C19: Proof-of-Unchanged for AI Governance and Digital Artefact Provenance

Custody-Boundary Verification Methodology for Models, Data, and Audit Evidence

Audience: AI Governance, Cloud Assurance, Enterprise Risk, Regulated Industry Solutions, Internal Audit
Applies to: Model artefacts, training/evaluation datasets, audit evidence, retained documentation
Methodology Type: Deterministic integrity verification at custody boundaries
Anchoring Software: AuditLog.AI **Auditing Software:** QMS Auditor **Version:** v5
Mode: Zero-Custody | Hash-Only | Human-Verified | Machine-Deterministic | Time-Anchored
Protocol Originator: Dr. Fernando Telles
Date: 06 February 2026
AI_used: true
LLM_used: LLM1 <> LLM4
Human_verified: true (HV_FT)
Classification: Public methodology document (governance & assurance infrastructure; non-clinical)
Primary references:
- C12 AuditLog.AI Global Compliance Matrix (Ordinal 12; DOI: 10.5281/zenodo.17462383)
- C17 Proof-of-Unchanged Global Application Matrix (Ordinal 16; DOI: 10.5281/zenodo.18501507)

> **One-sentence summary:** Proof-of-Unchanged is a custody-boundary verification methodology that deterministically establishes whether AI and digital artefacts have changed since their last verified checkpoint, without relying on platform trust or system integration.

Why this matters to Big Tech

Large technology platforms now operate under overlapping obligations for: - **AI governance and accountability** (EU AI Act Articles 11–12, emerging global AI regulation), - **enterprise assurance** (SOC 2, ISO 27001/27701, internal controls), - **data and model provenance** (training datasets, model artefacts, audit evidence), - **long-term retention and re-use of regulated evidence**.

Across these domains, the problem is the same:

> Once data or model artefacts leave an operating system, how do you prove—later and independently—that they have not changed?

Proof-of-Unchanged addresses this problem **without interfering with production systems** and **without assuming ongoing trust in platforms, vendors, or cloud providers**.

What Proof-of-Unchanged is (and is not)

What it is

- A **verification methodology**, not a monitoring or enforcement system.
- Applied **at custody boundaries** (export, archive, migration, deployment).
- Based on **cryptographic invariants** (dual-hash, time attestation, public anchoring).
- Produces **deterministic outcomes**:
  - **PASS** — artefact proven unchanged relative to a prior canonical state.
  - **Divergence enumerated** — explicit, cryptographic description of what differs.

What it is not

- Not real-time monitoring.
- Not content analysis or semantic interpretation.
- Not security prevention or threat detection.
- Not clinical decision support or medical software.
- Not an operational control layer inside production systems.

The custody-boundary model (global)

Proof-of-Unchanged is applied **immediately after export** and **immediately after any sanctioned transformation**.

Phase	Trigger	Action	Result
T_0 — Export	Artefact leaves a source system	Freeze → dual-hash → time-attest → anchor	Canonical state established
T_1 — Verification	Audit, inspection, or re-use	Re-hash and compare	PASS or divergence enumerated
T_2 — Sanctioned change	Compression, normalization, migration	Verify → transform → re-anchor	New canonical state
T_n — Re-verification	Any future challenge	Re-verify against last anchor	Continuous provenance preserved

This pattern generalizes across **AI, cloud, financial audit, and regulated data environments**.

Domain-specific relevance for Big Tech

1. AI model governance

Question: Is the deployed model identical to the version that passed review?
Application:
- Freeze and anchor model artefacts at approval. - Re-verify before deployment, audit, or regulatory disclosure. - Divergence triggers bounded investigation (no inference about intent).

2. Training data and evaluation datasets

Question: Has the training or evaluation dataset changed since bias/safety review?
Application:
- Evidence Set Fingerprint (ESF) verifies dataset membership and integrity. - Enables independent confirmation during internal or external audits.

3. Cloud compliance and assurance

Question: Can we prove audit evidence has not been altered after export?
Application:
- Supports SOC 2 (particularly **Processing Integrity** and **Security** trust service criteria), ISO 27001, and internal control evidence reliability. - Operates outside the cloud control plane; no integration required.

4. Regulatory evidence retention (EU AI Act and beyond)

Question: Can we demonstrate documentation integrity years later, across platform migrations?
Application:
- Proof-only anchoring survives re-hosting, vendor exit, or system decommissioning. - Verification remains possible using retained copies alone.

PASS and divergence: proportional human effort

Proof-of-Unchanged enforces **proportionality**:

- **PASS**
    - Evidence proven unchanged.
    - No reconstructive investigation required.
- **Divergence enumerated**
    - Cryptographic identifiers describe the delta.
    - Human review is **bounded** to what differs.

> Divergence is informational, not accusatory.
> It does not imply error, misconduct, or non-compliance.

This preserves human authority over interpretation while removing ambiguity at the integrity layer.

Regulatory positioning (negative scope clarity)

Proof-of-Unchanged operates under **electronic records, audit documentation, and assurance frameworks**, including: - FDA **21 CFR Part 11**, - EMA **Annex 11** and GCP guidance, - TGA / **PIC/S PE 009-17**, - PCAOB **AS 1105 / AS 1215** (including **AS 1105.10A**, effective for fiscal years beginning on or after December 15, 2025), - ISA **230 / 500 / 240**.

It is **not**: - Clinical Decision Support Software, - a medical device, - or a system that provides recommendations to healthcare professionals.

How Big Tech typically evaluate this methodology

Engagement is **methodology-first**, not vendor-first:

- Internal governance or assurance teams assess the primitive against controlled scenarios.
- No production integration or customer data is required.
- Evaluation focuses on:
    - determinism,
    - independence,
    - and auditability over time.

Proof-of-Unchanged can be assessed using **public reference material** and **local test artefacts**.

What this enables (strategic)

- Independent verification of AI artefacts without platform dependence.
- Reduced audit burden through deterministic PASS outcomes.
- Clear separation between **verification** and **interpretation**.
- A reusable integrity layer across domains and jurisdictions.

Further reading

Full methodology reference: **C17 — Proof-of-Unchanged Global Application Matrix** (Ordinal 16; DOI: 10.5281/zenodo.18501507).
Compliance matrix: **C12 — AuditLog.AI Global Compliance Matrix** (Ordinal 12; DOI: 10.5281/zenodo.17462383).

Verification Model (hash-only, zero-custody) **Classification:** Methodology overview — non-commercial, non-interpretive

No regulatory authority has reviewed, classified, or endorsed this methodology. This page describes documented positioning, not regulatory acceptance.