sub-clause! It summarises each of the identified risks and how you intend to manage them (e.g. avoid risk by ceasing an activity; modify it by changing processes; share the risk such as out-sourcing; accept the risk because costs outweigh benefits). Include target dates.*						
	Obtained approval of the plan and any risks from the 'risk owners'. *A 'risk owner' is someone with the authority to resolve the problem.*						

Clause 6 - Planning

Risk-based thinking is one of the cornerstones of ISO 27001. This is all about ensuring that the expected results are achieved, and no unwanted incidents occur.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
6.2	Have in place information security objectives relating to relevant functions/processes that support and continually improve the ISMS which are measurable, montiored, communicated and updated when needed. Should be available as documented information. *In determining the objectives and how to achieve them, consider what resources are needed, responsibilities, target dates and how results will be evaluated.*						
6.3	When changes are identified, are these implemented in a planned manner? *Don't rush into making haphazard changes without proper controls and checks.*						

Clause 7 – Support

The organisation is required to establish and maintain the necessary infrastructure to ensure smooth operation and continual improvement of the Information Security Management System.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
7.1	Determined and provided the resources (people, budget, infrastructure, tools, IT etc.) to support the ongoing running of the ISMS. *You should be able to explain to the Auditor how you did this.*						
7.2	Individuals are competent and records are kept as evidence. *Relates to skills and experience of individuals. Consider training plans, certificates etc. Keep records.*						
7.3	Individuals are aware of the ISMS, their roles, the benefits of improved information security and the implications of nonconformance. *Individuals should be able to answer questions put by the Auditor.*						
7.4	The organisation must determine what to communicate with regard to the ISMS (internal and external) e.g. what, to whom, how, when. *It may be as simple as a statement on your website but possibly much more detailed.*						

Clause 7 - Support

The organisation is required to establish and maintain the necessary infrastructure to ensure smooth operation and continual improvement of the Information Security Management System.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
7.5	The level of documented information required for effective running of the ISMS has been considered and created. *Can be electronic. Only needs to be proportionate to size and complexity of your organisation, activities and competence of individuals.*						
	Systems of control (e.g. title, date, author, reference number) and for updating documented information are in place. Must also be adequately protected (especially where confidential), accessible and retained. *Don't forget to include relevant documentation from external sources.*						

Clause 8 - Operation

This is the 'Do' part of the Plan-Do-Check-Act (PDCA) cycle and is the day-to-day part of what your organisation does. This clause is at the very heart of the of the Information Security Management System.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
8.1	Maintain processes to run the ISMS and implement actions identified in 6.1 and 6.2. *Need to have control of processes and be able to demonstrate this.*						
	Documentation retained as required to demonstrate processes carried out as planned. *So you can provide evidence to the Auditor.*						
	Process for controlling planned changes and to mitigate adverse effects. *Remember this includes outsourced activities.*						
8.2	Information Security Risk Assessment (6.1.2) performed at planned intervals or when significant changes are proposed. *Keep evidence to show to the Auditor.*						
8.3	Implement the Information Security Risk Treatment Plan. *This clause is simply telling you that the plan you developed at 6.1.3 must actually be activated! Keep evidence.*						

Clause 9 – Performance Evaluation

The organisation is required to determine what needs to be monitored, how to monitor and when to do it.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
9.1	Determined what needs to be monitored and measured, and when.						
	Established methods for monitoring, measuring, analysing, evaluating and when this should be done. *The above is used to evaluate conformity and effectiveness of processes and identify need for improvements in the ISMS. Make sure you identify who will do the monitoring and when analysis and evaluation will be done.*						
9.2	Established and implemented a planned approach to internal audits mindful of the frequency, methods, responsibilities, scope.						
	Results of internal audits are reported to management, appropriate corrective action taken. *You may wish to attend an Internal Auditor **training course** to learn how to do this.*						
9.3	Management review meetings are taking place as planned and documented evidence is available.						
	There is an appropriate agenda for the management review meetings to cover all requirements as stated in 9.3 of the standard.						
	There is documented evidence of the outputs of the reviews, identifying opportunities for improvement, any required changes to the ISMS and how to resource any changes required. *Don't forget to review the needs and expectations of interested parties.*						

Clause 10 – Performance Evaluation

Underpinning the concept of an ISMS are the principles of corrective action and continual improvement.
The organisation must identify opportunities for improvement as well as introduce necessary actions.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
10.1	Evidence that you react to, control and correct noncomformities and deal with the consequences. *You should have a procedure for this.*						
	Have a system for, and be able to provide examples of, reviewing and analysing nonconformities and implementing improvements to the ISMS. *To ensure mistakes and errors are not repeated. This is the essence of continual improvement.*						
	Review the effectiveness of any changes made to the ISMS as a consequence of the above.						
10.2	Overall, an approach to continually improve the suitability and effectiveness of the ISMS. *Much of this will be covered in clause 9.*						

About Global Standards

With a commitment to excellence, Global Standards Co. empower its customers to reach new heights through precision, passion, and unwavering expertise. As an international consulting firm, we proudly serve with a dedication to business planning, research and development, project management, and a suite of strategic consulting services.

At Global Standards Co., we strive to be a catalyst for success in the business consulting industry. Through our integrated solutions, we provide our clients with the tools they need to work effectively and efficiently – helping them achieve their goals with timely precision.‘

With a global presence spanning nine countries, we have partnered with organizations of all types, drawing from wide-ranging experience to break through barriers and create successful outcomes.

As we look to the future, we are excited to introduce our newest service; Carbon Foot-printing, CSR, SMETA SEDEX Consulting for Manufacturers, Service Providers, traders, processors, and Farmers.

At Global Standards Co., we are passionate about helping our clients grow, and we're ready to **help you take the next step!**

Our Capabilities
How can we support your future

We believe that together, we can create lasting change and builda brighter future. Our clientele includes visionary leaders and innovative thinkers from multinational and regional corporations, as well as passionate entrepreneurs and craftsmen who are building a sustainable future. Let's work together to make a difference!

E: info@gsc-co.com
T: 962 6 4024999
W: gsc-co.com

Global
Standards™