This checklist walks an Indian SME through an **ISO/IEC 27001:2022** implementation — from scope to certificate. It covers the mandatory management-system clauses (4–10), the Annex A control themes, the 11 new 2022 controls auditors probe hardest, and the certification journey with an accredited body. Tick what you can evidence today; anything unticked is your build plan. It pairs with the full implementation guide on GRC RADAR (vcisodesk.com/iso-27001-implementation-guide-india-sme/).

The 2022 standard — facts you plan against

Operative version: ISO/IEC 27001:2022 (published 25 Oct 2022) + Amendment 1:2024 (climate-change context, 23 Feb 2024). The 2013 version is dead — the IAF MD 26 transition window closed **31 October 2025**; a 2013 certificate today is an expired credential.

Annex A: 93 reference controls in 4 themes — Organizational (37), People (8), Physical (14), Technological (34). Referential, not prescriptive: your Statement of Applicability (SoA) justifies what you apply and what you exclude.

Accreditation: certify only with a CB accredited by an IAF-MLA signatory (NABCB in India). Unaccredited certificates are routinely rejected at vendor due diligence.

Cycle: Stage 1 (documentation) + Stage 2 (implementation) → 3-year certificate, surveillance audits end of Year 1 and Year 2, recertification before expiry.

Indian regulatory stack: not statutorily mandated by DPDP (but the strongest 'reasonable safeguards' evidence under s.8(5)); mandatory for SEBI MIIs only, recommended for Qualified REs (28 Aug 2025 clarifications); industry practice — not a CERT-In Directions requirement.

1. Scope & context — Clause 4

- ☐ **4.1** Internal and external issues relevant to the ISMS documented — including whether **climate change** is a relevant issue (Amd 1:2024; "not applicable" is acceptable if the reasoning is documented).
- ☐ **4.2** Interested parties (customers, regulators, employees, suppliers) and their requirements identified — noting any climate-related requirements.
- ☐ **4.3** ISMS scope precisely defined and documented — locations, products, teams, systems. Scope you cannot evidence is the most common first-cycle failure; start narrow and clean.
- ☐ **4.4** ISMS established as a managed system — process map of how context, risk, controls, and improvement connect.

2. Leadership & planning — Clauses 5–6

- ☐ **5.1** Top management commitment demonstrable — resources allocated, security objectives integrated with business planning.
- ☐ **5.2** Information security policy approved, communicated, and actually read by the director who signed it (a template signed unread is a guaranteed non-conformity).
- ☐ **5.3** Roles, responsibilities and authorities for information security assigned and communicated.
- ☐ **6.1** Risk assessment methodology established; information security risk assessment conducted and current.
- ☐ **6.1.3** Risk treatment plan produced; **Statement of Applicability** drafted with real, risk-driven justification per control — the single most-scrutinised audit document.
- ☐ **6.2** Measurable information security objectives set, with plans to achieve them.
- ☐ **6.3** Changes to the ISMS carried out in a planned manner (new 2022 clause requirement).

3. Support & operation — Clauses 7–8

- ☐ **7.2** Competence evidence on file — training records, role descriptions, certifications (the classic SME under-investment).
- ☐ **7.3** Awareness programme running — staff know the policy, their role in it, and the cost of ignoring it.
- ☐ **7.5** Documented information controlled — versioning, ownership, approval, availability.
- ☐ **8.1** Operational controls implemented per the risk treatment plan; outsourced processes controlled.
- ☐ **8.2** Risk assessment re-run at planned intervals and on significant change.
- ☐ **8.3** Risk treatment implemented and tracked to closure.

4. Evaluation & improvement — Clauses 9–10

- [ ] **9.1** Monitoring and measurement defined — what is measured, how, when, by whom, with results retained.
- [ ] **9.2** Internal audit programme operating — annual cycle, auditor independent of the area audited, documented findings and management response.
- [ ] **9.3** Management review held with documented inputs, outputs, decisions, and actions (a 20-minute calendar event will not satisfy 9.3).
- [ ] **10.1** Nonconformity register live — root-cause analysis, corrective action, verification of effectiveness.
- [ ] **10.2** Continual improvement evidenced — lessons from incidents, audits, and reviews feed back into the ISMS.

5. Annex A — the four themes (select via your SoA)

- [ ] **A.5 Organizational (37 controls)** — policies, roles, segregation of duties, threat intelligence, asset management, classification, access control policy, supplier relationships, incident management, compliance. Most SME implementation effort lands here.
- [ ] **A.6 People (8 controls)** — screening, employment terms, awareness training, disciplinary process, post-employment duties, NDAs, remote working, event reporting. Small in number, high in audit attention.
- [ ] **A.7 Physical (14 controls)** — perimeter, secure areas, equipment, secure disposal, clear desk/screen, media handling. Reduced — never zero — for cloud-native SMEs: laptops, home offices, and returned-device destruction remain in scope.
- [ ] **A.8 Technological (34 controls)** — endpoints, privileged access, authentication, malware, vulnerability management, network security, cryptography, secure development, change management, backup. SaaS-heavy SMEs usually have the substance, not the documentation.

The 11 controls new in 2022 — the ones auditors probe first: threat intelligence · cloud services security · ICT readiness for business continuity · physical security monitoring · configuration management · information deletion · data masking · data leakage prevention · monitoring activities · web filtering · secure coding. A 2013-era implementation that has not deliberately addressed these eleven is the one most likely to surface non-conformities.

6. Certification journey

- [ ] **C.1** Gap analysis against 27001:2022 complete (months 0–2 for a typical SME).
- [ ] **C.2** ISMS built — policies, risk assessment, SoA, controls, training (months 2–5).
- [ ] **C.3** Three months of operating evidence accumulated, including one internal audit cycle and one management review (months 5–7).
- [ ] **C.4** Certification body selected and **IAF-MLA accreditation verified** (NABCB list: nabcb.qci.org.in).
- [ ] **C.5** Stage 1 audit passed (documentation review); findings remediated.
- [ ] **C.6** Stage 2 audit passed (implementation); certificate issued — 3-year validity.
- [ ] **C.7** Surveillance calendar booked — Year 1 and Year 2 audits, recertification before expiry.

7. Quick planning facts

Question	Realistic answer (Indian SME)
How long?	6–12 months from a low base. 6 months needs a focused team, prior maturity, and a small clean scope. Anyone promising 3 months is selling a thin implementation.
How much?	Blended first-cycle estimates: small SME (<50 staff, cloud-native) ₹2L–₹3L; mid-size (50–500) ₹3L–₹8L; large (500+) ₹10L+. CB audit fees alone ₹1.5L–₹5L by scope.
Document set?	Roughly 25–35 documents for a 100-person company; about half that for a 25-person company.
Where SMEs fail?	Scope sprawl · SoA as fill-in-the-blanks · documents without operating evidence · non-independent internal audit · management review as a calendar event · unaccredited CB.
ISO 27001 or SOC 2?	Driven by buyers: US tech buyers → SOC 2 Type II first; EU/UK/Indian enterprise/government → ISO 27001 first. A solid ISMS commonly covers ~60–80% of the SOC 2 evidence set.

Source: ISO/IEC 27001:2022 (incl. Amd 1:2024), ISO/IEC 27002:2022, IAF MD 26. Summary for working use — not legal or certification advice.

Content current as of 5 June 2026. Read the full pillar guide at vcisodesk.com/iso-27001-implementation-guide-india-sme/ — free, like everything on GRC RADAR.