ISO IEC 27001:2022 Master Internal Audit Checklist

Quick Links: Guidance | Result Charts | Process Report | Action Report

Before you begin auditing, review and edit the process name list in Cell B161. This will populate the drop-down menus in Column E and various axes within the audit result charts. Use the drop-down menu in Column F to select one of four audit findings defined by the audit criteria. Column G will automatically display a recommendation based on the audit finding. The response is then automatically represented as an 'x' in either Column H, I, J, or K. These columns are hidden. The indicator in Column L will update according to the perceived level of risk, e.g., minor or major. (Ref. Clause 6.4.8, ISO 19011:2018). Use the drop-down menus in Col M to select an appropriate root-cause. You can change this list by editing the root-cause list in Cell M161. Describe how to correct a nonconformance or adopt an opportunity in Col N. Record audit evidence, such as document numbers and revisions in Col O.

					Audit Findings & Actions					
Ref No.	**Clause Title**	**Q-No**	**Requirements/Questions**	**Process Name**	**Audit Result**	**Recommendations**	**Score**	**Possible Root-cause**	**Action Plan**	**Audit Evidence & Notes**
4.1	Organizational Context	1	Has your organization determined external and internal issues (Incl. whether climate change is a relevant issue) are applicable to its purpose and its strategic direction that affect its ability to achieve the intended result(s) of its information security management system?	Process 1	Minor NC	Identify and discuss the root-cause within 4 weeks and correct.	75	Human - Poor employee involvement	Reinforce training	
4.2a	Relevant Interested Parties	2	Does your organization determine the interested parties that are relevant to the information security management system?	Process 1	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100	Process - Procedures or work-instructions were inadequate/non-existent	Review and rewrite WI	
4.2b	Relevant Interested Parties	3	Does your organization determine the requirements (Incl. those relating to climate change) of the interested parties that are relevant to the information security management system?	Process 1	Minor NC	Identify and discuss the root-cause within 4 weeks and correct.	75	Human - Lack of skill, training or experience	Reinforce training	
4.2c	Relevant Interested Parties	4	Does your organization determine which requirements (e.g. legal, regulatory or contractual) are addressed through the information security management system?	Process 2	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
4.3	Management System Scope	5	Has your organization determined the boundaries and applicability of the information security management system to establish its scope?	Process 2	Major NC	Contain the problem imediately. Identify the root-cause within one week and correct.	25	Process - Procedure was contradictory or confusing	Review and rewrite procedure	
4.3a	Management System Scope	6	When determining this scope, has your organization considered the external and internal issues referred to in 4.1?	Process 2	Major NC	Contain the problem imediately. Identify the root-cause within one week and correct.	25	Human - Inadequate management involvement	Reinforce training	
4.3b	Management System Scope	7	When determining this scope, has your organization considered the requirements of relevant interested parties referred to in 4.2?	Process 2	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
4.3c	Management System Scope	8	When determining this scope, has your organization considered c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations?	Process 2	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
4.3	Management System Scope	9	Is the scope of your organization's information security management system available and maintained as documented information and available to interested parties and workers? (See 7.5.1a)	Process 2	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
4.4	Management System Processes	10	Has your organization established, implemented, maintained and continually improved its information security management system, including the processes needed and their interactions, in accordance with the requirements of ISO IEC 27001:2022?	Process 2	Minor NC	Identify and discuss the root-cause within 4 weeks and correct.	75	Human - Poor employee involvement	Review training procedure	
5.1a	Leadership & Commitment	11	Has Top Management demonstrated leadership and commitment to the information security management system by ensuring that your organization's information security policy and objectives are established, are documented; and are compatible your organization's goals (See 6.2) and its context (See 4.0)?	Process 3	Opportunity	Review and implement actions to deploy the opportunity to improve the process(s).	100	Opportunity for improvement	Review scope	
5.1b	Leadership & Commitment	12	Has Top Management demonstrated leadership and commitment to the information security management system by ensuring that information security management requirements are integrated into your organization's business processes?	Process 3	Major NC	Contain the problem imediately. Identify the root-cause within one week and correct.	25	Human - Human error	Reinforce training	
5.1c	Leadership & Commitment	13	Has Top Management demonstrated leadership and commitment to the information security management system by ensuring that your organization has the required resources to implement it?	Process 3	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
5.1d	Leadership & Commitment	14	Does Top management demonstrate leadership and commitment with respect to the information security management system by communicating the importance of effectiveinformation security management and of conforming to information security management requirements?	Process 3	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
5.1e	Leadership & Commitment	15	Does Top management demonstrate leadership and commitment to the information security management system by ensuring that the information security management system achieves its intended results?	Process 3	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
5.1f	Leadership & Commitment	16	Does Top management demonstrate leadership and commitment to the information security management system by by engaging, directing and supporting persons to contribute to the effectiveness of the information security management system?	Process 3	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
5.1g	Leadership & Commitment	17	Does Top management demonstrate leadership and commitment with respect to the information security management system by promoting improvement?	Process 3	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
5.1h	Leadership & Commitment	18	Does Top management demonstrate leadership and commitment with respect to the information security management system by supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility?	Process 3	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
5.2a	Information Security Policy	19	Has Top Management established, implemented and maintained as documented information (See 7.5.1) a information security policy, that is appropriate to the purpose and organizational context that supports its strategic direction?	Process 4	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
5.2b	Information Security Policy	20	Has Top Management established, implemented and maintained as documented information (See 7.5.1) a information security policy that provides a framework to establish the information security objectives?	Process 4	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
5.2c	Information Security Policy	21	Has Top Management established, implemented and maintained as documented information (See 7.5.1) a information security policy that includes a commitment to satisfy applicable (legal and non-legal) requirements?	Process 4	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
5.2d	Information Security Policy	22	Does Top management establish, implement and maintain a policy that includes a commitment to continual improvement of the information security management system?	Process 4	Major NC	Contain the problem imediately. Identify the root-cause within one week and correct.	25	Human - Did not follow procedures, a one-time lapse	Review training procedure	
5.2e	Information Security Policy	23	Is the information security management system policy available and be maintained as documented information? (See 7.5.1a)	Process 4	Major NC	Contain the problem imediately. Identify the root-cause within one week and correct.	25	Human - Physically unable perform the task	Reassign duties	
5.2f	Information Security Policy	24	Is the information security management system policy communicated, understood and applied within the organization?	Process 4	Opportunity	Review and implement actions to deploy the opportunity to improve the process(s).	100	Opportunity for improvement	Review previous management review minutes	
5.2g	Information Security Policy	25	Is the information security management system policy available to relevant interested parties, as appropriate?	Process 4	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
5.3	Roles, Responsibilities & Authorities	26	Does Top management ensure that the responsibilities and authorities for relevant roles are assigned, communicated and understood, and maintained as documented information?	Process 5	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
5.3a	Roles, Responsibilities & Authorities	27	Has Top management assigned the responsibility and authority for ensuring that the information security management system conforms to the requirements of ISO IEC 27001:2022?	Process 5	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
5.3b	Roles, Responsibilities & Authorities	28	Has Top Management assigned responsibility and authority to relevant personnel for reporting of the performance of the information security management system to Top Management?	Process 5	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			
6.1.1a	Actions to Address Risks & Opportunities - General	29	When planning for the information security management system, has your organization considered the issues referred to in 4.1, the requirements referred to in 4.2 and determined the risks and opportunities that need to be addressed to give assurance that the information security management system can achieve its intended results?	Process 6	Conforms	Continue to monitor trends and indicators to determine ongoing stability.	100			