Aegentra
ACADEMY

ISO/IEC 27001:2022 Nonconformity Report

Two worked findings — one major, one minor — plus a blank column to copy

A nonconformity needs three things to survive challenge: the requirement, the objective evidence, and the gap between them. A finding without evidence is an opinion, and root cause that restates the finding is not a root cause.

FIELD	NC-2026-001 (MAJOR)	NC-2026-002 (MINOR)	YOUR FINDING
Grade	Major	Minor	
Grading rationale	A required process is absent — not a lapse in an existing one. Absence of a mandatory clause requirement is the textbook major.	A defined process exists and generally operates; a single instance departed from it.	
Clause / control	Clause 9.3 — Management review	A.5.15 — Access control	
Requirement	Top management shall review the ISMS at planned intervals, covering the inputs listed in 9.3.2, and retain documented information as evidence.	Access rights shall be reviewed in accordance with the organisation's topic-specific policy. The policy specifies a quarterly review of privileged accounts.	
Objective evidence	No management review has been held since 14 March 2025. The stated interval is annual. No minutes, agenda or decision record exists for the 2026 period. Confirmed with the ISMS owner and the CTO, and by inspection of the governance folder.	Privileged access reviews are evidenced for Q3 and Q4 2025 and Q2 2026. No record exists for Q1 2026. Sampled 4 of 4 quarters; 1 of 4 has no record. The reviewer was on extended leave and no delegate was assigned.	
Statement of nonconformity	The organisation has not conducted a management review within its own stated interval, and holds no documented information evidencing review for the current period.	The quarterly privileged access review required by the access control policy was not performed for Q1 2026.	
Auditee response	Accepted. Review scheduled for 12 August 2026 with all 9.3.2 inputs.	Accepted. Q1 review performed retrospectively 22 July 2026; no inappropriate access found.	
Correction	Hold the overdue management review and minute the decisions.	Perform the missed review and record the outcome.	
Root cause	Governance calendar ownership was never assigned when the previous ISMS owner left. No trigger existed to schedule the review.	The control depended on one named individual with no delegate. A single point of failure in the process, not a lapse by the individual.	
Corrective action	Assign the governance calendar to a named role with a documented deputy; add a standing quarterly agenda item; add ISMS handover to the offboarding checklist.	Name a backup reviewer in the access control policy; add an automated reminder with escalation if no record is filed within 10 business days of quarter end.	
Owner / target date	CTO — 12 August 2026	Security Lead — 31 August 2026	
Effectiveness verification	Confirm at the next internal audit that two consecutive reviews were held on schedule with decisions minuted. Closure of the action is not evidence of effectiveness.	Confirm two consecutive quarters produce a filed record without manual chasing.	
Status	Open — verification due at next audit	Open — verification due Q4 2026	