Cycubix

ISO 27001 Implementation Plan

Requirements	Objective	Deliverable
Phase 1: PLAN / CREATE (Planning, Scoping and Risk)		
Planning		
Definitions and Terminology	Create your ISMS Glossary to keep the organisation aligned on the same terms.	**ISMS Glossary**
Context of the organization and stakeholder expectations (Clause 4.1 and 4.2)	Determine external and internal factors relevant to organisational purpose that drive security needs.	**Context Analysis Report** (Internal/External context, Drivers, Legal/Regulatory landscape, Stakeholder Needs Matrix)
Scope of the ISMS (clause 4.3)	Define critical assets, organisational boundaries, assets, business processes, and regulatory requirements covered by the ISMS.	**ISMS Scope Statement** Comprehensive document detailing included/excluded systems, processes, locations, and justifications.

Cycubix

ISO 27001 Implementation Plan

Requirements	Objective	Deliverable
Leadership (Clause 5.1)	Secure leadership commitment and accountability, strategic alignment, and resource allocation for ISMS success.	**Leadership Agreement** CEO statement and stakeholder engagement framework with defined responsibilities
Information Security Policy (Clause 5.2)	The Information Security Policy aligns security goals with business goals up front. It answers the question "Why do we care about security?" and provides strategic guidance for all subsequent milestones.	**Information Security Policy** It is created up front and finalised in Phase 2.

Organizational Roles, responsibilities and authorities (Clause 5.3)	Assign formal accountability for all ISMS roles including Information Security Officer, Risk Owners, and Internal Auditors
	Identify project resources:
	• Funding
	• Project Team
	  ○ Project Leader
	  ○ Cross-Functional Team
	  ○ External Consultants
	  ○ Audit and Certification Partners
	• Technologies
		ISMS Organisation Chart
		RACI (Responsibility, Accountability, Consulted, Informed) Matrix.
		Clear accountability structure with reporting relationships.
		Project Kick Off bringing together the Business Objectives/Plan/People/Technologies

Cycubix

ISO 27001 Implementation Plan

Requirements	Objective	Deliverable
Risk		
Perform Gap Assessment	Benchmark current state against ISO 27001 requirements. Is the control/procedure present or absent? It identifies the problem.	**Gap Assessment Report** **Initial Maturity Baseline**
Identify Assets (Clause 6.1.2)	Define which information assets need protection. Identify owners, and dependencies.	**Asset Registers** Systems, Data, Devices, Suppliers.
Information Security Risk Assessment (Clause 6.1.2)	Establishes how the organisation will assess risk (risk methodology, scoring, appetite).	**Risk Register** Documents the impact of the identified risks.
Information Security Risk Treatment (Clause 6.1.3, Annex A ISO 27001, ISO 27002)	Decide how to handle each risk (mitigate, transfer, etc.).	**Risk Treatment Plan** Includes selected controls, rationale, residual risk and resources needed.

Cycubix

ISO 27001 Implementation Plan

Requirements	Objective	Deliverable
SOA (6.1.3)	Select the controls to be implemented, rationale, and exclusion justifications.	**Statement of Applicability (SoA)** Comprehensive control framework with implementation status (framework, structure, methodology).
Information Security Objectives (Clause 6.2)	The ISMS objectives are the measurable solutions to the problems previously identified. Should be consistent with security policy, available, monitored, communicated and updated.	**ISMS Objectives**
Plan Remediation Activities to Achieve Objectives (Clause 6.2)	Define actionable remediation and milestones.	**Remediation Plan** with owners and deadlines.
Support (the bridge between planning and execution)		
Secure Resources (Clause 7.1)	Allocate required personnel, tools, and budget required to address the Remediation Plan.	**Resource Plan** **Budget Approval**

Cycubix

ISO 27001 Implementation Plan

Requirements	Objective	Deliverable
Competence (Clause 7.2)	Ensure personnel possess necessary competencies for ISMS roles.	**Competence Assessment** **Training Plan**
Awareness (Clause 7.3)	Build organisational security awareness through targeted education and training.	**Security Awareness Training Evidence**
Communication (Clause 7.4)	Establish internal and external communication processes for ISMS information.	**Communication Strategy** What, when, with and how to communicate relevant information about the ISMS.
Documentation and control (Clause 7.5)	Formalise the system to create, update, and control ISMS documentation throughout its lifecycle	**Document Management System** Document hierarchy, version control, and access management. **Update Information Security Policy.**
Phase 1 outcomes: ISMS Scope, Information Security Policy, RACI Matrix, Objectives, Project Plan, Gap Assessment, Assets Registers, Risk Register, Risk Treatment Plan, Initial SoA,Remediation Plan, Competence & Training Records.		

Cycubix

ISO 27001 Implementation Plan

Requirements	Objective	Deliverable
Phase 2: DO/ IMPLEMENT(Building the ISMS)		
Operations		
Operational Planning and Control (Clause 8.1)	Implement planned processes and controls to achieve ISMS objectives Establish KPIs (risk reduction, incident response time, compliance levels).	**Operational Procedures** Process documentation, work instructions, and performance monitoring (Operational Procedures + ISMS Runbook).
Information Security Risk Assessment (Clause 8.2)	Execute risk assessment processes according to methodology defined in clause 6.1.2.	**Updated Risk Register** **Assessment Records**
Information Security Risk Treatment (Clause 8.3)	Implement selected risk treatment measures and security controls.	**Control Implementation Evidence** **Updated SoA**
Phase 2 Outcomes: ISMS Documentation (Policies, Standards, Procedures), Security Control Evidence		

Cycubix

ISO 27001 Implementation Plan

Requirements	Objective	Deliverable
Phase 3: CHECK / MAINTAIN (Audits and Certification)		
Monitoring and Measurement (Clause 9.1)	Monitor ISMS performance against objectives using defined metrics.	**Performance Dashboard** KPIs, trend analysis, and performance reports.
Internal Audit (Clause 9.2)	Conduct independent and systematic audits to verify ISMS conformity and effectiveness.	**Internal Audit Program** Audit schedule, Non-conformity logs, and corrective action tracking.
Management Review (Clause 9.3)	Leadership review of ISMS performance and strategic alignment	**Management Review Reports**: Performance analysis, improvement opportunities, and resource allocation decisions
Certification Stages	Prepare for external audit by an accredited body, and certification.	• **Stage 1** (documentation and readiness review) and **Stage 2** (implementation and effectiveness audit) **Audit Reports** • **Certification**
Phase 3 Outcomes: Audit Report, Recommendations, Certification, Maintenance procedure		

Cycubix

ISO 27001 Implementation Plan

Requirements	Objective	Deliverable
Phase 4: ACT / IMPROVE		
Nonconformity and Corrective Action (Clause 10.1)	Address non-conformities and implement corrective actions to prevent recurrence.	**Corrective Action Register** Root cause analysis, remediation plans, and effectiveness verification
Continual Improvement (Clause 10.2)	Drive ongoing enhancement of ISMS suitability, adequacy, and effectiveness	**Improvement Roadmap** Enhancement initiatives, innovation opportunities, and maturity advancement
Phase 4 Outcomes: Non-Conformity & Corrective Action Logs, Records of Improvement.		

https://www.cycubix.com

Terms of Use

Thank you for your interest in this **ISO 27001 Implementation Plan Template**, a complimentary resource offered to you by Cycubix LTD, to assist you and your organisation.

By downloading or using this artifact, you agree to the following terms of use. This artifact is offered for personal or organisational use only and may not be reproduced, sold, or distributed as your own.
All intellectual property rights remain exclusively with Cycubix LTD. You are granted a non-exclusive, non-transferable, and revocable license to utilize the artifact for internal purposes within your organisation. However, you are strictly prohibited from redistributing, modifying, or presenting this artifact in a manner that implies ownership or authorship outside of Cycubix LTD.

Cycubix LTD provides this artifact "as is" without any warranties, express or implied. We are not liable for any damages arising from the use of this artifact. By using this resource, you acknowledge and agree to these terms.

If you have any questions or require additional permissions, please contact us at info@cycubix.com.