C18: Proof-of-Unchanged for Audit Evidence Reliability

Custody-Boundary Verification Methodology for External Electronic Information

Audience: Audit & Assurance Partners, Audit Quality Leadership, Digital Assurance / Innovation, Technology Risk
Applies to: Audit evidence sets, external electronic information, assembled audit files, retained documentation
Methodology Type: Deterministic integrity verification (post-receipt, post-assembly, post-retention)
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 (audit infrastructure; non-interpretive)
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 audit evidence has changed since the last verified checkpoint, independent of system trust or vendor custody.

---

1) The problem (audit reality)

Modern engagements increasingly depend on **external electronic information** and digitally assembled evidence bundles: - external reports and confirmations, - third-party extracts and exports, - analytics outputs assembled from multiple sources, - evidence packages that move through retention and archival transformations.

Over time, evidence can be: - re-exported, - re-packaged, - migrated, - normalized, - compressed, - or re-assembled.

If bytes change, auditors need a defensible way to: - **detect** change, - **document** what changed, - and scale review effort proportionally.

---

2) The methodology

Proof-of-Unchanged (canonical)

If evidence and membership bytes are identical to a prior canonical state, this is deterministically provable (PASS).

Divergence enumeration (informational)

If evidence and/or membership bytes differ, the deltas are enumerated to bound investigation.

Important boundary: - Divergence is **not** an accusation. - Divergence does **not** imply control failure. - Divergence is a directional signal to allocate human effort to the minimal delta set.

> PASS reduces reconstructive work.
> Divergence bounds reconstructive work.

3) Where it fits (custody boundaries, not inside systems)

Verification is applied **immediately before and/or after custody boundaries**: - **Receipt boundary:** when evidence is received into the audit file. - **Assembly boundary:** when workpapers/evidence packages are assembled. - **Transformation boundary:** immediately before and after evidence is converted, compressed, or migrated. - **Retention boundary:** at periodic re-verification points.

No integration into client source systems is required.

4) Canonical state cycle ($T_0 \rightarrow T_n$)

Standard cycle

1. **Freeze** the evidence bundle locally (stable baseline).
2. **Manifest + dual-hash** deterministically.
3. Optional: **time attestation** (hash-only).
4. **Anchor hash-only** canonical state (publicly verifiable digest reference).
5. Re-verify later (T_n) against the last canonical (T_k).

Handling legitimate transformations ($T_1 \rightarrow T_2$)

If SOP transforms bytes (packaging/migration), the correct method is: - verify pre-transform (T_1), - transform, - re-freeze and re-anchor (T_2), - future verification compares against T_2.

This preserves **evidentiary continuity** without blocking lawful operations.

5) What this does not do

- Does not determine whether evidence is "true," "accurate," or "compliant."
- Does not replace auditor judgment, professional skepticism, or substantive procedures.
- Does not assert source authenticity; it asserts post-checkpoint **integrity**.
- Does not infer intent, misconduct, or control failure when divergence is detected.
- Does not operate inside client source systems; verification occurs at custody boundaries.

6) Standards alignment (positioning)

This methodology supports audit evidence and documentation frameworks such as: - PCAOB **AS 1105 / AS 1215** *(including AS 1105.10A — external electronic information reliability evaluation, effective for fiscal years beginning on or after December 15, 2025)* - ISA **230 / 500 / 240** - Cross-domain electronic record integrity frameworks (FDA **21 CFR Part 11**, EMA **Annex 11**, TGA / **PIC/S PE 009-17**) when engagements involve regulated systems or external electronic evidence from regulated environments.

7) Terminology mapping (audit language)

Proof-of-Unchanged term	Audit & assurance translation
Canonical state	Evidence set baseline / retained audit file state
PASS	Integrity confirmed; no integrity exception
Divergence enumerated	Exception requiring investigation / attribution
Custody boundary	Receipt / assembly / transfer / retention checkpoint
Proportional review	Risk-/materiality-aligned investigation scope

8) Public verification references (representative)

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).

9) Evaluation (methodology-first)

If your Audit Innovation / Digital Assurance team is evaluating methods for evidence reliability documentation:

- A controlled methodology evaluation can be performed using **public documentation** and **local test artefacts**.
- No client data transfer is required.
- Outputs are hash-only verification outcomes (PASS / divergence enumeration).
- No regulatory authority has reviewed, classified, or endorsed this methodology.

Contact: Fernando.Telles@AuditLog.AI

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