

ISO/IEC 27001 gap analysis checklist

ISO/IEC 27001:2022 – Information security management systems (clauses 4–10 and Annex A themes)

For each requirement, record whether your organisation conforms, partly conforms or has a gap, and note the evidence (documents, records, interviews) that supports your answer. To score the results, track corrective actions and produce a report automatically, use the free online Gap Assessment at paperwingpdf.com/iso-gap-assessment/ – it runs in your browser and nothing is uploaded.

Organisation: _____ Assessed by: _____ Date: _____

4.1 Context — ISMS context (internal & external issues)

Identify and document internal issues (governance, risk appetite, contractual commitments, current security posture, IT architecture, culture) and external issues (regulatory landscape, threat intelligence, industry sector risks, geopolitical factors, supply chain characteristics) relevant to the ISMS. Review when significant change occurs. Maintain a documented context register and link findings to clause 6.1 risk assessment.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

4.2 Context — Interested parties & requirements

Identify interested parties relevant to the ISMS (regulators, customers, business partners, insurers, employees, shareholders, law enforcement). Document their information security requirements (contractual SLAs, regulatory mandates, NDA obligations, sector-specific standards). Determine which requirements will be included in the ISMS and which will be addressed through controls. Review annually and when significant new relationships are established.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

4.3 Context — ISMS scope

Define the ISMS scope in documented form — specifying the information assets, processes, organisational units, physical locations, and technology platforms included. Justify any exclusions from ISO/IEC 27001 requirements. The scope must be available as documented information. Ensure the scope is realistic and defensible: excludes must not undermine the effectiveness of controls included in the SoA. Align scope with the risk assessment boundaries.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

4.4 Context — ISMS establishment & continual improvement

Establish, implement, maintain, and continually improve the ISMS in accordance with the requirements of ISO/IEC 27001:2022. Demonstrate that the ISMS is a managed system (not just a document set) through evidence of active risk management, control operation, monitoring, audit, management review, and improvement activities. Maintain an ISMS manual or framework document linking all ISMS elements.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

5.1 Leadership — Information security commitment

Top management must demonstrate leadership: approve the information security policy, ensure ISMS objectives are established, ensure integration of ISMS into business processes, ensure adequate resources, communicate the importance of information security, ensure the ISMS achieves intended outcomes, direct people to contribute, promote continual improvement, and support other relevant management roles. Auditors look for direct executive involvement — not just delegation to IT or security teams.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

5.2 Leadership — Information security policy

Establish an information security policy appropriate to the organisation's purpose, providing a framework for setting information security objectives, including a commitment to satisfying applicable requirements, and including a commitment to continual improvement. The policy must be available as documented information, communicated within the organisation, and available to interested parties as appropriate. Review after significant organisational or threat-landscape changes.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

5.3 Leadership — Roles, responsibilities & authorities

Assign and communicate information security responsibilities. Specifically: assign responsibility for ensuring ISMS conforms to ISO 27001 requirements, and for reporting ISMS performance to top management. Document the ISMS organisational chart, RACI matrix, and job descriptions incorporating information security responsibilities. Define the information security function's authority relative to IT operations, risk management, compliance, and legal.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

6.1 Planning — Information security risk assessment process

Define and apply a documented information security risk assessment process. The process must: establish risk acceptance criteria; identify risks associated with loss of confidentiality, integrity, and availability of information assets within ISMS scope; assign asset owners; analyse risks (consequences, likelihood, risk level); evaluate risks against acceptance criteria. Use a consistent, repeatable, and comparable methodology (e.g. ISO 27005, FAIR, qualitative matrix). Retain documented risk assessment results.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

6.1.3 Planning — Risk treatment & Statement of Applicability (SoA)

Select appropriate risk treatment options (modify, retain, avoid, share). For the 'modify' option, select controls from Annex A (93 controls across 4 themes: Organisational, People, Physical, Technological) and other sources as needed. Produce a Statement of Applicability (SoA) that lists all Annex A controls, states whether each is included or excluded, and provides justification. Where controls are excluded, document that no unacceptable residual risks exist. Develop a risk treatment plan and obtain asset owner approval of residual risks.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

6.2 Planning — Information security objectives

Establish information security objectives consistent with the information security policy. Objectives must be measurable, take into account applicable requirements (legal, contractual, risk-based), be monitored, communicated, and updated as appropriate. For each objective document what will be done, resources required, responsibility, timeline, and how results will be evaluated. Link objectives to the risk treatment plan and ISMS performance metrics.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

6.3 Planning — Planning of changes

When changes to the ISMS are required, carry them out in a planned manner, considering the purpose and potential consequences of changes, integrity of the ISMS, availability of resources, and allocation of responsibilities. Maintain a change management process for ISMS changes (policy updates, scope changes, control changes, technology changes). Retain records of ISMS change decisions and approvals.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

7.1 Support — Resources

Determine and provide resources needed to establish, implement, maintain, and continually improve the ISMS — including personnel (internal or outsourced), tools and technology, budget, and time. Document resource allocation decisions linked to risk treatment plan and ISMS objectives. Demonstrate that information security has adequate budget and headcount relative to the organisation's risk profile. Review resource adequacy at management review.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

7.2 Support — Competence

Determine required competence for persons performing ISMS-relevant work (risk assessors, auditors, security operations, privacy officers, developers, system administrators). Ensure competence through appropriate education, training, experience, or qualifications (e.g. CISSP, CISM, ISO 27001 Lead Implementer/Auditor). Evaluate effectiveness of training actions. Retain a competency matrix and training records as documented evidence.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

7.3 Support — Awareness

Ensure all persons under the organisation's control are aware of the information security policy, their contribution to ISMS effectiveness, the implications of non-compliance, and their role in incident reporting. Implement an annual security awareness programme covering: phishing, social engineering, password hygiene, data classification, incident reporting, acceptable use. Retain training completion records.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

7.4 Support — Communication

Determine what to communicate regarding information security, when, to whom, how, and by whom. Establish communication channels for: management reporting on ISMS performance, customer security queries, regulatory notifications, incident communications, and third-party security obligations. Maintain a communication plan and retain records of significant ISMS communications.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

7.5 Support — Documented information

Create and maintain all documented information required by ISO 27001 (including the SoA, risk assessment, risk treatment plan, policies, procedures, and records of monitoring). Control documented information: version control, approval, distribution, access, protection, retention, and disposal. Distinguish between controlled documents (policies, procedures) and records (evidence of ISMS activities). Retain records for at least the period specified by compliance obligations or a defined retention schedule.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

8.1 Operation — Operational planning & control

Plan, implement, control, and maintain ISMS processes needed to meet requirements and implement risk treatment actions. Establish and document operational security procedures (change management, access management, incident response, backup, patch management, etc.). Ensure outsourced processes are controlled. Control planned changes and review unintended changes to prevent or mitigate adverse effects. Retain documented evidence that processes have been carried out as planned.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

8.2 Operation — Information security risk assessments

Perform information security risk assessments at planned intervals (at least annually) or when significant changes occur (new systems, new threat intelligence, scope changes, major incidents). Each assessment must use the defined risk assessment methodology and asset inventory. Retain documented results of each assessment. Track how risk ratings change over time. Ensure asset owners review and accept residual risks.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

8.3 Operation — Information security risk treatment

Implement the risk treatment plan. Track the status of each treatment action. Retain documented evidence that controls are implemented and operating as intended. Where treatment actions are delayed, document the rationale and interim controls. Re-assess residual risk after treatment is implemented. Ensure the SoA remains current and reflects actual control implementation status.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

9.1 Performance — Monitoring, measurement, analysis & evaluation

Determine what to monitor and measure (controls, processes, ISMS objectives, risk landscape), the methods used, when to perform monitoring/measurement, when to analyse/evaluate results, and who is responsible. Define and track information security KPIs and KRIs (key risk indicators). Retain documented results as evidence of performance. Report security performance metrics to management on a defined schedule (at minimum quarterly).

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

9.2 Performance — Internal audit

Plan and conduct internal ISMS audits at planned intervals. Establish an audit programme covering scope, methods, frequency, responsibilities, and reporting. Ensure auditors are independent and competent (cannot audit own work). Audit criteria: ISO 27001 requirements + organisation's own ISMS requirements. Report findings to management. Track and close audit nonconformities. Retain audit programme records and audit reports as documented information.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

9.3 Performance — Management review

Top management must review the ISMS at planned intervals (at minimum annually). Review inputs must include: status of actions from previous reviews, changes in external/internal issues, ISMS performance data (monitoring results, KPIs, audit results, risk treatment status, nonconformities), feedback from interested parties, risk assessment results, improvement opportunities. Outputs: decisions on improvement opportunities, ISMS changes needed, resource requirements. Retain management review minutes as documented information.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

10.1 Improvement — Continual improvement

Continually improve the suitability, adequacy, and effectiveness of the ISMS. Use audit results, management review outputs, monitoring data, incident analysis, and threat intelligence to identify improvement opportunities. Maintain an improvement register and demonstrate year-on-year measurable improvement in ISMS maturity and security performance indicators.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

10.2 Improvement — Nonconformity & corrective action

When a nonconformity occurs (audit finding, incident, failed control, regulatory breach): react, contain, and correct it; evaluate the root cause; implement corrective action; review effectiveness; update risk assessment if needed; make ISMS changes if required. Retain documented information: nature of nonconformity, actions taken, results of corrective action. Track corrective actions through to verified closure.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

A.5 Annex A Theme 1 — Organisational controls (37 controls)

Implement organisational controls including: information security policies (A.5.1), roles and responsibilities (A.5.2), segregation of duties (A.5.3), management responsibilities (A.5.4), contact with authorities (A.5.5), contact with special interest groups (A.5.6), threat intelligence (A.5.7), information security in project management (A.5.8), inventory of information and associated assets (A.5.9), acceptable use (A.5.10), return of assets (A.5.11), data classification (A.5.12–A.5.14), access control policy (A.5.15), identity management (A.5.16), authentication (A.5.17), access rights (A.5.18), supplier security (A.5.19–A.5.23), incident management (A.5.24–A.5.28), business continuity (A.5.29–A.5.30), legal/regulatory compliance (A.5.31–A.5.36), privacy (A.5.34), and intellectual property (A.5.32). For each included control retain documented implementation evidence.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

A.6 Annex A Theme 2 — People controls (8 controls)

Implement people controls covering: screening (A.6.1), terms and conditions of employment (A.6.2), information security awareness, education and training (A.6.3), disciplinary process (A.6.4), responsibilities after termination or change of employment (A.6.5), confidentiality or non-disclosure agreements (A.6.6), remote working (A.6.7), and information security event reporting (A.6.8). Retain records of screening, training completion, signed NDAs, and remote working agreements.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

A.7 Annex A Theme 3 — Physical controls (14 controls)

Implement physical security controls: physical security perimeters (A.7.1), physical entry (A.7.2), securing offices, rooms, facilities (A.7.3), physical security monitoring (A.7.4), protection against physical and environmental threats (A.7.5), working in secure areas (A.7.6), clear desk and clear screen (A.7.7), equipment siting and protection (A.7.8), security of assets off-premises (A.7.9), storage media (A.7.10), supporting utilities (A.7.11), cabling security (A.7.12), equipment maintenance (A.7.13), and secure disposal or re-use of equipment (A.7.14). Retain physical access logs, visitor records, and equipment disposal certificates.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____

A.8 Annex A Theme 4 — Technological controls (34 controls)

Implement technological controls covering: user endpoint devices (A.8.1), privileged access rights (A.8.2), information access restriction (A.8.3), access to source code (A.8.4), secure authentication (A.8.5), capacity management (A.8.6), protection against malware (A.8.7), management of technical vulnerabilities (A.8.8), configuration management (A.8.9), information deletion (A.8.10), data masking (A.8.11), data leakage prevention (A.8.12), information backup (A.8.13), redundancy of information processing facilities (A.8.14), logging (A.8.15–A.8.16), clock synchronisation (A.8.17), use of privileged utility programs (A.8.18), installation of software on operational systems (A.8.19), network security (A.8.20–A.8.22), web filtering (A.8.23), cryptography (A.8.24), secure development (A.8.25–A.8.32), and security testing (A.8.33–A.8.34). Retain vulnerability scan results, penetration test reports, patch management records, and SIEM/log evidence.

☐ Conforms ☐ Partly ☐ Gap ☐ Not applicable

Evidence / notes: _____