MAGELLAN AI · SEMANTIC MATCH ENGINE · ONE-PAGER

FedRAMP Moderate / High — NIST SP 800-53 AU & AC Families

Co-located audit writer with structural splits, WORM secondary sink, and role grants in the ledger itself.

What the regulator asks

Across recent 3PAO authorization packages, AU-2, AU-9, AU-6, and AC-5 generate the highest concentration of POA&M items. The pattern: application-layer log shipping satisfies AU-2 (the event happened) but fails AU-9 (protection from modification by the actor that generated it). Magellan's answer is structural — privilege separation enforced at the database, immutable secondary sink.

Clause → Magellan primitive

Clause	What it requires	How Magellan answers it
`AU-2 / AU-3`	Define auditable events with sufficient content.	Every mapping decision is a ledger entry: actor, role-at-time, action, signature, ISO-8601 timestamp, ULID identity.
`AU-9`	Protection of audit information from modification by the actor that generated it.	WORM secondary sink (S3 Object Lock, compliance mode) — application has PutObject only. Bytes are immutable for the retention period.
`AU-10`	Non-repudiation — actor cannot later deny the action.	Two-component e-signature is itself in the ledger; SHA-256 hash chain prevents silent edit.
`AU-11`	Audit record retention aligned with authorization package.	Retention is configurable per the SSP; only Compliance Officer can shorten retention, and shortening is itself a signed ledger entry.
`AU-6`	Audit record review, analysis, and reporting on a defined frequency.	Compliance Officer attestation cadence configurable to align with continuous-monitoring frequency.
`AC-5`	Separation of duties enforced.	Two Postgres roles inside one container: `magellan_app` cannot write to `audit_ledger`; `magellan_ledger_writer` has INSERT only.
`AC-6(7)`	Privilege review — silent escalation is detectable.	Role grants are themselves ledger entries (AC-6(9) logging of privileged functions). Administrator cannot grant audit roles.
`CM-3`	Configuration change control with documented approval.	Two-component e-signature on every release; signature is the configuration-change record.

Why this works on inspection

- **Same evidence pack covers continuous monitoring and 3PAO assessment.** No bespoke export per assessor.
- **Co-located writer with structural splits.** Privilege separation lives at the database, not in the application layer.
- **Year-2 capability:** dedicated authorization-boundary container if the SSP requires it without rewriting application code.

Evidence pack the assessor receives

Ledger range with hash chain, role-grant entries (AC-6(9)), retention-policy entries (AU-11), Compliance Officer attestation entries (AU-6), and a verification script. Maps cleanly into the standard FedRAMP Continuous Monitoring deliverable structure.