MINISTRY OF SECURITY

ISO 27001:2022 AUDIT CHECKLIST

PART 1: CLAUSES

MINISTRY OF SECURITY

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	