K7

ISO 27001 Implementation Roadmap

3 pages • CyberK7 Whitepaper

A phase-by-phase guide from initial gap assessment through Statement of Applicability, control implementation, internal audit and certification body audit.

1. What ISO 27001 Actually Requires

ISO 27001 requires an Information Security Management System (ISMS) — a structured, risk-based approach to managing security across people, processes and technology, not just a checklist of technical controls.

The standard requires you to identify risks, decide how to treat them, implement proportional controls from Annex A, and continually monitor and improve the system over time.

2. The Six-Phase Roadmap

Phase 1 — Gap Assessment: Evaluate current controls against ISO 27001 Annex A to understand your starting point.

Phase 2 — Scope & Statement of Applicability (SoA): Define what's in scope for certification and document which of the 93 Annex A controls apply to your organization and why.

Phase 3 — Policy & Control Implementation: Build the required policies, risk treatment plans, and implement technical and procedural controls.

Phase 4 — Internal Audit: Conduct an internal audit to validate readiness and catch gaps before the external audit does.

Phase 5 — Certification Audit: Undergo Stage 1 (documentation review) and Stage 2 (implementation evidence) audits with an accredited certification body.

Phase 6 — Continuous Improvement: Maintain the ISMS through annual surveillance audits and a 3-year recertification cycle.

3. What Slows Teams Down

The most common delay isn't technical control implementation — it's building genuine evidence of operation. Auditors want to see controls working over time (access reviews actually happening, incidents actually being logged), not just policies that exist on paper.

About CyberK7

CyberK7 is a cybersecurity consulting firm based in Delhi, India, helping organizations build secure, resilient and compliant digital environments through GRC, VAPT, SOC monitoring, cloud security, IAM, EDR/XDR, backup & disaster recovery, and security awareness training.

Our consultants hold certifications including CISA and ISO 27001 Lead Auditor, with hands-on experience across banking, healthcare, manufacturing, education and fast-growing startups.

To discuss how this whitepaper applies to your organization, reach us at info@cyberk7.com or +91 98990 62199.

Quick Reference

Phase	Typical Duration	Key Output

Gap Assessment	1–2 weeks	Baseline maturity report
Scope & SoA	2–3 weeks	Statement of Applicability
Implementation	6–10 weeks	Policies & operating controls
Internal Audit	1–2 weeks	Internal audit report
Certification Audit	2–4 weeks	ISO 27001 certificate

For a tailored consultation, contact CyberK7 at info@cyberk7.com or +91 98990 62199.