Aegentra
ACADEMY

ISO/IEC 27001:2022 Internal Audit Report

The structure a certification body will accept, section by section

This report is what a certification body reads as evidence that Clause 9.2 was met. Anything that cannot be traced to a working paper does not belong in it.

SECTION	CONTENTS	WHY IT IS THERE	COMMON OMISSION
1. Cover and distribution	Organisation, ISMS scope, audit dates, report date, audit type, lead auditor, distribution list.	Establishes what was audited and when, so the certification body can place it in the cycle.	Report date missing — so it cannot be shown to predate the management review.
2. Executive summary	Overall conclusion on conformity and effectiveness, counts of major and minor nonconformities and opportunities for improvement, and the status of previous findings.	The only section most of the board reads. It must state a conclusion, not describe activity.	A summary of what was done instead of what was concluded.
3. Objective, criteria and scope	Restated from the audit plan, with any in-flight changes and the reason.	A report whose scope differs from its plan without explanation is not defensible.	Silent scope reduction where an area proved unavailable.
4. Audit programme position	Where this audit sits in the multi-year programme, and which areas are scheduled next.	Demonstrates full ISMS coverage across the certification cycle — routinely tested.	Treating a single audit as though it covered everything.
5. Impartiality statement	Confirmation the auditor was independent of the design and operation of what was audited.	Clause 9.2.2(c). Without it the audit can be dismissed regardless of quality.	Omitted entirely, or asserted without a signature.
6. Method and evidence	How evidence was obtained — interview, inspection of documented information, examination of records and configuration, sampling of operational records — and the sample basis.	Lets a reader judge whether the conclusion is supported by the work.	No sample sizes, so no way to judge sufficiency.
7. Clause-by-clause results	Clauses 4–10, each with a conformity statement and reference to supporting working papers.	Shows every mandatory clause was tested, not just the interesting ones.	Clauses grouped as "no issues found" with no evidence reference.
8. Annex A results	Controls sampled, the rationale for the sample, and results against the Statement of Applicability.	Ties the audit back to the SoA, which is the document the certification body starts from.	A control list with no link to the SoA revision audited.
9. Nonconformities	Each finding with grade, clause, requirement, objective evidence and the statement of nonconformity. Cross-referenced to the corrective action log.	The findings are the audit. Everything else supports them.	Findings written as advice — "should consider" — rather than as a stated gap.
10. Opportunities for improvement	Observations that are not nonconformities, clearly separated so they cannot be confused.	Adds value without inflating the nonconformity count.	OFIs mixed into the findings register, making the result look worse than it is.
11. Matters raised and closed on evidence	Potential findings examined further and closed, with the reasoning.	Shows the report is tested rather than a list of first impressions. Rarely included, and it is what makes an internal audit trustworthy.	Omitted, so the reader cannot see what was considered and rejected.
12. Previous findings	Status of every finding from the last audit, with verification of effectiveness.	Clause 10.2 requires effectiveness to be verified, not merely actioned.	Marked closed on the strength of the action plan, not the outcome.
13. Conclusion	Whether the ISMS conforms and is effectively implemented and maintained, with any caveats.	The auditor's opinion, stated plainly.	Trailing off without an opinion.
14. Appendices	Audit plan, attendance records, evidence index, corrective action log.	Makes the audit reproducible and the findings traceable.	No evidence index, so no finding can be independently checked.