CyberTechJournals

ISO/IEC 27001:2022 ISMS Implementation Checklist

This checklist outlines the key steps for establishing, implementing, and certifying an ISO/IEC 27001:2022 Information Security Management System (ISMS). It aligns with the 2022 revision of the standard and references Annex A control categories (Organisational, People, Physical, Technological) [1]. Each item includes implementation guidance and columns for audit-ready tracking (Status, Notes, Responsible, Timeline).

Step	Implementation Guidance	Annex A Category	Status	Notes	Responsible	Timeline
1. Top Management Commitment	Secure active support from top management and allocate sufficient resources (personnel, budget, authority) [2]. Form an ISMS project team with defined roles across departments to oversee implementation.	Organisational				
2. Define Scope, Objectives, Project Plan	Define the ISMS scope (boundaries and applicability) (Clause 4.3) and establish measurable security objectives [3]. Develop a project plan outlining scope, timelines, and required resources [4].	Organisational				

Step	Implementation Guidance	Annex A Category	Status	Notes	Responsible	Timeline
3. Analyze Context and Stakeholders	Analyze internal and external issues affecting the ISMS (Clause 4.1) [5] . Identify interested parties and their requirements (Clause 4.2) to align the ISMS with stakeholder needs [6] .	Organisational				
4. Conduct Risk Assessment	Perform a comprehensive risk assessment (Clause 6.1.2) to identify information security risks (threats, vulnerabilities, impacts) [7] . Evaluate and prioritize risks based on their potential impact and likelihood.	Organisational				
5. Perform Risk Treatment and Select Controls	Develop a Risk Treatment Plan (RTP) to mitigate identified risks (Clauses 6.1.3, 8.3) [8] . Select appropriate controls from Annex A to address each risk and document these selections in the Statement of Applicability (SoA) [9] .	Organisational				

Step	Implementation Guidance	Annex A Category	Status	Notes	Responsible	Timeline
6. Establish Security Policy and Objectives	Establish an Information Security Policy and define measurable security objectives (Clauses 5.2, 6.2) [10]. Align policies with organizational goals and communicate them clearly to the organization.	Organisational				
7. Develop ISMS Documentation	Develop and maintain required ISMS documentation (policies, procedures, records) (Clause 7.5) [11]. Ensure documents are approved, version-controlled, and accessible to relevant personnel.	Organisational				

Step	Implementation Guidance	Annex A Category	Status	Notes	Responsible	Timeline
8. Allocate Resources and Responsibilities	Allocate necessary resources (personnel, technology, budget) (Clause 7.1) and assign clear responsibilities for each ISMS task [2] [12]. Ensure accountability and authority for security roles.	Organisational				
9. Implement Training and Awareness	Implement an awareness and training program (Clauses 7.2, 7.3) so that all staff understand their ISMS responsibilities [13] [14]. Provide regular security training and maintain records of competency.	People				

Step	Implementation Guidance	Annex A Category	Status	Notes	Responsible	Timeline
10. Implement Security Controls	Implement the selected Annex A controls across all categories. This includes: organisational controls (e.g., policies, procedures, roles); people controls (e.g., background checks, training); physical controls (e.g., facility access, equipment protection); and technological controls (e.g., access control, encryption) [1] [15] .	Organisational, People, Physical, Technological				
11. Operate ISMS and Maintain Records	Operate the ISMS as part of day-to-day operations. Maintain records/logs of implemented controls and security events (Clause 7.5) [16] . Use these records as evidence of compliance during audits.	Organisational				

Step	Implementation Guidance	Annex A Category	Status	Notes	Responsible	Timeline
12. Monitor and Measure ISMS Performance	Define metrics (Clause 9.1) and monitor performance indicators (e.g., incidents, audit results) [17]. Regularly review results against objectives and initiate corrective actions as needed.	Organisational				
13. Conduct Internal Audit	Conduct internal audits (Clause 9.2) at planned intervals to verify ISMS conformance [18]. Document audit findings and ensure nonconformities are addressed.	Organisational				
14. Management Review	Hold management review meetings (Clause 9.3) to evaluate ISMS performance, resource needs, and strategic alignment [19]. Use the outcomes to approve improvements and align security with business strategy.	Organisational				

Step	Implementation Guidance	Annex A Category	Status	Notes	Responsible	Timeline
15. Implement Corrective Actions	Systematically address nonconformities (Clause 10.1). Investigate root causes and implement corrective actions; update ISMS documentation and controls as needed [20].	Organisational				
16. Certification Audit Preparation	Engage an accredited certification body and prepare for audit. Ensure all ISMS documentation, controls, and records are audit-ready. The auditor will verify compliance with ISO/IEC 27001:2022 requirements [21].	Organisational				

Each checklist item above should be reviewed and marked **Status** (e.g. “Not Started/In Progress/Complete”), with any **Notes**, and assigned a **Responsible Party** and planned **Timeline** to ensure audit readiness. All guidance points and references align with ISO/IEC 27001:2022 clauses and Annex A control categories for a thorough and compliant implementation.

Sources: Implementation guidance and controls reference based on ISO/IEC 27001:2022 materials [1] [10] [9] [21] (see citations above).

---

[1] [2] [3] [4] [5] [6] [7] [8] [10] [11] [12] [13] ISO 27001 Checklist - Your Guide for Compliance | ISMS.online
https://www.isms.online/iso-27001/checklist/

[9] [14] [15] [16] [17] [18] [19] [20] Implement ISO 27001 | Easy ISO 27001 implementation checklist
https://advisera.com/27001academy/knowledgebase/iso-27001-implementation-checklist/

21 ISO 27001 Implementation | Free Checklist | IT Governance USA
https://www.itgovernanceusa.com/implementing_iso27001