MAGELLAN AI · SEMANTIC MATCH ENGINE · ONE-PAGER

ISO/IEC 27001:2022 — Annex A.5, A.8, A.5.35

Logging integrity, segregation of duties, and independent review — as system properties, not ISMS prose.

What the regulator asks

Across recent ISO 27001:2022 surveillance and recertification audits, the most frequent major nonconformities cluster around **A.8.15** (logging — completeness and protection), **A.5.3** (segregation of duties — actually enforced), and **A.5.35** (independent review — documented and performed). The ISMS describes these controls; the supporting system rarely produces the evidence in the time the audit allows.

Clause → Magellan primitive

Clause	What it requires	How Magellan answers it
A.8.15	Logging — events recorded, protected, reviewed.	SHA-256 hash chain — log integrity is structural. The certifier re-walks the chain on their own laptop; no verbal assurance needed.
A.5.3	Segregation of duties — enforced, not aspirational.	Seven-role RBAC: no role can both edit mappings and read the full audit ledger. Enforced via row-level security.
A.5.18	Access rights granted, reviewed, removed under control.	Role grants are themselves ledger entries; Administrator cannot grant audit roles. Periodic access review is a query.
A.5.35	Independent review of information security on a defined cadence.	Compliance Officer signs the periodic attestation as a ledger entry inside the ledger being reviewed.
A.5.2	Information security roles and responsibilities defined.	Named Security Officer role with documented mandate; role grants flow through Security Officer, not Administrator.
A.5.33	Protection of records — preserved per business / legal requirement.	WORM secondary sink with configurable retention; shortening retention requires Compliance Officer signature.
A.8.34	Protection of information systems during audit testing.	Append-only enforced twice: privilege REVOKE + database trigger. Audit testing cannot inadvertently mutate evidence.

Why this works on inspection

- **The ISMS document references a real system.** A.8.15 stops being "we have logging" and becomes "here is the verification script."
- **Same evidence supports SOC 2, ISO 27001, and SOX overlapping controls.** One pack, multiple certifiers.
- **Suspended certificates are revenue events.** Magellan compresses the major-NC remediation cycle from quarters to weeks.

Evidence pack the assessor receives

Ledger range with hash chain, role-grant history, retention-policy entries, Compliance Officer attestation entries, and a verification script. Format matches what a UKAS- or ANAB-accredited certifier expects on a surveillance audit.