ISO/IEC 27001:2022 Audit Checklist

Information Security Management Systems - Downloadable Website Resource

This ISO/IEC 27001:2022 audit checklist helps organizations review the readiness of their Information Security Management System (ISMS). It supports internal reviews, pre-certification preparation, evidence collection, Annex A control evaluation, and follow-up action planning.

How to Use This Checklist

- Review each requirement and record objective evidence such as ISMS policies, risk assessments, Statement of Applicability, control records, interviews, system screenshots, logs, incident records, and management review outputs.
- Use the status column to indicate Conforming, Partially Conforming, Nonconforming, or Not Applicable based on evidence reviewed.
- Record gaps, information security risks, missing controls, corrective actions, responsible persons, and target dates in the notes column.
- This resource is for educational and preparation purposes. Certification decisions must be based on an independent certification assessment process.

Organization and Assessment Details

Organization Name		**Assessment Date**	
Location / Site		**ISMS Scope**	
Reviewer / Team		**Department / Process**	
Cloud / IT Environment		**Applicable Legal / Contractual Requirements Reviewed**	Yes / No

Checklist Rating Guide

Rating	Meaning	Typical Evidence
C	Conforming - requirement is implemented and supported by adequate evidence.	Approved ISMS documentation, risk records, control evidence, logs, interviews, test results, review outputs.
PC	Partially Conforming - requirement is partly implemented but incomplete or inconsistently applied.	Draft documents, inconsistent control operation, missing retention records, weak awareness, incomplete SoA justification.
NC	Nonconforming - requirement is not implemented or evidence is missing.	No defined process, absent risk treatment plan, missing incident records, unmanaged access, no review evidence.
NA	Not Applicable - requirement or control is not applicable, with clear justification.	Documented applicability rationale, scope boundaries, risk acceptance, Statement of Applicability notes.

The checklist below follows the ISO/IEC 27001:2022 management system clause structure and includes a practical Annex A control review section. The questions are intentionally written as review prompts and should be adapted to the organization's ISMS scope, assets, technologies, outsourced processes, cloud services, legal obligations, customer requirements, and risk profile.

Clause 4 - Context of the Organization

Clause	Audit Question	Evidence to Review	Status C/PC/NC/NA	Notes / Gaps / Actions
4.1	Has the organization determined internal and external issues relevant to information security and the ISMS?	Context analysis, business objectives, threat landscape review, regulatory environment, technology and supplier context.		
4.2	Have interested parties and their information security requirements been identified?	Interested party register, customer contracts, regulatory requirements, supplier requirements, stakeholder needs.		
4.3	Is the ISMS scope defined with boundaries, interfaces, locations, technologies, and exclusions?	ISMS scope statement, network and process boundaries, site list, cloud/service boundaries, scope approval.		
4.4	Has the ISMS been established, implemented, maintained, and continually improved?	ISMS process map, policy framework, risk methodology, procedures, performance review records.		

Clause 5 - Leadership

Clause	Audit Question	Evidence to Review	Status C/PC/NC/NA	Notes / Gaps / Actions
5.1	Does top management demonstrate leadership, accountability, and commitment for the ISMS?	Leadership communications, resourcing decisions, ISMS objectives, management review, security governance records.		
5.2	Is the information security policy appropriate, approved, communicated, and available where needed?	Information security policy, approval record, communication records, intranet publication, employee acknowledgement.		
5.3	Are information security roles, responsibilities, and authorities assigned and communicated?	Responsibility matrix, job descriptions, ISMS committee records, CISO/security owner appointment, escalation matrix.		

Clause 6 - Planning

Clause	Audit Question	Evidence to Review	Status C/PC/NC/NA	Notes / Gaps / Actions
6.1.1	Has the organization planned actions to address ISMS risks and opportunities?	Risk and opportunity register, action plans, governance review records.		
6.1.2	Is there a defined information security risk assessment process with consistent criteria?	Risk assessment methodology, impact/likelihood criteria, risk acceptance criteria, risk register.		
6.1.2	Are information security risks identified, analyzed, evaluated, and reviewed at planned intervals?	Asset/risk register, threat and vulnerability review, risk evaluation results, review approvals.		
6.1.3	Is there a risk treatment process with selected controls and documented justification?	Risk treatment plan, control selection rationale, risk owner approvals, residual risk acceptance.		
6.1.3	Has a Statement of Applicability been prepared and maintained?	Statement of Applicability, Annex A applicability decisions, control implementation status, exclusion justifications.		
6.2	Are measurable information security objectives established and monitored?	ISMS objectives, KPIs, action plans, responsibility assignments, progress reviews.		
6.3	Are ISMS changes planned and controlled?	Change plans, change impact assessments, approvals, implementation review records.		

Clause 7 - Support

Clause	Audit Question	Evidence to Review	Status C/PC/NC/NA	Notes / Gaps / Actions
7.1	Has the organization determined and provided resources needed for the ISMS?	Budget, tools, staffing, monitoring systems, security awareness platforms, external support records.		
7.2	Are personnel competent for information security responsibilities?	Competency matrix, training records, role-based security training, qualification/experience records.		
7.3	Are personnel aware of policies, responsibilities, risks, and consequences of nonconformance?	Awareness campaigns, induction records, phishing simulations, interviews, acknowledgement records.		
7.4	Are internal and external ISMS communications defined and controlled?	Communication matrix, escalation procedure, customer/regulator communication process, incident notification rules.		
7.5	Is documented information controlled, maintained, retained, protected, and available?	Document control procedure, master list, access permissions, retention schedule, version control evidence.		

Clause 8 - Operation

Clause	Audit Question	Evidence to Review	Status C/PC/NC/NA	Notes / Gaps / Actions
8.1	Are ISMS operational processes planned, implemented, and controlled?	Operational procedures, control operation records, service management records, monitoring dashboards.		
8.1	Are outsourced processes and externally provided services controlled within the ISMS scope?	Supplier contracts, security clauses, SLA reviews, vendor risk assessments, cloud service reviews.		
8.2	Are information security risk assessments performed at planned intervals and when changes occur?	Periodic risk assessment reports, change-triggered risk reviews, updated risk register.		
8.3	Is the risk treatment plan implemented and monitored for progress and effectiveness?	Treatment action plans, implementation records, control testing, residual risk reviews.		

Clause 9 - Performance Evaluation

Clause	Audit Question	Evidence to Review	Status C/PC/NC/NA	Notes / Gaps / Actions
9.1	Does the organization monitor, measure, analyze, and evaluate ISMS performance?	Metrics/KPIs, monitoring reports, log review results, vulnerability trends, incident trends.		
9.1	Are monitoring and measurement methods defined and appropriate?	Monitoring plan, KPI definitions, measurement frequency, data sources, dashboard configuration.		
9.2	Are internal ISMS assessments conducted at planned intervals by competent and impartial reviewers?	Internal assessment program, checklist, reports, reviewer competence, findings and action tracking.		
9.2	Does the internal assessment program consider scope, risk, changes, and previous results?	Risk-based schedule, process coverage plan, previous finding trend review.		
9.3	Does top management review the ISMS for suitability, adequacy, effectiveness, and alignment?	Management review agenda, inputs and outputs, decisions, actions, resource decisions.		

Clause 10 - Improvement

Clause	Audit Question	Evidence to Review	Status C/PC/NC/NA	Notes / Gaps / Actions
10.1	Does the organization identify improvement opportunities for the ISMS?	Improvement register, control enhancement plans, lessons learned, risk reduction initiatives.		
10.2	Are nonconformities and corrective actions managed effectively?	NC records, root cause analysis, corrective action plans, effectiveness verification.		
10.2	Are information security incidents, weaknesses, and recurring issues used as improvement inputs?	Incident reports, lessons learned, trend analysis, updated controls, updated risk treatment plans.		
10.3	Is the ISMS continually improved based on performance, risks, assessments, and management review?	Improvement projects, objective results, updated policies/procedures, control maturity improvements.		

Annex A - Organizational Controls

Clause	Audit Question	Evidence to Review	Status C/PC/NC/NA	Notes / Gaps / Actions
A.5	Are policies, responsibilities, segregation of duties, and contact with authorities/special interest groups defined where relevant?	Policy set, roles matrix, segregation review, authority contact list, industry group participation records.		
A.5	Are threat intelligence, information security in project management, asset inventory, acceptable use, and return of assets controlled?	Threat feeds, project security reviews, asset inventory, acceptable use acknowledgement, exit checklist.		
A.5	Are classification, labeling, information transfer, access control rules, identity management, authentication, and supplier security addressed?	Classification scheme, transfer procedure, access control policy, user lifecycle records, supplier assessments.		
A.5	Are cloud services, ICT supply chain, incident management, business continuity, legal requirements, privacy, records, and independent review addressed?	Cloud reviews, supplier clauses, incident procedure, continuity tests, legal register, privacy records, review reports.		

Annex A - People Controls

Clause	Audit Question	Evidence to Review	Status C/PC/NC/NA	Notes / Gaps / Actions
A.6	Are screening, employment terms, security awareness, disciplinary processes, and confidentiality obligations managed?	Screening records where applicable, contracts, training records, disciplinary procedure, NDAs.		
A.6	Are remote working, teleworking, and reporting of security events or weaknesses controlled?	Remote work policy, VPN/MFA evidence, endpoint controls, event reporting channels, awareness records.		

Annex A - Physical Controls

Clause	Audit Question	Evidence to Review	Status C/PC/NC/NA	Notes / Gaps / Actions
A.7	Are secure areas, entry controls, physical security monitoring, and protection against physical/environmental threats managed?	Access logs, visitor records, CCTV checks, secure room controls, environmental monitoring, maintenance logs.		
A.7	Are equipment siting, media handling, cabling, maintenance, secure disposal, and clear desk/screen practices controlled?	Equipment records, media disposal certificates, cabling maps, maintenance records, clear desk checks.		

Annex A - Technological Controls

Clause	Audit Question	Evidence to Review	Status C/PC/NC/NA	Notes / Gaps / Actions
A.8	Are endpoint devices, privileged access, access restrictions, authentication, capacity, malware, vulnerability, and configuration controls implemented?	MDM/EDR console, admin access review, MFA evidence, capacity reports, patch/vulnerability reports, baselines.		
A.8	Are logging, monitoring, clock synchronization, software installation, network security, web filtering, cryptography, and secure development controlled?	SIEM/logs, NTP settings, software approval, firewall rules, secure coding records, encryption/key management.		
A.8	Are test data, backup, redundancy, technical vulnerability management, audit logging, data leakage prevention, masking, deletion, and cloud controls managed?	Backup tests, DLP rules, deletion records, masking evidence, vulnerability remediation, cloud configuration reviews.		
A.8	Are system acquisition, development, testing, change control, outsourced development, and production environment protection managed?	SDLC records, change tickets, test approvals, release notes, outsourced development controls, environment segregation.		

Gap Summary and Action Plan

No.	Requirement / Control Area	Finding Summary	Risk Level	Responsible Person	Target Date	Closure Evidence
1						
2						
3						
4						
5						
6						
7						
8						

Common ISO/IEC 27001:2022 Evidence Examples

Area	Examples of Objective Evidence
ISMS scope and context	Context analysis, interested parties, ISMS scope, business process map, technology and cloud boundaries.
Risk management	Risk methodology, risk register, risk treatment plan, risk owner approvals, residual risk acceptance.
Statement of Applicability	Applicability decisions, control implementation status, exclusion justification, control owner assignments.
Access control	User lifecycle records, access reviews, MFA evidence, privileged access records, joiner/mover/leaver records.
Operations security	Asset inventory, vulnerability reports, patch records, backups, logging, monitoring, malware protection, configuration baselines.
Supplier and cloud security	Supplier assessments, cloud service reviews, contracts, SLAs, security clauses, performance monitoring.
Incident and continuity	Incident procedure, incident logs, lessons learned, backup tests, continuity exercises, escalation contacts.
Performance evaluation	ISMS KPIs, internal assessment report, nonconformity records, management review minutes, improvement actions.