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.

CyberK7 | Delhi, India | cyberk7.com

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.

2. The Six-Phase Roadmap

Phase 1 — Gap Assessment. Phase 2 — Scope & Statement of Applicability. Phase 3 — Policy & Control Implementation. Phase 4 — Internal Audit. Phase 5 — Certification Audit (Stage 1 & Stage 2). Phase 6 — Continuous Improvement through annual surveillance audits.

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, not just policies that exist on paper.

About CyberK7

CyberK7 supports organizations through every phase of the ISO 27001 journey, from gap assessment to certification. Contact 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.