INSERT COMPANY NAME/LOGO HERE

ISO 27001:2022 Information Security Management System (ISMS) – Gap Analysis Checklist

This gap analysis checklist is prepared for use in evaluating your Information Security Management System (ISMS) against the requirements of ISO/IEC 27001:2022. Each requirement is expressed as a question that the user (auditor / assessor) can use to evaluate ISMS capabilities. Use the ISO 27001:2022 standard along with this checklist and refer to ISO requirements and controls in Annex A.

After you have prepared an assessment schedule, and assigned responsibility to personnel for different areas or processes to assess, copy each section of the checklist for the assessors working with that section. As you work through the checklist take notes on what is in place, and what needs to be developed. Reference the procedures or other documents that you review. Take notes on the status of legacy / older documents (will they need to be revised for the new system, or can they be used as is?). Also note where processes are in place, but documentation is needed. Focus on what is in place, and what needs to be developed.

While you want to know if procedures and processes are being complied with, compliance is not your main focus during a gap assessment. Remember that the final outcome of this assessment should be a list of things that your company needs to do to comply with ISO 27001:2022.

ISMS Clause	Assessment Question	Currently in Place	Compliant Yes / No	If No - % Completed	Items Needed
4	**CONTEXT OF THE ORGANIZATION**				
This clause includes sub-clauses relating to the context of the organization: (1) Understanding the Organization and its Context, (2) Understanding the Needs and Expectations of Interested Parties, and (3) Determining the Scope of the Information Security Management System. They require that you determine the issues and requirements that can impact ISMS planning.					
4.1	**Understanding the organization and its context**				
	Has your company determined the external and internal issues that are relevant to your purpose and strategic direction? Have you considered the relevant issues that affect your ability to achieve the intended outcomes of the Information Security Management System (ISMS)?				

4.2	**Understanding the needs and expectations of interested parties**				
	With consideration given to information and data security, have you determined: • The interested parties relevant to the ISMS? • The relevant requirements of these interested parties? • Which requirements (if any) will be addressed through the ISMS? How do you monitor and review the information about the interested parties and their relevant requirements? Has the organization considered legal requirements, regulatory requirements, and contractual obligations?				
4.3	**Determining the scope of the quality management system**				
	To establish a proper ISMS scope, has your company determined the boundaries and applicability of the ISMS? When determining the scope of the ISMS, have you considered: • External and internal issues (per 4.1)? • Requirements of relevant interested parties (per 4.2)? • Interfaces and dependencies between activities performed by your company and those that are performed by other				

	organizations (such as suppliers or subcontractors)? Is the scope of the ISMS available and maintained as documented information? In the scope of the ISMS, have you stated exemptions or exclusions from the ISMS? If yes, are such exemptions or exclusions explained or justified (justification for any instance where a requirement of the ISMS standard cannot be applied)?				
4.4	**Information security management system**				
	Has your company obtained the current version of the ISO 27001:2022 international standard? As required by the standard, have you established, documented, implemented, maintained, and continually improved the ISMS? Have you determined the processes needed for the ISMS and their applications throughout your company? For the ISMS processes have you determined: • Inputs required and the outputs expected from the processes? • Criteria, methods, including measurements and related performance indicators needed to ensure the effective operation, and control of the processes? • Resources needed?				

	• Assignment of responsibilities and authorities over processes? • Methods for monitoring, measuring, and evaluating processes; and, if needed, the changes to processes to ensure that they achieve intended results? Does your organization have processes in place to establish, implement, maintain, and continually improve ISMS processes and their interactions?				
5	**LEADERSHIP**				
This clause requires that top management demonstrate leadership and commitment with respect to the ISMS. This section also asks top management to establish, implement, and maintain an ISMS policy that is appropriate to your company and to ensure that the responsibilities and authorities for relevant roles are assigned, communicated, and understood.					
5.1	**Leadership and commitment**				
	Has top management demonstrated leadership and commitment with respect to the ISMS by: • Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization? • Ensuring the integration of the information security management system requirements into the organization's processes? • Ensuring that the resources needed for the information security management system are available?				