

ADAPTIVE CERTIFICATIONS





MINIMUM REQUIREMENTS







ISO 27001:2022 INFORMATION SECURITY MANAGEMENT SYSTEMS











# ITEM	ELEMENT	27001 CLAUSE	ADDRESSED	COMMENTS
1	Have the internal and external issues that are relevant to the ISMS, and that impact on the achievement of its expected outcome, been determined?			
2	Has the organization determined the interested parties that are relevant to the ISMS?			
3	Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements?			
4	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?			
5	Is the scope of the ISMS documented?			





# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
6	Does Top Management demonstrate leadership and commitment in establishing the information security policy and objectives, in consideration of the strategic direction of the organization, and in promotion of continual improvement?			
7	Does Top Management demonstrate leadership and commitment in ensuring the integration of the ISMS requirements into its business processes?			
8	Does Top Management demonstrate leadership and commitment in ensuring that resources are available for the ISMS, and directing and supporting individuals, including management, who contribute to its effectiveness?			
9	Does Top Management demonstrate leadership and commitment in communicating the importance of effective information security and conformance to ISMS requirements?			
10	Is there an established information security policy that is appropriate, gives a framework for setting objectives, and demonstrates commitment to meeting requirements and for continual improvement?			
11	Is the policy documented and communicated to employees and relevant interested parties?			
12	Are the roles within the ISMS clearly defined and communicated?			
13	Are the responsibilities and authorities for conformance and reporting on ISMS performance assigned?			
14	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, that undesired effects are prevented or reduced, and that continual improvement is achieved?			

# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
15	Have actions to address risks and opportunities been planned, and integrated into the ISMS processes, and are they evaluated for effectiveness?			
16	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?			
17	Have the controls determined, been compared with ISO/IEC 27001:2012 Annex A to verify that no necessary controls have been missed?			
18	Has a Statement of Applicability been produced to justify Annex A exclusions, and inclusions together with the control implementation status?			
19	Has an information security risk treatment plan been formulated and approved by risk owners, and have residual information security risks been authorised by risk owners?			
20	Is documented information about the information security risk treatment process available?			
21	Have measurable ISMS objectives and targets been established, documented and communicated throughout the organization?			
22	In setting its objectives, has the organization determined what needs to be done, when and by whom?			

23 Is the ISMS adequately resourced?

# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
24	Is there a process defined and documented for determining competence for ISMS roles?			
25	Are those undertaking ISMS roles competent, and is this competence documented appropriately?			
26	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?			
27	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?			
28	Has the organization determined the documented information necessary for the effectiveness of the ISMS?			
29	Is the documented information in the appropriate format, and has it been identified, reviewed and approved for suitability?			
30	Is the documented information controlled, such that it is available and adequately protected, distributed, stored, retained and under change control, including documents of external origin required by the organization for the ISMS?			
31	Has a programme to ensure the ISMS achieves its outcomes, requirements and objectives been developed and implemented?			
32	Is documented evidence retained to demonstrate that processes have been carried out as planned?			

# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
33	Have outsourced processes been determined and are they controlled?			
34	Are information security risk assessments performed at planned intervals or when significant changes occur, and is documented information retained?			
35	Has the information security risk treatment plan been implemented and documented information retained?			
36	Is the information security performance and effectiveness of the ISMS evaluated?			
37	Has it been determined what needs to be monitored and measured, when, by whom, the methods to be used, and when the results will be evaluated?			
38	Is documented information retained as evidence of the results of monitoring and measurement?			
39	Are internal audits conducted periodically to check that the ISMS is effective and conforms to both ISO/IEC 27001:2012 and the organization's requirements?			
40	Are the audits conducted by an appropriate method and in line with an audit programme based on the results of risk assessments and previous audits?			
41	Are results of audits reported to management, and is documented information about the audit programme and audit results retained?			





# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
42	Where non conformities are identified, are they subject to corrective action (see section 18)?			
43	Do top management undertake a periodic review of the ISMS?			
44	Does the output from the ISMS management review identify changes and improvements?			
45	Are the results of the management review documented, acted upon and communicated to interested parties as appropriate?			
46	Have actions to control, correct and deal with the consequences of non-conformities been identified?			
47	Has the need for action been evaluated to eliminate the root cause of non-conformities to prevent reoccurrence?			
48	Have any actions identified been implemented and reviewed for effectiveness and given rise to improvements to the ISMS?			
49	Is documented information retained as evidence of the nature of non-conformities, actions taken and the results?			





ADAPTIVE CERTIFICATIONS





MINIMUM REQUIREMENTS











ISO 27001:2022 INFORMATION SECURITY MANAGEMENT SYSTEMS. ANNEX OF CONTROLS





# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
1	Are there established policies for information security??			
2	Are roles and responsibilities for information security clearly defined?			
3	Is segregation of duties implemented and maintained?			
4	Are management responsibilities for information security clearly assigned?			
5	Is there established contact with relevant authorities for information security?			


# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
6	Is there engagement with special interest groups for information security matters?			
7	Is threat intelligence being gathered and utilized effectively?			
8	Is information security integrated into project management processes?			
9	Is there an inventory of information and other associated assets?			
10	Are there guidelines for the acceptable use of information and associated assets?			
11	Is there a process for the return of assets?			
12	Is information classified according to its sensitivity and importance?			
13	Is there a system for labeling information appropriately?			
14	Are there secure methods for information transfer?			

# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
15	Is access control implemented effectively?			
16	Is identity management in place and functioning properly?			
17	Are authentication processes for information secure?			
18	Are access rights assigned and managed appropriately?			
19	Is information security considered in supplier relationships?			
20	Are information security requirements addressed within supplier agreements?			
21	Is information security managed throughout the ICT supply chain?			
22	Are supplier services monitored, reviewed, and managed for changes in information security?			
23	Is information security maintained for the use of cloud services?			





# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
24	Is there a plan for information security incident management?			
25	Are information security events assessed and decisions made appropriately?			
26	Is there a response process for information security incidents?			
27	Is there a system for learning from information security incidents?			
28	Is evidence collected properly during information security incidents?			
29	Is information security maintained during disruptions?			
30	Is ICT readiness ensured for business continuity?			
31	Are legal, statutory, regulatory, and contractual requirements for information security identified and met?			
32	Are intellectual property rights protected?			





# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
33	Are records protected securely?			
34	Is privacy and protection of personally identifiable information ensured?			
35	Is there an independent review of information security?			
36	Is compliance with policies, rules, and standards for information security regularly checked?			
37	Are operating procedures documented and followed?			
38	Is employee screening conducted for information security purposes?			
39	Are terms and conditions of employment aligned with information security requirements?			
40	Is there ongoing information security awareness, education, and training?			
41	Is a disciplinary process in place for information security breaches?			





# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
42	Are responsibilities defined for after termination or changes in employment?			
43	Are confidentiality or non-disclosure agreements in place??			
44	Are there policies for remote working related to information security?			
45	Is there a process for reporting information security events?			
46	Are physical security perimeters established and maintained?			
47	Is physical entry to secure areas controlled?			
48	Are offices, rooms, and facilities secured?			
49	Is physical security monitoring in place?			
50	Are there measures against physical and environmental threats?			





# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
51	Is secure working maintained in secure areas?			
52	Are clear screen and clear desk policies enforced?			
53	Is equipment properly sited and protected?			
54	Are assets off-premises secured?			
55	Is storage media secured?			
56	Are supporting utilities protected?			
57	Is cabling security ensured?			
58	Is equipment maintenance conducted securely?			

59 Is there a process for secure disposal or reuse of equipment?

# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
60	Are user endpoint devices secured?			
61	Are privileged access rights managed securely?			
62	Are information access restrictions in place?			
63	Is access to source code controlled?			
64	Are secure authentication processes implemented?			
65	Is capacity management aligned with security requirements?			
66	Are measures in place to protect against malware?			
67	Are technical vulnerabilities managed properly?			
68	Is configuration management in place for security?			

# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
69	Is information deletion conducted securely?			
70	Is data masking used where appropriate?			
71	Are data leakage prevention measures in place?			
72	Are information backup procedures followed?			
73	Is redundancy ensured for information processing facilities?			
74	Are logging procedures in place and followed?			
75	Are monitoring activities conducted for security purposes?			
76	Is clock synchronization maintained across systems?			
77	Are privileged utility programs controlled securely?			

# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
78	Is the installation of software on operational systems controlled?			
79	Is network security implemented effectively?			
80	Are network services secured?			
81	Is network segregation implemented where necessary?			
82	Is web filtering used appropriately?			
83	Is cryptography used for securing information?			
84	Is there a secure development lifecycle process in place?			
85	Are application security requirements defined and met?			
86	Are secure system architecture and engineering controls in place?			

# ITEM	 ELEMENT	 27001 CLAUSE	 ADDRESSED	 COMMENTS
87	Are secure coding practices followed?			
88	Is security testing conducted during development and acceptance phases?			
89	Is outsourced development managed securely?			
90	Is there separation of development, test, and production environments?			
91	Is change management conducted securely?			
92	Is test information protected?			
93	Are information systems protected during audit testing?			