MAGELLAN AI · SEMANTIC MATCH ENGINE

Audit Ledger

ULID-keyed, SHA-256–chained, tamper-evident decision history

What is recorded

Every accepted Semantic Match decision is appended to an immutable, append-only ledger. Each entry is keyed by a ULID (never UUID) and references the previous entry's SHA-256 hash, producing a tamper-evident chain. The ULID prefix encodes the creation timestamp, so the chain is chronologically ordered without separate index keys.

Ledger entry schema

Field	Type	Purpose
`id`	`ULID`	Primary key; lexicographically sortable, time-ordered.
`prev_hash`	`sha256`	Hash of the previous entry; binds the chain.
`entry_hash`	`sha256`	Hash of this entry's canonical JSON.
`source.id / target.id`	`A-ULID`	Stable attribute identities from the MetaModel.
`source.path / target.path`	`string`	Dot-delimited schema path (e.g. patient.address.zip).
`confidence`	`int 0–100`	Engine's confidence for the pair.
`algorithm`	`enum`	exact_match | synonym_match | abbreviation_match | context_hierarchy | domain_equivale
`rationale`	`string`	Short natural-language justification from the model.
`decision`	`enum`	AUTO-ACCEPT | REVIEW | REJECT (from active threshold profile).
`profile_ver`	`semver`	Threshold profile identifier in effect at decision time.
`model`	`string`	Model identifier, e.g. google/gemini-2.5-flash.
`api_version`	`semver`	semantic-match edge function version (currently 1.0.0).
`actor`	`string`	Authenticated user or service principal.
`ts`	`ISO-8601`	Wall-clock timestamp; ULID timestamp is authoritative.

Why ULID, not UUID

- Lexicographic sort = chronological sort. No secondary index needed for time-range scans.
- 26 characters, Crockford base32 — case-insensitive, URL-safe, copy-paste friendly.
- 128 bits of entropy + 48-bit timestamp prefix; collision-resistant without a coordinator.
- Aligns with regulatory expectations for monotonically traceable identifiers.

Reproducibility guarantee

Given any decision ULID, a reviewer can reconstruct exactly which model version, which threshold profile, and which annotations were in effect — six months or six years later. The ledger is the audit answer to HIPAA §164.312(b), 21 CFR Part 11 §11.10(e), and HHS Information Blocking review.

MAGELLAN AI · SEMANTIC MATCH ENGINE · ONE-PAGER

SOX §404 — Audit Evidence for Data Mapping Changes

Two-component e-signature, hash-chained ledger, role-at-time-of-action — mapped to PCAOB AS 2201.

What the regulator asks

PCAOB inspections keep citing change-management ITGCs and segregation-of-duties as Part II findings. The question on the walkthrough is the same every cycle: *show me every change to this mapping, prove no one altered it, and prove a single contributor did not push it to production.* Magellan answers each as a property of the data structure, not a process commitment.

Clause → Magellan primitive

Clause	What it requires	How Magellan answers it
`§404 ICFR`	Change integrity over financial-reporting data flows.	SHA-256 hash chain over every ledger entry. A verifier walks the chain in O(n); any altered byte invalidates every downstream hash.
`AS 2201`	Segregation of duties between preparer and approver, evidenced.	Two-component e-signature on every release — Contributor draft + Approver release, enforced as distinct identities at the database, not in code.
`§404 + AS 2201`	Privilege escalation cannot rewrite who-did-what historically.	Role-at-time-of-action stamped on every entry. A contributor promoted to approver next quarter still appears as contributor in last quarter's ledger.
`§103`	Seven-year retention of audit working papers.	WORM secondary sink (S3 Object Lock, compliance mode); 7-year default retention is configurable but a Compliance-Officer-only operation.
`§302 / §906`	Officer attestation traceable to underlying records.	Quarterly Compliance Officer attestation is itself a ledger entry, signed and hash-bound to the range it certifies.

Why this works on inspection

- **The walkthrough takes minutes, not weeks.** Filter by mapping ULID and date range; the chronological order is the primary key, not a sortable column.
- **Reproducible exports.** Two pulls of the same range produce byte-identical evidence packs — the verification script runs on the auditor's own laptop.
- **Administrator cannot read the ledger.** Magellan's seven-role RBAC keeps platform admin and audit-evidence access on different roles. SoD is structural.

Evidence pack the assessor receives

A signed archive containing the ledger range (chronologically ordered by ULID), the SHA-256 hash chain, the role grants in effect during the range, the Compliance Officer's attestation entries, and a dependency-free verification script. Same shape every quarter, every walkthrough, every framework.

MAGELLAN AI · SEMANTIC MATCH ENGINE · ONE-PAGER

GxP — 21 CFR Part 11 & EU GMP Annex 11

Audit-trail integrity, two-component e-signatures, and independent review — by structure, not by SOP.

What the regulator asks

FDA Form 483s and EU GMP critical findings cluster around **§11.10(e)** (audit trail integrity), **§11.10(j)** (independent review), and **Annex 11 §9**. The pattern is the same: audit trails exist, but the Administrator can read or alter them, and the "independent review" is performed by the same person who could have edited the records.

Clause → Magellan primitive

Clause	What it requires	How Magellan answers it
`§11.10(e)`	Audit trails shall not obscure previously recorded information.	Append-only ledger enforced twice: REVOKE UPDATE/DELETE on the role, plus a row-level trigger that raises on any modification attempt.
`§11.10(j)`	Independent review of records on a defined cadence.	Compliance Officer is a distinct role; Administrator cannot read or alter the ledger. The review is itself a signed ledger entry.
`§11.50`	Signature manifestation includes signer, datetime, meaning.	Signature manifestation lives in the same row as the signature — name, ISO-8601 timestamp, and meaning string ("draft" / "release" / "attestation").
`§11.200`	Two-component electronic signatures.	Drafter ≠ releaser, enforced at the database. Same identity attempting both signatures is rejected before commit.
`Annex 11 §9`	Audit trails generated independently and protected from alteration.	SHA-256 hash chain — verification is a script the inspector runs themselves; no verbal assurance required.
`Annex 11 §14`	Electronic signatures linked to their records.	Signature is itself a ledger entry; hash-chained to the record it signs. Severing the link breaks the chain.

Why this works on inspection

- **The independent reviewer is structurally incapable of editing what they review.** Not a process commitment — an RBAC property.
- **Reproducibility across inspectors.** An FDA inspector and an EU GMP inspector see byte-identical evidence from the same export.
- **Product-lifecycle retention.** Default retention is the longer of 6 years (HIPAA), 7 years (SOX), or product lifecycle (GxP). Shortening it requires a Compliance Officer signature.

Evidence pack the assessor receives

Ledger range with hash chain, role grants during the range, all e-signatures with §11.50 manifestation in-line, Compliance Officer attestation entries, retention-policy entries, and a verification script. The pack is the same shape an FDA inspector and an EU GMP inspector both expect.

MAGELLAN AI · SEMANTIC MATCH ENGINE · ONE-PAGER

GDPR — Articles 30, 32, and 5(1)(c)

Time-accurate records of processing, by-reference pseudonymisation, and lawful-basis stamping.

What the regulator asks

Recent supervisory-authority decisions cite **Article 30** (records of processing) as a standalone violation, separate from breach. Fines under Art. 83(4) reach €10M or 2% of global turnover. The question: *what was the lawful basis, the recipient, and the retention rule for this processing on the day of the request?* — not what the dashboard says today.

Clause → Magellan primitive

Clause	What it requires	How Magellan answers it
`Art. 30(1)`	Records of processing — categories, recipients, retention, transfers — kept up to date.	ULID primary key — lexicographic order is chronological order. "What was true on day X" is a primary-key range scan.
`Art. 5(1)(c)`	Data minimisation in records of processing themselves.	Mappings reference data by ULID; payload never enters the ledger. The Art. 30 record does not become an Art. 5 problem.
`Art. 5(2)`	Accountability — controller must demonstrate compliance.	SHA-256 hash chain over Art. 30 records. The controller can prove the record was not retroactively edited after the supervisory request.
`Art. 6`	Lawful basis recorded and traceable to the processing activity.	Lawful-basis tag on every mapping, signed by the Approver. The basis at release time is what the supervisory authority sees.
`Art. 32(4)`	Persons act only under instructions of the controller.	Role-at-time-of-action stamping. Contractor or processor role is preserved retroactively; promotion does not rewrite history.
`Art. 33`	Breach notification within 72 hours — evidence ready.	Reproducible exports — the Art. 30 record needed for the notification is a query, not a project.

Why this works on inspection

- **The DPO answers a supervisory request as a query, not a project.** Time-accurate Art. 30 evidence is a property of ULID ordering.
- **Pseudonymisation by reference.** Personal data lives in the mapped store; the ledger references it by ULID. Art. 30 export ≠ Art. 5 problem.
- **Joint-controller scenarios.** Per-tenant signing keys (year-2 capability) keep evidence separable when controllers diverge.

Evidence pack the assessor receives

Art. 30 record for the queried date range, SHA-256 hash chain, role grants and processor designations in effect, lawful-basis tags on every referenced mapping, and a verification script. Format matches what a supervisory authority case officer expects under most national DPA practice.

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.

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.