



CERTCROWD

ISO/IEC 27001:2022

Self-Assessment Checklist



This checklist is a practical way to test your readiness for ISO 27001:2022 certification. It covers the management system requirements (Clauses 4–10) and the updated Annex A controls.

PARTIES

Clause 4 — Context of the Organisation

-  **Understanding your environment (4.1):**
Have you identified the external (laws, regulations, market pressures) and internal (culture, structure, processes) factors that affect information security?
- *Evidence:* SWOT analysis, compliance register, business context analysis.
-  **Understanding stakeholders (4.2):**
Do you know which “interested parties” (customers, regulators, suppliers, staff) expect specific security measures from you?
- *Evidence:* Stakeholder list, requirements register.
-  **Defining scope (4.3):**
Have you clearly documented what parts of your organisation, processes, and systems are included in your ISMS?
- *Evidence:* Scope statement, system boundary diagrams.
-  **Establishing the ISMS (4.4):**
Is your ISMS documented and actively maintained?
- *Evidence:* ISMS manual, policy framework, continual improvement log.

Clause 5 — Leadership

-  **Commitment from the top (5.1):**
Is senior management visibly supporting and funding the ISMS?
- *Evidence:* Meeting minutes, resource allocation, security initiatives signed off by executives.
-  **Policy (5.2):**
Do you have a high-level Information Security Policy that is communicated to all staff and stakeholders?
- *Evidence:* Policy document, onboarding packs, intranet posts.
-  **Roles & responsibilities (5.3):**
Are information security roles and authorities clearly defined, assigned, and communicated?
- *Evidence:* RACI charts, job descriptions, org charts with security roles.



Clause 6 — Planning

Risk management (6.1):



Do you have a repeatable risk assessment and risk treatment methodology, and do you update it when things change?

- *Evidence:* Risk register, risk treatment plans, methodology document.

Objectives (6.2):



Do you set measurable information security objectives that align with business needs (e.g., reduce phishing incidents, meet compliance deadlines)?

- *Evidence:* Objectives dashboard, KPI reports, tracking tools.

Change planning (6.3):



When making organisational changes (new systems, mergers, process redesigns), do you consider security impacts?

- *Evidence:* Change management logs, risk assessments attached to projects.

Clause 7 — Support

Resources (7.1):



Are enough people, tools, and budget allocated for the ISMS?

- *Evidence:* Budget allocations, staff headcount, training schedules.

Competence (7.2):



Do you ensure staff have the right skills, training, and qualifications for their security responsibilities?

- *Evidence:* Training records, certifications, skill gap analyses.

Awareness (7.3):



Do employees understand the security policy, objectives, and consequences of not following them?

- *Evidence:* Awareness campaigns, phishing simulations, training feedback.

Communication (7.4):



Are there clear channels to communicate ISMS matters internally and externally?

- *Evidence:* Communication plans, email templates, incident notification procedures.

Documented information (7.5):



Are policies, procedures, and records properly controlled (approved, updated, accessible)?

- *Evidence:* Document control system, version history, approval logs.



Clause 8 — Operation



Operational planning (8.1):

Are ISMS processes defined, implemented, and managed effectively?

- *Evidence:* Process maps, SOPs, workflow tools.



Risk assessments (8.2):

Are risk assessments carried out regularly and when changes occur?

- *Evidence:* Updated risk register, audit trail of assessments.



Risk treatment (8.3):

Do you implement and monitor controls that address identified risks?

- *Evidence:* Control matrix, evidence of monitoring, treatment plan status reports.

Clause 9 — Performance Evaluation



Monitoring & measurement (9.1):

Are you tracking how well your ISMS is performing?

- *Evidence:* Security KPIs, incident stats, dashboard reports.



Internal audits (9.2):

Do you run audits against the ISMS and record findings?

- *Evidence:* Audit schedule, audit reports, follow-up actions.



Management reviews (9.3):

Does senior leadership review ISMS results and decide on improvements?

- *Evidence:* Management review agendas, minutes, outcomes.

Clause 10 — Improvement



Corrective actions (10.1):

Do you record incidents, investigate root causes, and take corrective action?

- *Evidence:* Incident reports, corrective action logs, lessons learned.



Continual improvement (10.2):

Do you track and implement opportunities for ongoing ISMS improvement?

- *Evidence:* Improvement register, performance reviews, security roadmap.



Annex A — Information Security Controls (Themes)

The 2022 revision reduces Annex A to **93 controls** across four categories.

A.5 Organisational Controls (37)

Focus: policies, governance, supplier management, incident response, business continuity.

Examples:

- ☐ Documented security policies (policies for acceptable use, classification, transfer).
- ☐ Threat intelligence and incident learning.
- ☐ Supplier and cloud service security management.
- ☐ Business continuity and ICT readiness.
- ☐ Legal and regulatory compliance (IP, records, PII).

A.6 People Controls (8)

Focus: HR and people security.

Examples:

- ☐ Screening before employment.
- ☐ Training and awareness programs.
- ☐ Confidentiality agreements.
- ☐ Responsibilities during and after employment.
- ☐ Remote working and teleworking guidelines.

A.7 Physical Controls (14)

Focus: secure facilities and physical protections.

Examples:

- ☐ Security perimeters and entry controls.
- ☐ Protection against fire, flood, and other physical risks.
- ☐ Equipment security and secure disposal.
- ☐ Clear desk / clear screen practices.
- ☐ Security monitoring in facilities.



A.8 Technological Controls (34)

Focus: access management, technical protections, secure development.

Examples:

- ☐ Identity and access management (MFA, privileged accounts).
- ☐ Backup, logging, and monitoring.
- ☐ Malware protection and vulnerability management.
- ☐ Cryptographic controls and key management.
- ☐ Secure development, coding, testing, and outsourced development.

