MINISTRY
OF
SECURITY

ISO 27001:2022 AUDIT CHECKLIST

PART 1: CLAUSES

ISO 27001:2022 Clauses	Sub Clauses	Gap Assessment Questionnaire	Response
4 Context of the organization	4.1 - Understanding organization and its context	Have the internal and external issues that are relevant to the organization's ISMS determined	
		Have impact and the risk associated to the issues determined	
		Have the remediation plan for issues documented	
	4.2 - Understanding the needs and expectations of interested parties	Has the organization determined the interested parties that are relevant to the ISMS	
		Has the organization determined the needs and expectations of these interested parties	
		Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements?	
	4.3 - Determining the scope of the information security management system	Have the boundaries and applicability of the ISMS been determined to establish its scope, taking into consideration the external and internal issues, the requirements of interested parties and the interfaces and dependencies with other organizations?	
		Has the organization defined the scope of ISMS including the in scope departments, interfaces, dependences and the locations	
		Is ISMS scope been documented	
5 Leadership	5.1 - Leadership and commitment	Is the organization’s leadership commitment to the ISMS demonstrated by establishing the information security policy and objectives, compatible with the strategic direction of the organization, and in promotion of continual improvement?	
		Has the leadership ensured the integration of the ISMS requirements into its business processes?	
		Has the leadership ensured resources are available for the ISMS, and directing and supporting individuals, including management, who contribute to its effectiveness?	
		Has the leadership communicated the importance of effective information security and conformance to ISMS requirements?	
		Has the leadership directing and supporting relevant roles to contribute to the effectiveness of ISMS	
	5.2 - Policy	Is there an established information security policy that is appropriate to ISMS	
		Does the information security policy gives a framework for setting objectives, and demonstrates commitment for continual improvement of ISMS	
		Is the policy documented and communicated to employees and relevant interested parties?	
	5.3 - Organizational roles,	Are the roles, responsibilities & authorities relevant to ISMS scope clearly defined and communicated?	
		Is the Org Chart defined and inline with the defined roles and responsibilities	

	responsibilities and authorities	Are the responsibilities and authorities for conformance and reporting on ISMS performance assigned?	
Clause 6	6.1 - Actions to address risks and opportunities	Have the internal and external issues, and the requirements of interested parties been considered to determine the risks and opportunities that need to be addressed to ensure that the ISMS achieves its outcome	
		Have actions to address risks and opportunities been planned, and integrated into the ISMS processes, and are they evaluated for effectiveness?	
		Has an information security risk assessment process that establishes the criteria for performing information security risk assessments, including risk acceptance criteria been defined?	
		Is the information security risk assessment process repeatable and does it produce consistent, valid and comparable results?	
	6.1.2 - Information security risk assessment	Does the information security risk assessment process identify risks associated with loss of confidentiality, integrity and availability for information within the scope of the ISMS, and are risk owners identified?	
		Are information security risks analysed to assess the realistic likelihood and potential consequences that would result, if they were to occur, and have the levels of risk been determined?	
		Are information security risks compared to the established risk criteria and prioritised?	
		Is documented information about the information security risk assessment process available?	
	6.1.3 - Information security risk treatment	Is there an information security risk treatment process to select appropriate risk treatment options for the results of the information security risk assessment, and are controls determined to implement the risk treatment option chosen?	
		Have the controls determined, been compared with ISO/IEC 27001:2022 Annex A to verify that no necessary controls have been missed?	
		Has a Statement of Applicability been produced to justify Annex A exclusions, and inclusions together with the control implementation status?	
		Has the organization formulated an information security risk treatment plan and obtained the risk owners approval for residual risk acceptance	
	6.2 - Information security objectives and planning to achieve them	Have measurable ISMS objectives and targets been established, documented and communicated throughout the organization?	
		In setting its objectives, has the organization determined what needs to be done, when and by whom?	
		Is everyone within the organization's control aware of the importance of the information security policy, their contribution to the effectiveness of the ISMS and the implications of not conforming?	
		Has the organization determined the need for internal and external communications relevant to the ISMS, including	

		what to communicate, when, with whom, and who by, and the processes by which this is achieved?	
7 **Support**	7.1 - Resources	Has the organization determined the resources needed for ISMS	
	7.2 - Competence	Has the organization determined the competency of the persons relevant to ISMS	
		Has the organization taken corrective measures to acquire the necessary competency of the persons relevant to ISMS	
		Has the organization retained information as evidence for showcasing that the persons relevant to ISMS have necessary competency	
	7.3 - Awareness	Has the organization defined and documented Information Security Awareness Plan	
		Does the employees undergo security awareness sessions upon hire and on periodic basis	
		Does the organization have a method to evaluate the effectiveness of the awareness training	
		How does the organization ensures that the employees are aware about the information security policy	
		Are the employees aware of the implications of not confirming to information security requirements	
	7.4 - Communication	Has the organization developed internal and external communication plan	
		Does the communication plan include the details of what to share, when to share, whom to share, how to share and with whom to share	
	7.5.1 - General 7.5.2 - Creating and updating 7.5.3 - Control of documented information	Has the organization determined the documented information necessary for the effectiveness of the ISMS?	
		Is the documented information in the appropriate format, and has it been identified, reviewed and approved for suitability?	
		Has the organization defined naming conventions including (document tittle, date, author & approval)	
		While creating and updating the documents does the organization ensure the integrity of the documents by capturing version numbers and appropriate approvals	
		Does the organization have a process to control the distribution of its documented information to ensure it is only available for intended persons	
		Does the organization protects the documented information from loss of confidentiality, integrity and availability	
		Is the documented information properly stored and adequately preserved for its legibility	
		Has the organization identified and documentation of external origin	
8 **Operation**	8.1 - Operational planning and control	Does the organization has a programme to ensure that the ISMS achieves its outcomes, requirements and objectives been developed and implemented?	
		Is documented evidence retained to demonstrate that processes have been carried out as planned?	
		Are changes planned and controlled, and unintended changes reviewed to mitigate any adverse results?	

		How does the organization control outsourced processes/services relevant to ISMS	
		Does the organization have documented information as an evidence to ensure that the processes are carried out and implemented as planned.	
	8.2 - Information security risk assessment	Are information security risk assessments performed at planned intervals or when significant changes occur, and is documented information retained?	
		Does the organization retain relevant documented information of the results of the information security risk assessments	
	8.3 - Information security risk treatment	Has the information security risk treatment plan been implemented as per the information risk treatment plan	
		Does the organization retain relevant documented information of the results of the information security risk treatment	
9 Performance evaluation	9.1 - Monitoring, measurement, analysis and evaluation	Is the information security performance and effectiveness of the ISMS evaluated?	
		How does the organization determine the processes and controls that needs to be monitored and controlled	
		How does the organization determine the methods for monitoring, measurement, analysis and evaluation of security processes and controls	
		How does the organization ensure that the selected methods produce comparable, repeatable and reproducible results	
		Has the organization determined the frequency for monitoring, measurement, analysis and evaluation of security processes and controls	
		Has the organization determined when to analyze the results of monitoring, measurement, analysis and evaluation of security processes and controls	
		Has the organization determined what needs to be monitored and measured, when, and by whom	
		Is documented information retained as evidence of the results of monitoring and measurement?	
	9.2 - Internal audit	Does the organization plan, establish, implement and maintain an internal audit program	
		Has the organization defined the frequency of internal audits	
		Has the organization defined the objective and criteria for the internal audit	
		Has the organization defined the frequency, methods, responsibilities and requirements for the audit program	
		Are internal audits conducted periodically to check that the ISMS is effective and conforms to both ISO/IEC 27001:2022 and the organization's requirements?	
		Does the audit program take into consideration of importance of the process during the audit	
		Are the audits performed by competent personnel	
		How does the organization ensure objectivity and impartiality of the audit	

		Are the results of the internal audit reported to relevant management personnel	
		Are results of audits reported to management, and is documented information about the audit programme and audit results retained?	
	9.3 - Management review	Does the review consider results from previous management reviews	
		Does the Top Management review the effectiveness of ISMS at planned intervals	
		Does the review consider changes to the internal and external issues	
		Does the review consider changes to the needs and expectations of interested parties	
		Does the review consider the non conformities and corrective actions	
		Does the review consider monitoring and measurement results	
		Does the review consider audit results	
		Does the review consider feedback from interested parties	
		Does the review consider results of risk assessment and risk treatment	
		Does the review consider opportunities for continual improvement	
		Does the outputs of the review include decisions related to continual improvement and any needs for changes to ISMS	
		Has the organization retained documented information as evidence for the results of management reviews	
		Are the results of the management review documented, acted upon and communicated to interested parties as appropriate?	
10 Improvement	10.1 - Continual improvement	Does the organization continually improve the suitability, adequacy and effectiveness of the ISMS	
	10.2 - Nonconformity and corrective action	What are the steps taken by the organization on the non conformities identified	
		Does the organization takes actions to control and correct the non conformities	
		Does the organization identifies the root cause for the non conformity	
		Does the organization take steps to eliminate the root cause	
		Does the organization take steps to identify similar non conformities within the organization.	
		Does the Organization take steps to review the effectiveness of corrective actions taken'	
		Is documented information retained as evidence of the nature of non-conformities, actions taken and the results?	

PART 2: CONTROLS – CONTINUED

FOLLOW US ON LINKEDIN FOR MORE FREE CHECKLISTS

PLAYBOOK
MADE WITH ❤

MINISTRY
OF
SECURITY