Gap Analysis Tool for ISO 27001:2022

Document Control Information

- **Document Title:** ISO 27001:2022 Gap Analysis Tool
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]

Purpose

This gap analysis tool is designed to help organizations assess their current information security practices against the requirements of ISO 27001:2022. It identifies gaps that need to be addressed before pursuing certification or to improve the existing Information Security Management System (ISMS).

Instructions for Use

1. Complete all sections of the gap analysis
2. For each requirement, assess the current implementation status using the following scale:
   - Not Implemented (0): No evidence of implementation
   - Partially Implemented (1): Some evidence, but significant gaps exist
   - Mostly Implemented (2): Substantial evidence, minor gaps exist
   - Fully Implemented (3): Complete implementation with evidence
3. Document evidence and gaps for each requirement
4. Develop an action plan to address identified gaps
5. Prioritize actions based on risk and resource availability

Section 1: Context of the Organization (Clause 4)

4.1 Understanding the organization and its context

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Determination of external and internal issues relevant to the organization’s				

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
purpose and affecting its ability to achieve ISMS outcomes				
Process to monitor and review information about external and internal issues				

4.2 Understanding the needs and expectations of interested parties

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Determination of interested parties relevant to the ISMS				
Determination of requirements of interested parties relevant to information security				
Determination of which requirements will be addressed through the ISMS				
Process to monitor and				

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
review information about interested parties and their requirements				

4.3 Determining the scope of the ISMS

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Determination of boundaries and applicability of the ISMS				
Consideration of external and internal issues (4.1)				
Consideration of requirements of interested parties (4.2)				
Consideration of interfaces and dependencies between activities				
Documented scope				

4.4 Information security management system

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Establishment, implementation, maintenance, and continual improvement of ISMS				
Determination of processes				

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
needed for the ISMS				
Determination of process interactions				

Section 2: Leadership (Clause 5)

5.1 Leadership and commitment

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Top management demonstration of leadership and commitment				
Establishment of information security policy and objectives				
Integration of ISMS requirements into business processes				
Availability of resources for the ISMS				
Communication of importance of effective information security management				
Ensuring ISMS achieves intended outcomes				
Direction and support of persons contributing to the ISMS				
Promotion of continual improvement				
Support of other relevant management roles				

5.2 Policy

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Established information security policy				
Policy includes information security objectives or framework				
Policy includes commitment to satisfy applicable requirements				
Policy includes commitment to continual improvement				
Policy available as documented information				
Policy communicated within the organization				
Policy available to interested parties				

5.3 Organizational roles, responsibilities and authorities

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Assignment and communication of responsibilities and authorities				
Assignment of responsibility for ISMS conformance to ISO 27001				
Assignment of responsibility for reporting on ISMS performance				

Section 3: Planning (Clause 6)

6.1 Actions to address risks and opportunities

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Planning actions to address risks and opportunities				
Integration and implementation of actions into ISMS processes				
Evaluation of effectiveness of actions				
Defined and applied information security risk assessment process				
Defined and applied information security risk treatment process				
Statement of Applicability				
Information security risk treatment plan				
Risk owner approval of risk treatment plan and residual risks				

6.2 Information security objectives and planning to achieve them

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Established information security objectives				
Measurable objectives				
Communication of objectives				
Planning to achieve objectives				

6.3 Planning of changes

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Planned approach to ISMS changes				

Section 4: Support (Clause 7)

7.1 Resources

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Determination and provision of resources for ISMS				

7.2 Competence

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Determination of necessary competence				
Ensuring competence based on education, training, or experience				
Actions to acquire necessary competence				
Evaluation of effectiveness of actions taken				
Documented information as evidence of competence				

7.3 Awareness

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Awareness of information security policy				
Awareness of contribution to ISMS effectiveness				
Awareness of implications of not conforming with ISMS requirements				

7.4 Communication

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Determination of internal and external communications				
Determination of what, when, with whom, who, and how to communicate				

7.5 Documented information

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
ISMS documented information required by ISO 27001				
ISMS documented information determined as necessary				
Appropriate identification, description, format, and media				
Review and approval for suitability and adequacy				

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Control of documented information				
Protection of documented information				

Section 5: Operation (Clause 8)

8.1 Operational planning and control

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Planning, implementation, and control of processes				
Established criteria for processes				
Control of processes according to criteria				
Documented information of process execution				
Control of planned changes and unintended changes				
Control of outsourced processes				

8.2 Information security risk assessment

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Performance of risk assessments at planned intervals				
Documented information of risk assessment results				

8.3 Information security risk treatment

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Implementation of risk treatment plan				
Documented information of risk treatment results				

Section 6: Performance Evaluation (Clause 9)

9.1 Monitoring, measurement, analysis and evaluation

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Evaluation of information security performance and ISMS effectiveness				
Determination of what needs to be monitored and measured				
Determination of methods for monitoring, measurement, analysis, and evaluation				
Determination of when to monitor and measure				

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Determination of who shall monitor and measure				
Determination of when to analyze and evaluate results				
Determination of who shall analyze and evaluate results				
Documented information as evidence of results				

9.2 Internal audit

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Internal audits at planned intervals				
Planned, established, implemented, and maintained audit program				
Defined audit criteria and scope				
Selection of auditors and conduct of audits				
Reporting of audit results to relevant management				
Documented information as evidence of audit program and results				

9.3 Management review

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Management review at planned intervals				
Consideration of status of actions from previous reviews				
Consideration of changes in external and internal issues				
Consideration of feedback on information security performance				
Consideration of feedback from interested parties				
Consideration of risk assessment results and risk treatment plan status				
Consideration of opportunities for continual improvement				
Outputs including decisions related to continual improvement and changes				
Documented information as evidence of management review results				

Section 7: Improvement (Clause 10)

10.1 Nonconformity and corrective action

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Reaction to nonconformity and action to control and correct it				

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Dealing with consequences				
Evaluation of need for action to eliminate causes				
Implementation of any action needed				
Review of effectiveness of corrective action				
Changes to ISMS if necessary				
Appropriateness of corrective actions				
Documented information as evidence				

10.2 Continual improvement

Requirement	Status (0-3)	Evidence	Gaps	Actions Required
Continual improvement of ISMS suitability, adequacy, and effectiveness				

Section 8: Annex A Controls Assessment

This section provides a high-level assessment of the implementation status of controls from Annex A of ISO 27001:2022. For a detailed assessment, refer to the Statement of Applicability.

Organizational Controls (A.5)

Control Category	Status (0-3)	Key Gaps	Priority Actions
Information Security Policies (A.5.1)			

Control Category	Status (0-3)	Key Gaps	Priority Actions
Information Security Roles and Responsibilities (A.5.2-A.5.4)			
Segregation of Duties (A.5.3)			
External Party Relationships (A.5.5-A.5.6, A. 5.19-A.5.22)			
Threat Intelligence (A.5.7)			
Project Management (A.5.8)			
Asset Management (A.5.9-A.5.14)			
Access Control (A.5.15-A.5.18)			
Cloud Services (A.5.23)			
Incident Management (A.5.24-A.5.28)			
Business Continuity (A.5.29-A.5.30)			
Compliance (A.5.31-A.5.37)			

People Controls (A.6)

Control Category	Status (0-3)	Key Gaps	Priority Actions
Human Resource Security (A.6.1-A. 6.5)			
Awareness and Training (A.6.3)			
Confidentiality (A.6.6)			
Remote Working (A.6.7)			
Incident Reporting (A.6.8)			

Physical Controls (A.7)

Control Category	Status (0-3)	Key Gaps	Priority Actions
Physical Security Perimeters and Entry (A.7.1-A.7.2)			
Physical Security Monitoring (A.7.4)			
Clear Desk and Clear Screen (A.7.7)			
Equipment Security (A.7.8-A.7.14)			

Technological Controls (A.8)

Control Category	Status (0-3)	Key Gaps	Priority Actions
User Access Management (A.8.1-A.8.4)			
Authentication (A.8.5)			
Malware Protection (A.8.7)			
Vulnerability Management (A.8.8)			
Configuration Management (A.8.9)			
Data Protection (A.8.10-A.8.12)			
Backup (A.8.13)			
Logging and Monitoring (A.8.15-A.8.16)			
Network Security (A.8.20-A.8.23)			
Cryptography (A.8.24)			
Secure Development (A.8.25-A.8.31)			
Change Management (A.8.32)			

Gap Analysis Summary

Overall Implementation Status

- **Clause 4 (Context)**: [Average Score] - [Brief Assessment]
- **Clause 5 (Leadership)**: [Average Score] - [Brief Assessment]
- **Clause 6 (Planning)**: [Average Score] - [Brief Assessment]
- **Clause 7 (Support)**: [Average Score] - [Brief Assessment]
- **Clause 8 (Operation)**: [Average Score] - [Brief Assessment]
- **Clause 9 (Performance Evaluation)**: [Average Score] - [Brief Assessment]
- **Clause 10 (Improvement)**: [Average Score] - [Brief Assessment]
- **Annex A Controls**: [Average Score] - [Brief Assessment]

Major Gaps Identified

1. [Gap 1]
2. [Gap 2]
3. [Gap 3]
4. [Gap 4]
5. [Gap 5]

Recommended Priority Actions

1. [Action 1]
2. [Action 2]
3. [Action 3]
4. [Action 4]
5. [Action 5]

Implementation Roadmap

Priority	Action	Responsible	Target Date	Resources Required	Status
High					
High					
Medium					
Medium					
Low					

Conclusion

[Provide an overall assessment of the organization’s readiness for ISO 27001:2022 certification and key recommendations]

Gap Analysis Information

- **Assessment Date(s):** [DATE]
- **Assessment Scope:** [SCOPE]
- **Lead Assessor:** [NAME]
- **Assessment Team Members:** [NAMES]
- **Organization Representatives:** [NAMES]

Approval

This Gap Analysis has been reviewed and approved by:

Name: ________________________ Position: ______________________ Date: _________________________ Signature: _____________________