Aegentra
ACADEMY

ISO/IEC 27001:2022 Internal Audit Plan

Worked example — a 100-staff Australian B2B SaaS, second surveillance cycle

Clause 9.2 requires a documented audit programme, defined criteria and scope, and auditors who are objective and impartial. Agree the plan, criteria and sampling rationale before fieldwork begins — reconstructing them afterwards is the finding.

REF	AUDIT ELEMENT	DETAIL	WHAT THE CERTIFICATION BODY CHECKS
1.1	Audit objective	Determine whether the ISMS conforms to ISO/IEC 27001:2022 and to the organisation's own documented requirements, and whether it is effectively implemented and maintained.	That the objective is stated and is about conformity AND effectiveness, not just documents.
1.2	Audit criteria	ISO/IEC 27001:2022 Clauses 4–10; the Statement of Applicability rev 3.1; the information security policy; documented procedures; applicable contractual and legal obligations.	That criteria are named and versioned. "ISO 27001" alone is not audit criteria.
1.3	Audit scope	The whole ISMS as defined in the scope statement: the SaaS platform, supporting corporate IT, and the Melbourne and remote workforce. Excludes the customer's own environments.	That scope matches the certificate scope, and that exclusions are boundary statements, not avoidance.
1.4	Audit type	First-party (internal) audit, delivered by an independent external party under Clause 9.2.	Independence of the auditor from the design and operation of what is audited.
1.5	Auditor and impartiality	Lead auditor holds an ISO 27001 Lead Auditor credential and had no role in designing or operating the ISMS. Impartiality declaration signed and retained in the working papers.	A signed declaration. "We used a different team member" is routinely challenged.
1.6	Audit programme context	Year 1 of a documented two-year programme. Controls sampled this cycle plus those scheduled next together achieve full coverage across the certification cycle.	That the programme — not the single audit — covers the whole ISMS over time. Frequently tested and frequently missing.
1.7	Risk-based sampling rationale	All of Clauses 4–10 tested. Annex A sampled by risk: every control treating a High residual risk, every control changed since the last audit, plus a rotating sample of the rest.	That sampling is justified, written down before fieldwork, and reproducible.
2.1	Opening meeting	Day 1, 09:00. Confirm scope, criteria, schedule, evidence handling, confidentiality, nonconformity grading, and the closing-meeting time. Attendance recorded.	An attendance record and confirmation that grading was explained before findings were raised.
2.2	Fieldwork — Clauses 4–6	Day 1. Context, interested parties, scope, leadership, policy, roles, risk assessment and treatment, Statement of Applicability, objectives.	That the SoA reconciles to the risk register in both directions.
2.3	Fieldwork — Clauses 7–8	Day 1–2. Resources, competence, awareness, communication, documented information, operational planning and control, risk assessment at planned intervals.	Competence evidence for named individuals, not a training policy.
2.4	Fieldwork — Annex A sample	Day 2. Sampled controls tested by interview, inspection of records and configuration, and examination of operational records. Every item indexed to a working paper reference.	That evidence is traceable. An untraceable finding cannot be defended.
2.5	Fieldwork — Clauses 9–10	Day 3. Monitoring and measurement, previous internal audit results, management review inputs and outputs, nonconformities, corrective action and verification of effectiveness.	That prior findings were closed with verified effectiveness, not just marked closed.
2.6	Findings validation	Every potential nonconformity tested against the organisation's evidence before it is reported. Matters closed on evidence are reported as such, with the reasoning retained.	That the report is not a list of first impressions.
2.7	Closing meeting	Day 3, 16:00. Findings presented with grade, clause reference and objective evidence. Agreement on factual accuracy — not on whether the finding is welcome.	That the auditee had the opportunity to challenge facts before the report issued.
3.1	Report issue	Final report within four business days of the closing meeting. Interim summary available earlier where a surveillance audit is imminent.	That the report predates the certification body visit and management review.
3.2	Corrective action	Root cause, correction, corrective action, owner and target date for each nonconformity. Effectiveness verified at a follow-up review, not at the point of closure.	Root cause that is a cause, not a restatement of the finding.
3.3	Records retained	Audit plan, impartiality declaration, working papers, evidence index, findings register, attendance records, report, corrective-action log.	That records exist and are retrievable. Clause 9.2.2(f) requires retention as evidence.