CyberSentinels

PRACTITIONER GUIDE

Security & Compliance Starter Kit

A practical 12-week path to ISO 27001, SOC 2, GDPR and DPDPA readiness — with the control checklists, evidence lists and board metrics we use on live engagements.

What is inside

- 12-week readiness roadmap with owners, milestones and exit criteria.
- ISO 27001:2022 mandatory documentation checklist (Annex A aligned).
- SOC 2 Trust Services Criteria evidence matrix and observation-window planner.
- GDPR and DPDPA privacy readiness checklist: records, notices, consent and DSR workflow.
- Vendor and third-party risk questionnaire starter set.
- Board-level security metrics pack — nine KPIs that survive scrutiny.

Free 30-minute scoping call

Bring this kit to a call and we will map it to your scope, deadline and customer requirements. Book at cybersentinels.in/contact

The 12-week readiness roadmap

Most first-time certification programmes fail on evidence, not controls. This sequence front-loads scope and ownership so the audit window is a formality rather than a scramble.

WEEKS 1–2

Scope & gap assessment

Define the ISMS or system boundary, list in-scope systems, data flows and third parties, and run a control gap assessment against the target framework.

WEEKS 3–5

Risk & treatment

Complete the risk assessment methodology, register and treatment plan. Produce the Statement of Applicability with justified exclusions.

WEEKS 6–9

Control implementation

Close policy, access, logging, change, vendor and incident gaps. Every control gets a named owner and a repeatable evidence source.

WEEKS 10–11

Evidence & internal audit

Collect one full cycle of operating evidence, run the internal audit and close nonconformities before the auditor sees them.

WEEK 12

Management review & audit readiness

Management review, corrective action log, auditor shortlist and stage 1 preparation pack.

ISO 27001:2022 documentation checklist

Mandatory records an accredited certification body will ask to see. Treat each as a working document with a version history, not a template you sign once.

- ISMS scope statement, including exclusions and their justification.
- Information security policy and measurable security objectives.
- Risk assessment and risk treatment methodology, plus documented results.
- Statement of Applicability covering all 93 Annex A controls.
- Risk treatment plan with owners, due dates and residual risk acceptance.
- Evidence of competence, awareness training and role assignments.
- Monitoring, measurement, analysis and evaluation results.
- Internal audit programme and audit reports.
- Management review minutes and decisions.
- Nonconformity and corrective action records.
- Operational planning and control records for in-scope processes.
- Supplier and third-party security agreements and review records.

SOC 2 evidence matrix — start here

- Common Criteria (Security) is mandatory; add Availability, Confidentiality, Processing Integrity or Privacy only where you make customer commitments.
- Map each criterion to a control, a system of record and a sampling frequency before the observation window opens.
- Type 1 attests design at a point in time; Type 2 tests operating effectiveness over three to twelve months.
- Reuse ISO 27001 controls where they overlap — typically more than half the control set.

GDPR & DPDPA privacy readiness

- Data inventory and records of processing, mapped to lawful basis or notified purpose.
- Layered privacy notices in every collection channel, in the languages you operate in.
- Consent capture, withdrawal and audit trail — including granular consent for DPDPA.
- Data subject and data principal request workflow with statutory response clocks.
- Cross-border transfer mechanism assessment and contractual safeguards.
- Breach detection, assessment and notification runbook with regulator timelines.
- Processor and sub-processor due diligence and contract clauses.
- Retention schedule and defensible deletion evidence.

Nine board metrics that survive scrutiny

01 Critical and high findings open past SLA

02 Mean time to remediate by severity

03 Assets under vulnerability management

04 Phishing simulation failure rate trend

05 Privileged accounts with MFA enforced

06 Third parties reviewed in 12 months

07 Backup restore tests passed

08 Security incidents by category and impact

09 Control evidence collected on schedule

Want this mapped to your scope?

Book a free 30-minute scoping call and we will tell you the smallest credible path to your deadline — cybersentinels.in/contact