ISO 27001 Certification Readiness Checklist

This high-level, non-exhaustive checklist helps organisations do an initial sense-check of their readiness for ISO27001 certification. It is not a full compliance assessment, audit tool, or legal advice, and it does not cover all ISO 27001 requirements.

Use this as a starting point to identify potential gaps. For a more detailed review or formal audit preparation, you should seek professional advice or conduct a comprehensive ISO27001 assessment.

1. Context of the Organisation (Clause 4)

☐ Internal and external issues relevant to information security are identified and documented (e.g. regulatory, technological, business, threat landscape).

☐ Interested parties (e.g. customers, regulators, partners, suppliers) and their information security requirements are identified and documented.

☐ The scope of the ISMS is clearly defined, including locations, processes, systems, and exclusions with justification.

☐ Dependencies and interfaces with external parties (e.g. cloud providers, MSPs, partners) are documented.

☐ Information security roles within the scope (business units, IT, vendors) are understood and mapped.

2. Leadership & Governance (Clause 5)

☐ An Information Security Policy is documented, approved by top management, communicated, and available to relevant parties.

☐ The policy includes high-level objectives, commitment to continual improvement, and alignment with business and legal requirements.

☐ Top management demonstrates leadership and commitment (e.g. through meeting minutes, resource allocation, communications).

☐ Information security roles, responsibilities, and authorities are clearly defined and formally assigned (e.g. ISMS owner, risk owner, control owner).

☐ Information security is integrated into organisational processes (e.g. project management, procurement, HR).

3. Planning & Risk Management (Clause 6)

☐ Risks and opportunities related to the ISMS are identified and addressed (beyond only technical risks).

☐ A documented information security risk assessment methodology exists (criteria, likelihood, impact, risk evaluation).

☐ A current information security risk assessment has been performed and recorded (risk register).

☐ Risk owners are assigned for identified risks.

☐ A risk treatment plan exists, linking risks to selected controls (including Annex A controls).

☐ Information security objectives are documented, measurable, and aligned with business goals and policy.

☐ Plans are in place to achieve information security objectives (responsibilities, timelines, resources).

4. Support & Resources (Clause 7)

☐ Resources necessary for the establishment, implementation, maintenance, and continual improvement of the ISMS are identified and provided.

☐ Competence requirements for information security-related roles are defined and documented.

☐ Evidence exists that people performing information security tasks are competent (training, experience, certifications).

☐ Information security awareness activities are in place and conducted regularly for all staff.

☐ Internal and external communications relevant to information security are defined (what, when, with whom, how).

☐ A documented information management process exists (creation, approval, version control, access, retention, disposal).

☐ Controlled documents (e.g. policies, procedures, standards) are versioned, approved, and accessible.

☐ Records (evidence) are controlled and retrievable (e.g. logs, meeting minutes, audit reports).

5. Operation (Clause 8)

☐ Operational planning and control are documented for key processes within the ISMS scope.

☐ Information security risk assessments are performed at planned intervals and when significant changes occur.

☐ Information security risk treatment is implemented as per the risk treatment plan.

☐ Change management procedures include information security impact assessment for system and process changes.

☐ Documented procedures exist for incident management, access control, backup, and vendor management.

☐ Security requirements are defined and embedded into procurement and supplier contracts where relevant.

☐ Outsourced processes and services are monitored for information security performance.

6. Performance Evaluation (Clause 9)

☐ Information security monitoring and measurement activities are defined (what is measured, methods, frequency, responsibilities).

☐ Key performance indicators (KPIs) or metrics are in place for the ISMS (e.g. incidents, training completion, vulnerabilities).

☐ Evidence exists of regular review and analysis of ISMS performance data.

☐ Internal audit programme for the ISMS is established with scope, criteria, frequency, and methods.

☐ Internal ISMS audits are conducted and records of findings and follow-up actions are maintained.

☐ Management review meetings are held at planned intervals and include required inputs (e.g. audit results, KPIs, risks, opportunities).

☐ Outputs of management reviews are documented (decisions, actions, resource needs, improvements).

7. Improvement (Clause 10)

☐ A formal process exists for handling nonconformities related to the ISMS (identification, evaluation, root cause analysis).

☐ Corrective actions are defined, implemented, and their effectiveness reviewed.

☐ Opportunities for continual improvement of the ISMS are identified and tracked.

☐ Lessons learned from incidents, audits, and reviews are captured and used to improve controls and processes.

8. Annex A Control Readiness (High-Level)

The following checklist provides a high-level view of readiness against Annex A control themes in ISO/IEC 27001:2022. It is recommended to map these to your detailed Statement of Applicability (SoA).

8.1 Information Security Policies (Annex A.5)

☐ Information security policies are documented, approved, and communicated.

☐ Policies are reviewed at planned intervals or when significant changes occur.

8.2 Organisation of Information Security & Roles (Annex A.6)

☐ Information security responsibilities are allocated across the organisation.

☐ Segregation of duties is considered for critical activities.

☐ Use of cloud services is governed by documented policies and criteria.

☐ Information security is addressed in project management practices.

8.3 Human Resource Security (Annex A.7)

☐ Background verification checks are conducted according to laws and risk level.

☐ Confidentiality and acceptable use requirements are included in employment terms.

☐ Information security responsibilities are communicated during onboarding.

☐ Offboarding process includes revocation of access and recovery of assets.

8.4 Asset Management (Annex A.8)

☐ Information assets and supporting assets (hardware, software, services) are inventoried and classified.

☐ Ownership is assigned for key information assets.

☐ Acceptable use rules for assets (e.g. devices, email, internet) are documented.

☐ Procedures exist for handling assets at end-of-life (secure disposal, data wiping).

8.5 Access Control (Annex A.9)

☐ Access control policy and principles (need-to-know, least privilege) are defined.

☐ User access provisioning and de-provisioning processes are documented and followed.

☐ Privileged access is tightly controlled, monitored, and regularly reviewed.

☐ Authentication mechanisms (passwords, MFA) are implemented according to policy.

☐ Periodic access reviews are conducted for key systems and applications.

8.6 Cryptography (Annex A.10)

☐ Cryptographic controls are used according to a documented cryptography policy.

☐ Key management procedures (generation, storage, rotation, revocation) are implemented.

☐ Use of encryption for data at rest and in transit is defined based on risk.

8.7 Physical & Environmental Security (Annex A.11)

☐ Physical security perimeters and access controls are defined for offices and server rooms.

☐ Visitor access is controlled and recorded where appropriate.

☐ Environmental controls protect against fire, water, temperature, and power issues.

☐ Secure areas and equipment are protected against unauthorised access and damage.

8.8 Operations Security (Annex A.12)

☐ Operational procedures are documented and maintained for key systems.

☐ Capacity and performance of systems are monitored and managed.

☐ Malware protection is deployed, updated, and monitored.

☐ Backup processes are defined, tested, and aligned with recovery objectives.

☐ Logging and monitoring are implemented for critical systems and security events.

☐ Time synchronisation is implemented for logs and systems.

8.9 Communications Security (Annex A.13)

☐ Network security controls are in place to protect data in transit.

☐ Segregation of networks (e.g. internal, external, guest) is implemented where appropriate.

☐ Information transfer policies and procedures are documented (including secure email and file sharing).

8.10 System Acquisition, Development & Maintenance (Annex A.14)

☐ Information security requirements are defined and included in new system and application projects.

☐ Secure development practices are followed (coding standards, testing, code review).

☐ Security testing (e.g. vulnerability assessment, penetration testing) is performed for key systems.

☐ Changes are subject to change management controls, including security impact assessment.

8.11 Supplier Relationships (Annex A.15)

☐ Information security requirements are defined for suppliers and service providers.

☐ Contracts include relevant information security clauses.

☐ Supplier performance and compliance with security requirements are periodically reviewed.

☐ Risks related to third-party and cloud services are assessed and managed.

8.12 Information Security Incident Management (Annex A.16)

☐ A documented incident management process exists, including detection, reporting, triage, response, and learning.

☐ Staff know how to report suspected incidents.

☐ Incident logs and records are maintained.

☐ Post-incident reviews are conducted to capture lessons learned.

8.13 Business Continuity & Information Security (Annex A.17)

☐ Business continuity requirements include information security considerations.

☐ Business continuity plans (BCP) and disaster recovery plans (DRP) exist and are documented.

☐ BCP/DRP are tested at planned intervals and updated based on test results.

☐ Recovery objectives (RTO/RPO) are defined and aligned with business needs.

8.14 Compliance & Legal (Annex A.18)

☐ Applicable legal, regulatory, and contractual requirements relating to information security are identified and documented.

☐ Compliance with these requirements is reviewed on a periodic basis.

☐ Intellectual property, data protection, and privacy obligations are addressed in policies and procedures.

☐ Records of compliance reviews, audits, and assessments are maintained.

For assistance, contact:

Hari Krishnan, Managing Director
Apex Organisational Solutions | www.apexorganisationalsolutions.com |
hari.krishnan@apexorganisationalsolutions.com