ISO 27001 Gap Analysis Checklist

Instructions:

This checklist helps assess compliance with ISO 27001 requirements. Answer each question using the following scale:

1 — Not implemented: No process or activity implemented, or little/no evidence of systematic achievement.

2 — Planned: Activity or process is planned but not implemented, or implementation just started.

3 — In progress: Activity or process is partially implemented, so full effects cannot yet be expected.

4 — Mostly implemented: Activity or process is fully or mostly implemented, documented, and relevant people are trained, but monitoring, measurement, and improvement are not systematic.

5 — Optimized: Activity or process is fully implemented, documented, continuously supervised, measured, and improved; relevant people are trained.

---

4. Context of the Organization

4.1 Understanding the Organization and Its Context

1. Did the organization determine the purpose(s) of the ISMS?
2. Did the organization determine internal and external issues relevant to the ISMS purpose?
3. Did the organization determine how internal and external issues could influence the ISMS ability to achieve its intended outcomes?

4.2 Understanding the Needs and Expectations of Interested Parties

4. Did the organization determine interested parties?
5. Does the list of all interested parties' requirements exist?

4.3 Determining the Scope of the Information Security Management System

6. Is the scope documented with clearly defined boundaries and applicability?

4.4 Information Security Management System

7. Have you established, documented, implemented, maintained, and continually improved an ISMS, including needed processes and interactions, per ISO 27001 requirements?

---

5. Leadership

5.1 Leadership and Commitment

8. Are the general ISMS objectives compatible with the strategic direction?
9. Does management ensure the necessary ISMS resources are available as needed?
10. Does management ensure that ISMS achieves its intended outcomes?

5.2 Policy

11. Does an Information Security Policy exist with included objectives or a framework for setting objectives?
12. Is the Information Security Policy documented and communicated within the company and to other interested parties?

5.3 Organizational Roles, Responsibilities, and Authorities

13. Are roles, responsibilities, and authorities for information security assigned and communicated?

---

6. Planning

6.1 Actions to Address Risks and Opportunities

6.1.1 General

14. Are internal and external issues, as well as interested parties' requirements, considered while addressing risks and opportunities?

6.1.2 Information Security Risk Assessment

15. Is there a documented process to identify information security risks, including risk acceptance criteria and criteria for risk assessment?

6.1.3 Information Security Risk Treatment

16. Is the risk treatment process documented, including risk treatment options and how to create a Statement of Applicability?

6.2 Information Security Objectives and Planning to Achieve Them

17. Are information security objectives and targets established at relevant functions of the organization, measured, and monitored where practical?
18. Is there a plan, or group of plans, to achieve the information security objectives and targets including responsibility, evaluation method, means, and timeframe?

6.3 Planning of Changes

19. Are changes in the ISMS done in a planned manner?

---

7. Support

7.1 Resources

20. Are adequate resources provided for all ISMS elements?

7.2 Competence

21. Is appropriate competence assessed, and training provided where needed for personnel doing tasks that affect information security? Are competence records maintained?

7.3 Awareness

22. Is the personnel aware of the Information Security Policy, their role, and consequences of not complying with the rules?

7.4 Communication

23. Are there identified communication needs related to information security, including responsibilities, what to communicate, to whom, and when?

7.5 Documented Information

24. Does the ISMS documentation include the Information Security Policy, objectives, scope, main elements, interactions, and records required by ISO 27001 and the company?

25. Is document and record management controlled, including reviews, approvals, storage, and protection?
26. Is documented information of external origin controlled?

---

8. Operation

8.1 Operational Planning and Control

27. Are established criteria for processes documented, and are controls implemented according to these criteria?
28. Is the necessary documented information available to ensure processes are carried out as planned?
29. Are planned changes controlled? Are consequences of unplanned changes reviewed for necessary mitigation?
30. Are outsourced processes identified and controlled?

8.2 Information Security Risk Assessment

31. Are risks, their owners, likelihood, consequences, and levels documented?

8.3 Information Security Risk Treatment

32. Does a risk treatment plan exist, approved by risk owners?
33. Is there a documented list of necessary controls with justifications and implementation status?

---

9. Performance Evaluation

9.1 Monitoring, Measurement, Analysis, and Evaluation

34. Is it defined what needs to be measured, by which method, who is responsible, and who will analyze and evaluate the results?
35. Are measurement results documented, analyzed, and evaluated by responsible persons?

9.2 Internal Audit

36. Does an audit program exist that defines timing, responsibilities, reporting, audit criteria, and scope?

37. Are internal audits performed according to an audit program, results reported, and corrective actions taken?

9.3 Management Review

38. Is management review regularly performed, and are results documented?
39. Did management decide on all crucial issues for ISMS success?

---

10. Improvement

10.1 Continual Improvement

40. Is the ISMS continuously adjusted to maintain suitability, adequacy, and effectiveness?

10.2 Nonconformity and Corrective Action

41. Does the organization react to every nonconformity?
42. Does the organization eliminate causes of nonconformities and take corrective action where appropriate?
43. Are all nonconformities recorded along with corrective actions?

ANNEX A. (Note: only the controls marked as applicable in the Statement of Applicability must be implemented.)

A.5 ORGANIZATIONAL CONTROLS

44. **Are there published policies, approved by management, reviewed, and updated to support information security**? (control A.5.1 Policies for information security)
45. **Are all information security responsibilities defined?** (control A.5.2 Information security roles and responsibilities)
46. **Are duties and responsibilities properly segregated considering situations of conflict of interest?** (control A.5.3 Segregation of duties)
47. **Is management actively requiring all employees and contractors to comply with information security rules?** (control A.5.4 Management responsibilities)

48. **Are contacts with relevant authorities defined?** (control A.5.5 Contact with authorities)
49. Are contacts with special interest groups or professional associations defined? (control A.5.6 Contact with special interest groups)
50. **Is information related to information security threats collected and analyzed to produce threat intelligence?** (control A.5.7 Threat intelligence)
51. **Do projects consider information security aspects?** (control A.5.8 Information security in project management)
52. **Does an Inventory of Assets exist, and does every asset in the inventory have a designated owner?** (control A.5.9 Inventory of information and other associated assets)
53. **Are rules and procedures for handling of information and other associated assets defined?** (control A.5.10 Acceptable use of information and other associated assets)
54. **Are company assets returned by employees and contractors when their employment is terminated?** (control A.5.11 Return of assets)
55. **Are criteria to classify information defined?** (control A.5.12 Classification of information)
56. **Are there procedures which define how to label and handle classified information?** (control A.5.13 Labelling of information)
57. **Is the information transfer properly protected**? (control A.5.14 Information transfer)
58. **Is there an Access Control Policy, and do users have access only to the resources they are allowed to use?** (control A.5.15 Access control)
59. Are access rights provided via a formal registration process? (control A.5.16 Identity management)
60. **Are there rules for passwords and other secret authentication information to be provided in a secure way, as well as for password**

management systems, and users, on how to manage and protect them? (control A.5.17 Authentication information)

61. **Is there a formal access management process to handle, review, and update access to information systems and users' access rights?** (control A.5.18 Access rights)
62. **Is there a policy on how to treat the risks related to suppliers and partners?** (control A.5.19 Information security in supplier relationships)
63. **Are relevant security requirements included in the agreements with the suppliers and partners**? (control A.5.20 Addressing information security within supplier agreements)
64. **Do the agreements with providers and suppliers include security requirements?** (control A.5.21 Managing information security in the ICT supply chain)
65. **Are suppliers regularly monitored, and are changes involving arrangements and contracts with suppliers and partners taking into account risks and existing processes?** (control A.5.22 Monitoring, review and change management of supplier service)
66. **Are cloud services acquired, used, managed, and canceled according to information security requirements?** (control A.5.23 Information security for use of cloud services)
67. **Are incidents managed properly?** (control A.5.24 Information security **incident management planning and preparatio**n)
68. **Are security events assessed and classified properly?** (control A.5.25 Assessment and decision on information security events)
69. **Are procedures on how to respond to incidents documented?** (control A.5.26 Response to information security incidents)
70. **Are security incidents analyzed properly?** (control A.5.27 Learning from information security incidents)

71. **Do procedures exist which define how to collect evidence?** (control A.5.28 Collection of evidence)
72. **Are requirements for continuity of information security defined, implemented, exercised, and tested?** (control A.5.29 Information security during disruption)
73. **Is ICT readiness managed according to business continuity objectives and ICT requirements?** (control A.5.30 ICT readiness for business continuity)
74. **Are legislative, regulatory, contractual, and other security requirements listed?** (control A.5.31 Legal, statutory, regulatory and contractual requirements)
75. **Do procedures exist to protect intellectual property rights?** (control A.5.32 Intellectual property rights)
76. **Are records protected properly?** (control A.5.33 Protection of records)
77. **Is personally identifiable information protected properly?** (control A.5.34 Privacy and protection of PII) **Is information security regularly reviewed by an independent auditor?** (control A.5.35 Independent review of information security)
78. **Do the managers regularly review if the security policies and procedures are performed properly in their areas of responsibility, and that information systems are in compliance with the information security policies and standards?** (control A.5.36 Compliance with policies, rules and standards for information security)
79. **Are operating procedures for IT processes documented?** (control A.5.37 Documented operating procedures)

A.6 PEOPLE CONTROLS

80. **Does the organization perform background checks on candidates for employment or for contractors?** (control A.6.1 Screening)

81. **Are there agreements with employees and contractors that specify information security responsibilities?** (control A.6.2 Terms and conditions of employment)
82. **Do employees and contractors attend trainings to better perform their security duties, and do the awareness programs exist?** (control A.6.3 Information security awareness, education and training)
83. **Does the organization have a formal disciplinary process?** (control A.6.4 Disciplinary process)
84. **Are there agreements covering information security responsibilities that remain valid after the termination of employment?** (control A.6.5 Responsibilities after termination or change of employment)
85. **Does the organization list all the confidentiality clauses that need to be included in agreements with third parties?** (control A.6.6 Confidentiality or non-disclosure agreements)
86. **Are there rules defining how the organization's information is protected considering teleworking sites?** (control A.6.7 Remote working)
87. **Are information security events and weaknesses reported in properly by employees and contractors?** (control A.6.8 Information security event reporting)

A.7 PHYSICAL CONTROLS

88. **Do secure areas that protect sensitive information exist?** (control A.7.1 Physical security perimeters)
89. **Are the entrances to secure areas protected?** (control A.7.2 Physical entry)
90. **Are secure areas located in a protected way?** (control A.7.3 Securing offices, rooms and facilities)
91. **Are premises monitored for unauthorized access?** (control A.7.4 Physical security monitoring)

92. **Are the alarms, fire protection, and other systems installed?** (control A.7.5 Protecting against physical and environmental threats)
93. **Are working procedures for secure areas defined?** (control A.7.6 Working in secure areas)
94. **Is there orientation for users about what to do when they are not present at their workstations?** (control A.7.7 Clear desk and clear screen)
95. **Is the equipment properly protected?** (control A.7.8 Equipment siting and protection)
96. **Are the organization assets properly protected when they are not at the organization premises?** (control A.7.9 Security of assets off-premises)
97. **Are there procedures that define how to handle, protect, transport, and dispose of storage media, inside and outside the organization premises, in line with the classification rules and information sensitivity?** (control A.7.10 Storage media)
98. **Does the equipment have protection against energy variations?** (control A.7.11 Supporting utilities)
99. **Are the power and telecommunication cables adequately protected?** (control A.7.12 Cabling security)
100. **Is the equipment maintained regularly?** (control A.7.13 Equipment maintenance)
101. **Is information properly removed from media or equipment that will be disposed of?** (control A.7.14 Secure disposal or re-use of equipment)

A.8 TECHNOLOGICAL CONTROLS

102. **Are rules for the secure handling of mobile devices, and for protecting equipment when not in the physical possession of its users, defined?** (control A.8.1 User endpoint devices)
103. **Are privileged access rights managed with special care?** (control A.8.2 Privileged access rights)

104. **Is the access to information in systems restricted according to the access control policy?** (control A.8.3 Information access restriction)
105. **Is the access to source code restricted to authorized persons?** (control A.8.4 Access to source code)
106. **Is secure log-on required on systems according to the Access Control Policy?** (control A.8.5 Secure authentication)
107. **Are resources monitored and plans made to ensure their capacity to fulfill users' demands?** (control A.8.6 Capacity management)
108. **Are anti-virus software, and other software for malware protection installed and properly used?** (control A.8.7 Protection against malware)
109. **Is information about vulnerabilities properly managed, and are information systems regularly reviewed to check their compliance with the information security policies and standards?** (control A.8.8 Management of technical vulnerabilities)
110. **Are configurations of relevant IT assets properly handled?** (control A.8.9 Configuration management)
111. **Is data that is no longer required properly disposed of?** (control A.8.10 Information deletion)
112. **Is data masking applied according to applicable requirements?** (control A.8.11 Data masking)
113. **Do systems, networks, and devices include data leakage prevention measures?** (control A.8.12 Data leakage prevention)
114. **Is a backup policy defined and performed properly?** (control A.8.13 Information backup)
115. **Does IT infrastructure have redundancy (e.g.: secondary location) included in its planning and operation?** (control A.8.14 Redundancy of information processing facilities)
116. **Are relevant events from IT systems logged periodically, and are logs protected properly?** (control A.8.15 Logging)

117. **Are systems, networks, and applications monitored, and proper actions taken when anomalous behaviors are found?** (control A.8.16 Monitoring activities)
118. **Are clocks on all IT systems synchronized?** (control A.8.17 Clock synchronization)
119. **Is the use of utility tools controlled and limited to specific employees?** (control A.8.18 Use of privileged utility programs)
120. **Is installation of software strictly controlled?** (control A.8.19 Installation of software on operational systems)
121. **Are the networks controlled to protect information in systems and applications?** (control A.8.20 Networks security)
122. **Are security requirements for network services defined, and included in agreements?** (control A.8.21 Security of network services)
123. **Are the networks segregated considering risks and assets classification?** (control A.8.22 Segregation of networks)
124. **Is access to external websites controlled?** (control A.8.23 Web filtering)
125. **Does a policy to regulate encryption and other cryptographic controls exist?** (control A.8.24 Use of cryptography)
126. **Are rules for the secure development of software and systems defined?** (control A.8.25 Secure development life cycle)
127. **Is application information, including transaction information, transferred through public networks appropriately protected?** (control A.8.26 Application security requirements)
128. **Are principles for engineering secure systems applied to the organization system's development process?** (control A.8.27 Secure system architecture and engineering principles)
129. **Is software code developed according to defined principles?** (control A.8.28 Secure coding)

130. **Is the implementation of security requirements tested during system development, and are the criteria for accepting the systems defined?** (control A.8.29 Security testing in development and acceptance)

131. **Is the outsourced development of systems monitored?** (control A.8.30 Outsourced development)

132. **Are development, testing, and production environments separated and properly secured?** (control A.8.31 Separation of development, test and production environments)

133. **Are changes that could affect the information security of new or existing systems properly controlled and tested?** (control A.8.32 Change management)

134. **Are test data carefully selected and protected?** (control A.8.33 Test information)

135. **Are audits of production systems planned and executed properly?** (control A.8.34 Protection of information systems during audit testing)