

ISO 27001 checklist for small teams (2022 version)

Seven steps in the order a small team works them, each item with its ISO/IEC 27001:2022 clause or Annex A reference and the proof to keep. Tick the box when the item is in place and the proof is filed. The last pages list all 93 Annex A controls for your Statement of Applicability.

From AccuSights. This checklist is general information, not legal or audit advice; check each item against the standard and your certification body. Clause and control names follow ISO/IEC 27001:2022.

Step 1: get leadership sign-off and name an owner

	Ref	Item	Proof to keep
☐	5.1	Leadership commitment	Meeting minutes and the approved plan
☐	5.2	Information security policy, approved and communicated	The signed policy and where staff can read it
☐	5.3	Roles and responsibilities: ISMS owner, risk owners, control owners	A role list that matches the org chart
☐	7.1, 7.2	Resources and competence	Training records, certificates or a skills matrix
☐	7.3, 7.4	Awareness and communication	Awareness training record and a communication plan
☐	7.5	Documented information: versioned, approved, stored, retired	A document register with owners and review dates

Step 2: set the ISMS scope

	Ref	Item	Proof to keep
☐	4.1	Context of the organization: internal and external issues	A context statement or issues register
☐	4.2	Interested parties and their requirements	A list with each party's requirements
☐	4.3	Scope statement: products, sites, teams, systems, interfaces, exclusions	The signed scope statement
☐	4.3	Asset inventory for the scope, each asset with an owner	The inventory, current and dated

Step 3: run the risk assessment

	Ref	Item	Proof to keep
☐	6.1.2	Risk assessment method with likelihood, impact and acceptance criteria	The methodology document
☐	6.1.2, 8.2	Risk register with owner, score and date for each risk	The register with its reassessment history
☐	6.1.3, 8.3	Risk treatment plan: controls, owner, due date	The plan and its progress
☐	6.1.3 f	Risk owners accept the plan and the residual risk	Their sign-off
☐	6.2	Measurable security objectives with owners and dates	The objectives and how they are tracked

Step 4: write the Statement of Applicability

	Ref	Item	Proof to keep
[]	6.1.3 d	All 93 Annex A controls listed, including exclusions	The SoA
[]	6.1.3 d	A justification for every inclusion and exclusion	The SoA
[]	6.1.3 d	Implementation status that matches the treatment plan	The SoA and the plan agree
[]	7.5	The SoA has a version, an owner and a review date	Version history

Step 5: implement the Annex A controls you selected

	Ref	Item	Proof to keep
[]	A.5	Organizational controls (37)	See the Annex A list
[]	A.6	People controls (8)	See the Annex A list
[]	A.7	Physical controls (14)	See the Annex A list
[]	A.8	Technological controls (34)	See the Annex A list
[]	Annex A	Evidence noted for every included control	A ticket, export, signed record or tool report per control

Step 6: internal audit and management review

	Ref	Item	Proof to keep
[]	9.1	Monitoring and measurement: what, how often, who reviews	A metrics list and the results
[]	9.2	Internal audit programme and an independent internal audit	The plan, the report and the findings
[]	9.3	Management review with decisions and actions	Minutes and actions
[]	10.2	Nonconformity and corrective action, with root cause	A corrective action log
[]	10.1	Continual improvement recorded	Improvements from audits, incidents and reviews

Step 7: Stage 1 and Stage 2 audits

	Ref	Item	Proof to keep
[]	Certification	Pick a certification body accredited by an IAF member (such as ANAB or UKAS)	Two or three written quotes
[]	Certification	Stage 1: documentation and readiness review	The Stage 1 report
[]	Certification	Fix the Stage 1 findings	Corrective actions, closed
[]	Certification	Stage 2: the ISMS in operation	The Stage 2 report and the certificate
[]	Certification	Plan the three-year cycle: two surveillance audits, then recertification	The audit calendar

Annex A: the 93 controls

Mark each control as applicable or not, with the reason, in your Statement of Applicability. Controls marked "new" were added in the 2022 version.

A.5 Organizational controls (37)

	Ref	Control	2022
☐	A.5.1	Policies for information security	
☐	A.5.2	Information security roles and responsibilities	
☐	A.5.3	Segregation of duties	
☐	A.5.4	Management responsibilities	
☐	A.5.5	Contact with authorities	
☐	A.5.6	Contact with special interest groups	
☐	A.5.7	Threat intelligence	new
☐	A.5.8	Information security in project management	
☐	A.5.9	Inventory of information and other associated assets	
☐	A.5.10	Acceptable use of information and other associated assets	
☐	A.5.11	Return of assets	
☐	A.5.12	Classification of information	
☐	A.5.13	Labelling of information	
☐	A.5.14	Information transfer	
☐	A.5.15	Access control	
☐	A.5.16	Identity management	
☐	A.5.17	Authentication information	
☐	A.5.18	Access rights	
☐	A.5.19	Information security in supplier relationships	
☐	A.5.20	Addressing information security within supplier agreements	
☐	A.5.21	Managing information security in the ICT supply chain	
☐	A.5.22	Monitoring, review and change management of supplier services	
☐	A.5.23	Information security for use of cloud services	new
☐	A.5.24	Information security incident management planning and preparation	
☐	A.5.25	Assessment and decision on information security events	
☐	A.5.26	Response to information security incidents	
☐	A.5.27	Learning from information security incidents	
☐	A.5.28	Collection of evidence	
☐	A.5.29	Information security during disruption	

	Ref	Control	2022
☐	A.5.30	ICT readiness for business continuity	new
☐	A.5.31	Legal, statutory, regulatory and contractual requirements	
☐	A.5.32	Intellectual property rights	
☐	A.5.33	Protection of records	
☐	A.5.34	Privacy and protection of PII	
☐	A.5.35	Independent review of information security	
☐	A.5.36	Compliance with policies, rules and standards for information security	
☐	A.5.37	Documented operating procedures	

A.6 People controls (8)

	Ref	Control	2022
☐	A.6.1	Screening	
☐	A.6.2	Terms and conditions of employment	
☐	A.6.3	Information security awareness, education and training	
☐	A.6.4	Disciplinary process	
☐	A.6.5	Responsibilities after termination or change of employment	
☐	A.6.6	Confidentiality or non-disclosure agreements	
☐	A.6.7	Remote working	
☐	A.6.8	Information security event reporting	

A.7 Physical controls (14)

	Ref	Control	2022
☐	A.7.1	Physical security perimeters	
☐	A.7.2	Physical entry	
☐	A.7.3	Securing offices, rooms and facilities	
☐	A.7.4	Physical security monitoring	new
☐	A.7.5	Protecting against physical and environmental threats	
☐	A.7.6	Working in secure areas	
☐	A.7.7	Clear desk and clear screen	
☐	A.7.8	Equipment siting and protection	
☐	A.7.9	Security of assets off-premises	
☐	A.7.10	Storage media	
☐	A.7.11	Supporting utilities	
☐	A.7.12	Cabling security	

	Ref	Control	2022
☐	A.7.13	Equipment maintenance	
☐	A.7.14	Secure disposal or re-use of equipment	

A.8 Technological controls (34)

	Ref	Control	2022
☐	A.8.1	User endpoint devices	
☐	A.8.2	Privileged access rights	
☐	A.8.3	Information access restriction	
☐	A.8.4	Access to source code	
☐	A.8.5	Secure authentication	
☐	A.8.6	Capacity management	
☐	A.8.7	Protection against malware	
☐	A.8.8	Management of technical vulnerabilities	
☐	A.8.9	Configuration management	new
☐	A.8.10	Information deletion	new
☐	A.8.11	Data masking	new
☐	A.8.12	Data leakage prevention	new
☐	A.8.13	Information backup	
☐	A.8.14	Redundancy of information processing facilities	
☐	A.8.15	Logging	
☐	A.8.16	Monitoring activities	new
☐	A.8.17	Clock synchronization	
☐	A.8.18	Use of privileged utility programs	
☐	A.8.19	Installation of software on operational systems	
☐	A.8.20	Networks security	
☐	A.8.21	Security of network services	
☐	A.8.22	Segregation of networks	
☐	A.8.23	Web filtering	new
☐	A.8.24	Use of cryptography	
☐	A.8.25	Secure development life cycle	
☐	A.8.26	Application security requirements	
☐	A.8.27	Secure system architecture and engineering principles	
☐	A.8.28	Secure coding	new
☐	A.8.29	Security testing in development and acceptance	

	Ref	Control	2022
☐	A.8.30	Outsourced development	
☐	A.8.31	Separation of development, test and production environments	
☐	A.8.32	Change management	
☐	A.8.33	Test information	
☐	A.8.34	Protection of information systems during audit testing	