AUREXIS TRAINING AG · FREE RESOURCE

ISO/IEC 27001:2022 Implementation Checklist

Clauses 4–10 · mandatory documents · all 93 Annex A controls · certification readiness

Aligned with: ISO/IEC 27001:2022 including Amendment 1:2024

How to use: tick each item when it is in place and you can show evidence. Use the matching Aurexis Excel workbook to track owners, dates and evidence. Requirements are paraphrased by Aurexis; always work from the official text. Using this checklist does not guarantee certification or compliance.

Part 1 — Clauses 4 to 10 (all mandatory)

✓	Clause	What must be in place
☐	4.1	Internal and external issues relevant to the ISMS are identified, including whether climate change is a relevant issue (Amd 1:2024).
☐	4.2	Interested parties and their information security requirements are identified, including any climate-related requirements, and it is decided which are addressed by the ISMS.
☐	4.3	ISMS scope is defined and documented, including boundaries, interfaces and dependencies.
☐	4.4	The ISMS and its processes, and how they interact, are established and maintained.
☐	5.1	Top management demonstrates commitment: resources, integration into business processes, direction and support.
☐	5.2	An information security policy is approved, documented, communicated and available to interested parties as appropriate.
☐	5.3	ISMS roles, responsibilities and authorities are assigned and communicated.
☐	6.1.1	Risks and opportunities affecting ISMS outcomes are determined and actions to address them are planned.
☐	6.1.2	A documented risk assessment process defines risk criteria (acceptance and assessment) and produces consistent, comparable results.
☐	6.1.3	A documented risk treatment process selects options and controls, compares them with Annex A, and produces a Statement of Applicability and a risk treatment plan approved by risk owners.
☐	6.2	Measurable information security objectives are set, documented, monitored and communicated, with plans to achieve them.
☐	6.3	Changes to the ISMS are carried out in a planned manner.
☐	7.1	Resources needed for the ISMS are determined and provided.
☐	7.2	Competence of people doing work under the ISMS is determined, achieved and evidenced.
☐	7.3	People are aware of the policy, their contribution and the implications of not conforming.
☐	7.4	Internal and external communication needs (what, when, with whom, how) are determined.
☐	7.5	Documented information is created, updated and controlled (identification, review, approval, access, retention).
☐	8.1	Processes are planned, implemented and controlled; criteria are set; externally provided processes are controlled.
☐	8.2	Risk assessments are performed at planned intervals and on significant change; results are retained.
☐	8.3	The risk treatment plan is implemented; results are retained.
☐	9.1	What is monitored and measured, how, when and by whom is defined; results are evaluated and retained.

✓	Clause	What must be in place
☐	9.2	An internal audit programme is planned and run by objective auditors; results are reported and retained.
☐	9.3	Management reviews take place at planned intervals with the required inputs; decisions and actions are retained.
☐	10.1	The suitability, adequacy and effectiveness of the ISMS are continually improved.
☐	10.2	Nonconformities are reacted to, root causes analysed, corrective actions taken and their effectiveness reviewed; records retained.

Part 2 — Mandatory documented information

✓	Clause	Document / record
☐	4.3	ISMS scope
☐	5.2	Information security policy
☐	6.1.2	Risk assessment process and risk criteria
☐	6.1.3	Risk treatment process
☐	6.1.3 d)	Statement of Applicability (SoA)
☐	6.1.3 e) / 6.2	Risk treatment plan
☐	6.2	Information security objectives
☐	7.2	Evidence of competence
☐	7.5.1 b)	Other documented information the organisation decides is necessary
☐	8.1	Evidence that processes are carried out as planned
☐	8.2	Results of risk assessments
☐	8.3	Results of risk treatment
☐	9.1	Monitoring and measurement results
☐	9.2	Internal audit programme and audit results
☐	9.3	Results of management reviews
☐	10.2	Nonconformities, actions taken and results of corrective action

Part 3 — Annex A controls (93): decide, justify, implement

For each control record in your Statement of Applicability whether it applies, why, and its status. ★ = new in the 2022 edition. Columns: A = applicable and justified in SoA · I = implemented with evidence.

5 Organizational controls (37)

A	I	No.	Control	A	I	No.	Control
☐	☐	5.1	Policies for information security	☐	☐	5.20	Addressing information security within supplier agreements
☐	☐	5.2	Information security roles and responsibilities	☐	☐	5.21	Managing information security in the ICT supply chain
☐	☐	5.3	Segregation of duties	☐	☐	5.22	Monitoring, review and change management of supplier services
☐	☐	5.4	Management responsibilities	☐	☐	5.23	★ Information security for use of cloud services
☐	☐	5.5	Contact with authorities	☐	☐	5.24	Information security incident management planning and preparation
☐	☐	5.6	Contact with special interest groups	☐	☐	5.25	Assessment and decision on information security events
☐	☐	5.7	★ Threat intelligence	☐	☐	5.26	Response to information security incidents
☐	☐	5.8	Information security in project management	☐	☐	5.27	Learning from information security incidents
☐	☐	5.9	Inventory of information and other associated assets	☐	☐	5.28	Collection of evidence
☐	☐	5.10	Acceptable use of information and other associated assets	☐	☐	5.29	Information security during disruption
☐	☐	5.11	Return of assets	☐	☐	5.30	★ ICT readiness for business continuity
☐	☐	5.12	Classification of information	☐	☐	5.31	Legal, statutory, regulatory and contractual requirements
☐	☐	5.13	Labelling of information	☐	☐	5.32	Intellectual property rights
☐	☐	5.14	Information transfer	☐	☐	5.33	Protection of records
☐	☐	5.15	Access control	☐	☐	5.34	Privacy and protection of PII
☐	☐	5.16	Identity management	☐	☐	5.35	Independent review of information security
☐	☐	5.17	Authentication information	☐	☐	5.36	Compliance with policies, rules and standards for information security
☐	☐	5.18	Access rights	☐	☐	5.37	Documented operating procedures
☐	☐	5.19	Information security in supplier relationships				

6 People controls (8)

A	I	No.	Control	A	I	No.	Control
☐	☐	6.1	Screening	☐	☐	6.5	Responsibilities after termination or change of employment
☐	☐	6.2	Terms and conditions of employment	☐	☐	6.6	Confidentiality or non-disclosure agreements
☐	☐	6.3	Information security awareness, education and training	☐	☐	6.7	Remote working
☐	☐	6.4	Disciplinary process	☐	☐	6.8	Information security event reporting

7 Physical controls (14)

A	I	No.	Control	A	I	No.	Control
☐	☐	7.1	Physical security perimeters	☐	☐	7.8	Equipment siting and protection
☐	☐	7.2	Physical entry	☐	☐	7.9	Security of assets off-premises
☐	☐	7.3	Securing offices, rooms and facilities	☐	☐	7.10	Storage media
☐	☐	7.4	★ Physical security monitoring	☐	☐	7.11	Supporting utilities

A	I	No.	Control	A	I	No.	Control
☐	☐	7.5	Protecting against physical and environmental threats	☐	☐	7.12	Cabling security
☐	☐	7.6	Working in secure areas	☐	☐	7.13	Equipment maintenance
☐	☐	7.7	Clear desk and clear screen	☐	☐	7.14	Secure disposal or re-use of equipment

8 Technological controls (34)

A	I	No.	Control	A	I	No.	Control
☐	☐	8.1	User endpoint devices	☐	☐	8.18	Use of privileged utility programs
☐	☐	8.2	Privileged access rights	☐	☐	8.19	Installation of software on operational systems
☐	☐	8.3	Information access restriction	☐	☐	8.20	Networks security
☐	☐	8.4	Access to source code	☐	☐	8.21	Security of network services
☐	☐	8.5	Secure authentication	☐	☐	8.22	Segregation of networks
☐	☐	8.6	Capacity management	☐	☐	8.23	★ Web filtering
☐	☐	8.7	Protection against malware	☐	☐	8.24	Use of cryptography
☐	☐	8.8	Management of technical vulnerabilities	☐	☐	8.25	Secure development life cycle
☐	☐	8.9	★ Configuration management	☐	☐	8.26	Application security requirements
☐	☐	8.10	★ Information deletion	☐	☐	8.27	Secure system architecture and engineering principles
☐	☐	8.11	★ Data masking	☐	☐	8.28	★ Secure coding
☐	☐	8.12	★ Data leakage prevention	☐	☐	8.29	Security testing in development and acceptance
☐	☐	8.13	Information backup	☐	☐	8.30	Outsourced development
☐	☐	8.14	Redundancy of information processing facilities	☐	☐	8.31	Separation of development, test and production environments
☐	☐	8.15	Logging	☐	☐	8.32	Change management
☐	☐	8.16	★ Monitoring activities	☐	☐	8.33	Test information
☐	☐	8.17	Clock synchronization	☐	☐	8.34	Protection of information systems during audit testing

Part 4 — Certification readiness

✓	Item
☐	At least one full cycle of internal audit (9.2) completed, findings addressed.
☐	Management review (9.3) held with all required inputs; minutes retained.
☐	Statement of Applicability approved; every exclusion justified.
☐	Risk treatment plan approved by risk owners; residual risks accepted.
☐	Climate change considered in context analysis (4.1) and interested parties (4.2).
☐	Certification body selected (accredited); Stage 1 (documentation) and Stage 2 (implementation) audits booked.

Want to lead this yourself? The PECB ISO/IEC 27001 Lead Implementer course teaches you to do it end to end, exam included. aurexistraining.com/training/iso-27001-lead-implementer