ISO 27001:2022 Readiness & Gap Assessment Checklist

A practical checklist for assessing ISMS readiness against ISO 27001:2022 and Annex A controls

ISO 27001 · ISO 27002 · ISMS · NIST CSF · GDPR · POPIA

Certification against ISO 27001 depends on a working information security management system, not just a policy set. This checklist sets out a practical sequence for scoping, assessing, and closing gaps before an external audit.

A Context, Scope & Leadership

- [ ] Define the ISMS scope, including sites, business units, and information systems covered
- [ ] Identify interested parties and their information security requirements
- [ ] Document the information security policy and get top management sign-off
- [ ] Assign information security roles, responsibilities, and authorities
- [ ] Confirm management commitment through resourcing and governance forums

B Risk Assessment & Treatment

- [ ] Maintain an asset inventory covering all information assets in scope
- [ ] Apply a documented risk assessment methodology consistently across the ISMS
- [ ] Identify threats and vulnerabilities against each in-scope asset
- [ ] Produce a risk treatment plan with owners and target dates
- [ ] Complete a Statement of Applicability covering all Annex A controls

C Organisational Controls (Annex A.5)

- [ ] Maintain information security policies approved and reviewed on a set cycle
- [ ] Define roles and segregation of duties for security-sensitive functions
- [ ] Maintain a supplier and third-party security requirements register
- [ ] Manage information security incidents through a documented process
- [ ] Track compliance with legal, statutory, and contractual requirements

D People Controls (Annex A.6)

- ☐ Screen personnel appropriately before granting access to sensitive information
- ☐ Include information security responsibilities in employment terms
- ☐ Deliver security awareness and role-specific training on a recurring basis
- ☐ Apply a disciplinary process for security policy violations
- ☐ Manage access and asset return at termination or change of role

E Physical & Technological Controls (Annex A.7 & A.8)

- ☐ Secure physical access to offices, data centres, and equipment
- ☐ Maintain endpoint protection and secure configuration baselines
- ☐ Enforce access control and authentication aligned to least privilege
- ☐ Apply encryption for data in transit and at rest where required
- ☐ Maintain logging, monitoring, and vulnerability management processes

F Internal Audit

- ☐ Maintain an internal audit programme covering all ISMS clauses and controls
- ☐ Assign auditors who are independent of the area being audited
- ☐ Raise nonconformities with objective evidence and clear descriptions
- ☐ Track corrective actions arising from audit findings to closure

G Management Review

- ☐ Hold management review at planned intervals with a defined agenda
- ☐ Review audit results, risk treatment status, and incident trends
- ☐ Review the continuing suitability of the information security policy
- ☐ Record decisions on resourcing, changes, and improvement opportunities

H Continual Improvement & Certification Readiness

- ☐ Track nonconformities and corrective actions to root-cause closure
- ☐ Reassess residual risk after treatment actions are implemented
- ☐ Confirm evidence trails exist for every control in the Statement of Applicability
- ☐ Conduct a pre-certification readiness review ahead of stage 1 audit