MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

ISMS IMPLEMENTATION · 2026 EDITION

ISO/IEC 27001:2022
Controls & ISMS Overview

A practical, non-normative guide to ISMS scope, risk treatment, Annex A themes, evidence, and audit readiness.

4–10	93	4
Requirement clauses	Annex A controls	Control themes

mnatech.in @mna_tech_academy +91 9216110094

MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

How to use this guide

This guide explains the implementation logic around ISO/IEC 27001:2022 without reproducing the copyrighted standard. Organizations seeking certification must obtain the official standard and work with qualified professionals.

> **Professional-use notice:** Security testing must stay within systems you own or have explicit written authorization to assess. Standards summaries are educational aids, not certification, legal, or audit advice.

Inside this resource

01 **ISMS Structure**
Connect organizational context, leadership, planning, support, operation, evaluation, and improvement.

02 **Scope & Risk Assessment**
Create a repeatable basis for deciding which risks require treatment.

03 **Risk Treatment & Statement of Applicability**
Explain selected controls, exclusions, ownership, and residual risk.

04 **Annex A Themes**
Organize 93 controls across organizational, people, physical, and technological themes.

05 **Evidence & Audit Readiness**
Show that controls operate consistently, not merely that documents exist.

06 **90-Day Implementation Starter**
Turn the framework into a realistic initial operating rhythm.

ISMS Structure

Connect organizational context, leadership, planning, support, operation, evaluation, and improvement.

Clause area	Implementation focus
4 Context	Interested parties, needs, boundaries, ISMS scope
5 Leadership	Policy, accountability, roles, commitment
6 Planning	Risks, opportunities, objectives, change planning
7 Support	Resources, competence, awareness, communication, documents
8 Operation	Risk assessment and treatment execution
9 Evaluation	Monitoring, internal audit, management review
10 Improvement	Nonconformity, corrective action, continual improvement

Scope & Risk Assessment

Create a repeatable basis for deciding which risks require treatment.

Scope statement
Define locations, technology, processes, interfaces, and exclusions.

Asset and process context
Connect information to business owners and consequences.

Risk criteria
Agree likelihood, impact, acceptance, and review triggers.

Assessment consistency
Use repeatable identification, analysis, and evaluation.

Risk ownership
Assign accountable decision makers, not only technical teams.

Change triggers
Reassess after material systems, suppliers, incidents, or threats.

Risk Treatment & Statement of Applicability

Explain selected controls, exclusions, ownership, and residual risk.

Artifact	Minimum content
Risk treatment plan	Risk, selected treatment, control, owner, due date, status
Statement of Applicability	Applicable Annex A controls, implementation status, justification
Residual risk decision	Remaining exposure, approver, date, review condition
Control evidence	Policy, process record, configuration, test, metric
Exception	Reason, compensating controls, owner, expiration

Annex A Themes

Organize 93 controls across organizational, people, physical, and technological themes.

Organizational — 37

Policies, roles, assets, suppliers, cloud, incidents, continuity, compliance.

People — 8

Screening, terms, awareness, remote work, and responsibilities after exit.

Physical — 14

Perimeters, entry, monitoring, equipment, media, utilities, maintenance.

Technological — 34

Identity, access, endpoints, networks, development, logging, resilience, data protection.

Remember: Annex A is a reference set for risk treatment. Applicability must be justified through the organization’s own risks and obligations.

Evidence & Audit Readiness

Show that controls operate consistently, not merely that documents exist.

Document control
Approvals, versions, owners, access, retention, and obsolete-document handling.

Operational records
Tickets, reviews, training, tests, backups, alerts, and supplier evidence.

Internal audit
Independent program covering requirements and ISMS effectiveness.

Management review
Inputs, decisions, actions, resource needs, and follow-up.

Corrective action
Contain, analyze root cause, correct, verify effectiveness.

Metrics
Use decision-relevant measures with thresholds, owners, and trends.

90-Day Implementation Starter

Turn the framework into a realistic initial operating rhythm.

Days 1–15 · Context

Nominate sponsor, define objectives, identify interested parties, draft scope.

Days 16–30 · Baseline

Inventory key processes and information, define risk method, identify obligations.

Days 31–50 · Assess

Run risk assessment, assign owners, prioritize unacceptable risks.

Days 51–70 · Treat

Build treatment plan and SoA; implement priority controls and evidence capture.

Days 71–82 · Evaluate

Measure, conduct internal audit, track nonconformities.

Days 83–90 · Review

Hold management review, approve actions, establish continual-improvement cycle.

Official references

- ISO/IEC 27001:2022 — https://www.iso.org/standard/27001
- ISO/IEC 27002:2022 — https://www.iso.org/standard/75652.html



Keep learning. Keep building.

Use this guide as a working plan: practise, document evidence, review outcomes, and improve the next iteration.

mnatech.in @mna_tech_academy +91 9216110094

© 2026 MNA Tech Academy. Original educational resource. Product names and trademarks belong to their respective owners. Verify standards and product details against official sources before production use.