Aegentra
ACADEMY

ISO/IEC 27001:2022 Internal Audit Checklist

Clauses 4–10 — lines of enquiry, evidence to request, and the common failure

Clauses 4 to 10 are mandatory and cannot be excluded. Annex A controls are sampled risk-based against your own Statement of Applicability, so no fixed Annex A checklist can be correct for every organisation.

CLAUSE	AREA	LINE OF ENQUIRY	EVIDENCE TO REQUEST	COMMON FAILURE
4.1	Context	Are internal and external issues relevant to the ISMS determined and current?	Documented issues list with a review date	A list written once at certification and never revisited
4.2	Context	Are interested parties and their relevant requirements identified?	Register of parties with their security requirements	Customers listed but no requirements captured
4.3	Context	Is the ISMS scope documented, justified, and available?	Scope statement naming locations, assets, technologies and exclusions	Scope that excludes something material without a boundary justification
4.4	Context	Is the ISMS established, implemented, maintained and continually improved?	Evidence the system operates — records, not intent	A documented system with no operating records
5.1	Leadership	Does top management demonstrate leadership and commitment?	Minutes, budget approvals, resourcing decisions	A signed policy treated as the whole of Clause 5.1
5.2	Leadership	Is there an approved information security policy, communicated and available?	Approved policy, communication evidence, staff able to describe it	Policy on the intranet that no sampled staff member can locate
5.3	Leadership	Are roles, responsibilities and authorities assigned and understood?	Assignment records; individuals able to state their own responsibilities	A RACI matrix nobody in the sample recognises
6.1.1	Planning	Are risks and opportunities to the ISMS itself addressed?	Planning records covering the management system, not only information risks	Confusing ISMS risk with information security risk
6.1.2	Planning	Is the risk assessment process documented, repeatable and applied?	Documented method with criteria; consistent results on re-run	A method described after the fact to match the register
6.1.3	Planning	Is there a risk treatment process and a Statement of Applicability?	SoA addressing all 93 Annex A controls with justifications for inclusion and exclusion	A partial SoA listing only implemented controls — the most common finding
6.2	Planning	Are information security objectives measurable, monitored and resourced?	Objectives with metrics, owners, target dates and progress	Aspirational objectives with no measurement
6.3	Planning	Are changes to the ISMS planned rather than ad hoc?	Change records showing the ISMS impact was considered	Infrastructure change control mistaken for ISMS change planning
7.1	Support	Are resources for the ISMS determined and provided?	Budget, headcount, tooling evidence	Resourcing asserted but not evidenced
7.2	Support	Is competence determined, achieved and evidenced?	Competence records for named individuals in ISMS roles	A training matrix with no completion records
7.3	Support	Are staff aware of the policy, their contribution and the consequences?	Sampled staff can describe how to report an incident	Awareness training completed but no retained understanding
7.4	Support	Is internal and external ISMS communication determined?	Who communicates what, to whom, when and how	No defined external communication for incidents
7.5	Support	Is documented information controlled — version, approval, access, retention?	Version control, approval records, access restrictions	Current documents alongside superseded copies with no version marking
8.1	Operation	Are planned processes carried out and evidenced?	Operational records matching the documented process	Process documented one way, performed another
8.2	Operation	Are risk assessments performed at planned intervals and on significant change?	Dated assessments; revision history on the register	A register with a single creation date
8.3	Operation	Is the risk treatment plan implemented and its results retained?	Treatment actions closed with evidence	Open treatments past their target date with no comment
9.1	Evaluation	Is what needs monitoring determined, measured, analysed and evaluated?	Defined metrics, actual numbers, and evidence someone reviewed them	Metrics collected but never analysed
9.2	Evaluation	Are internal audits conducted to a programme by impartial auditors?	Audit programme, plans, reports, and an impartiality declaration	The ISMS owner auditing their own management system
9.3	Evaluation	Is management review held covering every required input, with decisions?	Minutes showing decisions and actions against each 9.3.2 input	Minutes recording attendance and no decisions
10.1	Improvement	Is the ISMS continually improved?	Evidence of change driven by measurement, audit or review	Improvement asserted with no examples

CLAUSE	AREA	LINE OF ENQUIRY	EVIDENCE TO REQUEST	COMMON FAILURE
10.2	Improvement	Are nonconformities controlled, root-caused, corrected and verified?	Log with root cause, correction, corrective action and verified effectiveness	Root cause recorded as "human error" with no further analysis