C12 – AuditLog.AI Global Compliance Matrix

Globally Harmonized, Cryptographically-Anchored Regulatory Compliance Map for Digital Audit and Reproducibility Systems

Submitted as part of the AuditLog.AI Global Regulatory Submission Package (FDA/EMA/TGA/PCAOB/ISA Alignment)

Date: October 28, 2025

Inventor and Primary Contact: Fernando Telles BMedSc(Adv) MD(Dist)[1] [2]

Position: CEO & Founder **Email:** Dr.Telles@aihumansynergy.org **Phone:** Provided on Request **Address:** 21 Shields St, Flemington VIC 3031, AU **Web:** www.aihumansynergy.org

Engineers

Lead Software Engineer: Dr. Jacob Yang BEng, MEng, PhD[1] **Software Engineer:** Benjamin Hookey BEng (Mechatronics & Robotics), FSEng (Safety Instrumented Systems)[1]

Affiliations

[1] **Cardiovascular Diagnostic Audit & AI Pty Ltd (ACN 638 019 431)** – Registered Australian company conducting AuditLog.AI software development, audit and research services
[2] **Telles Investments Pty Ltd (ACN 638 017 384)** – Private IP holder

IP Rights

US Provisional #63/826,381 · AU Provisional #2025902482 · AU Trade Mark #2535745 & #2549093 IP Priority Date: 17 June 2025 (Global)

C12 – AuditLog.AI Global Compliance Matrix INDEX

- **Section V: ISA 230 / ISA 500 / ISA 240 (Revised 2025) — International Assurance Alignment**
- **Annex VI — Dossier Evidence Index (Execution Evidence Cross-Reference)**
- **Annex VII – Public Verification Provenance**

Executive Summary

This matrix provides a consolidated mapping between **AuditLog.AI** execution evidence and the regulatory clauses governing electronic records, validation, and audit documentation across the **FDA (21 CFR Part 11)**, **EMA (Annex 11)**, **TGA /PIC/S PE 009-17**, and international auditing standards (**PCAOB AS 1105 / 1215** and **ISA 230 / 500 / 240**).

All evidence in this compliance matrix originates from the AuditLog.AI Runtime Execution and System Validation Evidence Dossier (DOI 10.13140/RG.2.2.28551.25765 / Zenodo 10.5281/zenodo.17460850). Each artifact is verified through UTC timestamps, dual-hash cryptographic proofs (SHA-256 + RIPEMD-160), OpenTimestamps attestation, and Bitcoin mainnet anchoring (OP_RETURN). Complete provenance and anchor TXIDs are provided in Annex VII – Public Verification.

Regulatory Summary

Region	Submission Type	Regulatory Basis	Proposed Classification
FDA (USA)	Q-Submission (Q-Sub)	21 CFR Part 11 (Electronic Records / e-Signatures)	Standalone Electronic Records / Audit-Trail Infrastructure (non-device)
EMA (EU)	Scientific Advice (optional) + Annex 11 validation	EudraLex Vol 4 Annex 11 (Computerised Systems)	GMP Computerised System for Data Integrity (non-device)
TGA (Australia)	Excluded Software Determination	Excluded Goods Determination 2018 + PIC/S PE 009-17 Annex 11	LIMS-category audit infrastructure (non-medical device)

- **FDA (21 CFR Part 11)** — United States electronic records and signatures
- **EMA (Annex 11)** — European Union computerized systems for GMP
- **TGA (PIC/S PE 009-15)** — Australia therapeutic goods manufacturing principles

Auditing Standards Compliance Summary

Framework	Standard	Core Requirement	AuditLog.AI Compliance Mechanism
ISA / IAASB	**ISA 230**	Audit documentation enabling experienced auditor understanding	session log JSON compilation (who / what / when / meaning); append-only dual atomic ledgers for anchor receipts (TXID, block); frozen folder structure
ISA / IAASB	**ISA 500**	Sufficient appropriate audit evidence (quantity + quality: relevance + reliability)	cryptographic integrity + Bitcoin OP_RETURN (payload/TXID) external verification + OpenTimestamps
ISA / IAASB	**ISA 240**	Professional skepticism + fraud risk assessment + management override prevention	Append-only dual ledgers; non-repudiable e-signatures; fail-closed runtime checks; independent time attestations
PCAOB	**AS 1215**	Audit documentation with 60-day assembly + 7-year retention	Frozen sources UTC timestamp-locked archives; anchors linking records to public blockchain
PCAOB	**AS 1105**	Audit evidence evaluation (sufficiency + appropriateness)	Public blockchain TXID verification + OTS; deterministic hash parity from frozen session records
PCAOB	**AS 1105.10A (effective 2025)**	External electronic information reliability evaluation	Bitcoin blockchain (public, decentralized) + independent blockchain explorer verification tools

Notes: Evidence flow is zero-custody (proofs only); all artifacts are version-locked, non-adaptive, and human-approved prior to anchoring.

Section I: FDA 21 CFR Part 11 — Compliance Evidence Matrix

Official Reference Files:

`21 CFR Part 11 (up to date as of 9-29-2025)___20251020T193619Z.pdf`, `7883441_DataIntegrity___20251020T193619Z.pdf`, `58358119fnl___20251020T193619Z.pdf`, `58358119fnl___20251020T193619Z.pdf`

§11.10 Controls for Closed Systems — Evidence Mapping

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.10(a) (Validation: accuracy, reliability, consistent performance, discern invalid/altered records)	**4 & 8, 15-16, 38, 42-43**	Pre-/post-hasher audits (4 & 8) confirm 1:1 parity between the manifest and generated digests, ensuring every expected file is processed exactly once with no additions/omissions. PRE/POST runtime screenshots (15–16) show controlled execution and stable timing (Δ documented) consistent with intended performance. The session-log digest parity check (38) demonstrates that the anchored payload matches the frozen session log; validation records (42–43) evidence repeatability and release-level verification that altered or invalid records would be detected.

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.10(b) (Generate accurate complete copies — human readable + electronic form for FDA inspection)	**14, 17-18, 20, 38-39**	Post-verification audit logs (14), frozen per-folder audit logs (17–18), and the compiled session log (20) together provide human-readable (NDJSON/JSON) and machine-verifiable copies. Digest-match validation (38) and dual-ledger consistency (39) demonstrate that produced copies are complete and accurate and can be supplied to inspectors without transforming source evidence.
§11.10(c) (Protection of records — accurate ready retrieval throughout retention period)	**18, 20, 36-39**	Frozen audit logs (18) and the session log (20) are held under read-only/immutable controls, supporting durable local retention and ready retrieval. Blockchain anchors (36–37), digest-match validation (38), and dual-ledger checks (39) provide independent, long-term verifiability of record integrity and indexing without exposing content.
§11.10(d) (Limiting system access to authorized individuals)	**3, 21-26, 28**	Access is restricted to authenticated enterprise users (21) and registered reviewers (3, 22). A valid institutional HMAC session and a user e-signature are both required before a gate job is created (26). The FAIL/PASS tests (23–25) show fail-closed behavior; only authorized users advance to final anchoring authorization step (28).

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.10(e) (Secure computer-generated time-stamped audit trails — independently record date/time, no obscuring, retention)	**7, 14, 17-18, 20, 36-39**	OpenTimestamps (OTS) proofs (7), audit logs (14, 17–18), and the session log (20) capture computer-generated UTC timestamps for all key events. The dual-ledger record (39) maintains an append-only, time-sequenced trail; previous entries are never overwritten. Anchors (36–37) provide durable external time attestation; digest-match validation (38) preserves traceability from record → payload → TXID.
§11.10(f) (Operational system checks — enforce permitted sequencing)	**4 & 8, 6-7, 12-17, 19, 26, 28-29, 31-36, 39-41**	The software enforces a fixed order of operations: pre-checks (4), hashing/OTS (6–7), audit verification (8), mandatory user verification prior to logging (15–17, 19), gate-job creation only on multi-layer e-signature (26), and broadcast/confirmation (28–36), with state-machine transitions recorded in the dual ledger (39–41). Attempts to bypass steps are blocked by runtime checks; only sequenced events are accepted.
§11.10(g) (Authority checks — ensure only authorized individuals can use system, sign records, alter records)	**3, 21-26, 28**	Authority is dual-gated: (1) Institutional access via HMAC session (21) and (2) Individual approval via e-signature (3, 22). Evidence (23–25) shows that unauthorized or failed signings are rejected and do not create gate jobs; only authorized actions (26) can proceed to final anchoring (28).

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.10(h) (Device checks — determine validity of data input source)	**4 & 8, 6A, 7A, 15-16, 38-39, 42-43**	Device/input validity is enforced by accepting only frozen inputs from the controlled area documented by pre/post audits (4 & 8), by sidecar-exclusion and naming rules embedded in the audits, and by reproducibility testing (6A, 7A). PRE/POST screen-shots (15–16), digest-match (38), and dual-ledger checks (39) confirm that only permitted, verified inputs are processed. (Optional, non-biometric telemetry may flag automation risk but cannot ac-cept/deny; if triggered, a deterministic secondary verification is required.)
§11.10(i) (Personnel qualification — education, training, experience to perform assigned tasks)	**6A, 7A, 42-43**	Release-level validation records (42–43) and re-producibility audits (6A, 7A) evidence competent execution, review, and approval under the QMS (IQ/OQ/PQ). Training and role assignments for de-velopers/operators are managed within the QMS and are available under NDA; the artifacts here show qualified personnel performed and reviewed the validated runs.

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.10(j) (Written policies — accountability for electronic signature actions to deter falsification)	**3, 14, 20-26, 28, 37-41**	Each audit log (14) captures identity, UTC time, and meaning of each e-signature; session log compiles all audit logs, and enforces deterministic linking to prior sessions by recording anchor payload/txid (20); gates (22–26) bind actions to named users and institutional sessions. The pipeline (28) and on-chain receipts (37) record non-repudiable outcomes, while the dual-ledger trail (39–41) preserves who did what, when, consistent with written accountability policies under the QMS.
§11.10(k)(1) (Controls over systems documentation distribution, access, use)	**2, 18, 20, 27, 30, 33, 36-41**	Zero-custody, frozen archives (2, 18, 20) restrict modification and distribution of system records; gate-job and receipt artifacts (27, 30, 33) evidence controlled handoff from user to anchoring service. Anchors and ledger entries (36–41) provide traceable, read-only provenance, supporting governed access and use of system documentation.
§11.10(k)(2) (Revision/change control — audit trail documenting time-sequenced development/modification)	**6A, 7A, 42-43**	QMS records (42–43) document versioning, approvals, and release history; reproducibility runs (6A, 7A) are tied to specific versions/parameters, demonstrating that changes are evaluated, approved, and recorded in time sequence, with outputs independently repeatable.

§11.30 Controls for Open Systems — Evidence Mapping

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.30 (Open systems — procedures/controls ensuring authenticity, integrity, confidentiality including encryption + digital signature standards)	**4 & 8, 6-7, 15-16, 18, 36-41**	Authenticity and integrity are ensured by cryptographic digests (4, 6), pre/post execution audit confirming 1:1 file parity (8, 15–16), independent OTS time attestation (7), and on-chain OP_RETURN anchoring of proof-only payloads (36–37) that contain no source data or identifiers. Confidentiality is preserved by the zero-custody data flow (18, 20): only digests/receipts are transmitted; raw evidence never leaves the customer's environment. Gate-job and anchoring approvals are bound by an individual cryptographic e-signature (Ed25519) within an authenticated institutional session (21–22). Dual-ledger records and state-machine transitions (39–41) provide durable, tamper-evident provenance from creation to receipt.

§11.50 Signature Manifestations — Evidence Mapping

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.50(a)(1-3) (Signature manifestations — printed name, date/time, meaning clearly indicated)	**3, 14, 17, 20-22, 41**	Signature manifestations are captured and displayed in the approval workflow and records: the printed name/identity of the approver is recorded in the human-verifier/e-signature UI (3, 22) and written into the audit/session log entries (14, 17, 20); the UTC date/time of execution is stored with the signing record (14, 20, 41); and the meaning of the signature (e.g., review/approval/authorization) is explicitly logged in the same records (14, 20, 41).
§11.50(b) (Signature information subject to same controls as electronic records)	**18, 27, 30, 39**	Signature information (approver identity, UTC time, meaning, and associated proof digests) is stored within the same frozen audit/session artifacts (18) and gate-job/receipt trail (27, 30) that are protected by the system's append-only dual-ledger controls (39). Thus, signature data is subject to identical integrity, retention, and retrieval controls as other electronic records.

§11.70 Signature/Record Linking — Evidence Mapping

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.70 (Signature/record linking — signatures cannot be excised, copied, transferred to falsify records)	**14, 17-18, 20-22, 36-41**	The e-signature event (identity, UTC time, meaning) is stored inside the same audit/session log that hashed and anchored (14, 17–18, 20–22). The anchored payload derives from the frozen session log digest, so any attempt to remove, re-use, or alter a signature or its record breaks digest parity and is detectable via digest-match validation (38) and dual-ledger checks (39–41). Linking is therefore cryptographic and permanent.

§11.100 General Requirements — Evidence Mapping

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.100(a) (Electronic signature uniqueness — unique to one individual, not reused/reassigned)	**3, 21-22**	Each approver is provisioned a unique user identity under the customer's enterprise controls (21) and an individual cryptographic signing credential (Ed25519) used at the e-signature gate (3, 22). Under account/credential lifecycle procedures (QMS), keys are not reassigned, and de-provisioning occurs on role changes, maintaining one-to-one association between individual and electronic signature.

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.100(b) (Identity verification before establishing electronic signature)	**3, 21-26**	Identity is verified before electronic signature use via the customer's institutional authentication (21) and issuance of the individual signing credential (3, 22). At runtime, signature execution occurs within an authenticated institutional session (21–22). (Optional, non-biometric telemetry may be enabled as a supplemental fraud-prevention signal; it does not perform identity proofing and cannot accept/deny.)

§11.200 Electronic Signature Components and Controls — Evidence Mapping

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.200(a)(1)(i) (Two distinct identification components — first signing uses all components, subsequent use at least one component)	**3, 21-22**	AuditLog.AI uses two distinct components: (1) Institutional authentication (21) to establish a controlled access session, and (2) an individual cryptographic signing component (Ed25519) (3, 22). The first signing in a continuous session uses both components; subsequent signings within that session use at least the individual signing component, which is executable only by the individual.
§11.200(a)(2) (Signatures used only by genuine owners)	**3, 21-26**	Genuine use is enforced by private key custody (Ed25519 signing at 22–26) combined with institutional session controls (21). Only the key holder can produce the individual signature, and only authenticated users can initiate a gate-job; attempts without the rightful holder fail closed (23–25).

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.200(a)(3) (Attempted use by non-owner requires collaboration of two or more individuals)	**3, 21-22**	Because signature execution requires both a valid institutional session (21) and the individual's private signing key (3, 22), a non-owner would need to compromise two separate control domains (enterprise identity and individual key custody). Organizational policy segregates these controls, so attempted misuse typically requires collusion or multi-control compromise, aligning with §11.200(a)(3).

§11.300 Controls for Identification Codes/Passwords — Evidence Mapping

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.300(a) (Uniqueness of combined identification code and password)	**3, 21-22**	Uniqueness is maintained by enterprise user IDs/credentials (21) and per-individual signing keys (3,22). The combined factors (institutional access + personal signing credential) are unique to each individual and managed under QMS issuance, rotation, and de-provisioning procedures.

Clause	Dossier Evidence #	Relevance to AuditLog.AI Software
§11.300(d) (Transaction safeguards — prevent unauthorized use, detect/report attempts)	**3, 21-26**	The e-signature gate implements fail-closed safeguards: unauthorized or failed sign attempts are blocked (23–25), recorded with UTC time and reason, and do not create a gate-job. Authorized events proceed to gate-job creation (26) and are reflected in the dual-ledger trail (33–39) for rapid detection, investigation, and reporting. (Optional telemetry, when enabled, can trigger secondary deterministic verification; it does not approve/deny on its own.)

*Section II: EMA Annex 11 + GCP Guideline Integration (2023) *

Official Reference Files:

`annex11_01-2011_en_0___20251020T193619Z.pdf`, `mp_vol4_chap4_annex11_consultation_guideline_en___20251020T193619Z.pdf`, `guideline-computerised-systems-and-electronic-data-clinical-trials_en___20251020T193619Z.pdf`

Annex 11 Section; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
Validation (§4); Validation documentation covering relevant lifecycle steps; manufacturers should justify standards, protocols, acceptance criteria based on risk assessment	**6-7, 42-43**	Validation is demonstrated end-to-end: deterministic hashing + OTS generation (6–7) show repeatable, intended behavior; release/change control, IQ/OQ/PQ, and version locking are documented under the Sentinel QMS (42–43), keeping the application validated and the IT/ops environment qualified. This aligns with Annex 11's principle that the application should be validated; IT infrastructure should be qualified and with the EMA GCP guideline's dedicated "Validation of systems" and Annex 2 validation controls.
Accuracy Checks (§6); For critical data entered manually, additional check on accuracy by second operator or validated electronic means; risk management of erroneous data consequences	**4 & 8, 38-39**	Pre-Hasher Execution Audit (4) establishes the baseline inventory; Post-Hasher Verification (8) confirms 1:1 parity between manifest rows and produced digests; Session Log Digest Match (38) and dual-ledger consistency (39) provide a validated electronic cross-check that would detect any divergence. This satisfies Annex 11 §6 and mirrors the EMA GCP guideline expectations for edit checks/audit-trail review.

Annex 11 Section; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
Data Storage (§7); Data secured by physical and electronic means against damage; stored data checked for accessibility, readability, and accuracy; access ensured throughout the retention period	**6, 18, 20, 36–39, 41**	AuditLog.AI secures all records through: (1) tamper-evident dual-hash cryptography (Evidence 6 & 38: SHA-256 + RIPEMD-160 verifying byte-level integrity); (2) frozen copies with read-only and immutable filesystem controls (Evidence 18: `chmod 444` + `chflags uchg`); (3) dual-ledger atomic consistency between user and master ledgers (Evidence 39); (4) session-log compilation linking each audit log to the previous session's blockchain anchor (Evidence 20 & 41); and (5) Bitcoin OP_RETURN anchoring (Evidence 36–37) providing permanent public proof of existence. Together these controls satisfy EMA Annex 11 §7 requirements for secure storage, accessibility, and data integrity throughout the defined retention period.
Audit Trails (§9); System-generated record of all GMP-relevant changes and deletions; reasons documented; audit trails available in intelligible form and regularly reviewed	**7, 14, 17-18, 20, 36-39**	AuditLog.AI produces secure, time-stamped audit records (OTS 7; session/audit logs 14, 17–18, 20) and on-chain receipts (36–37); dual-ledger events with state transitions (39) present an intelligible, append-only trail reviewed during validation and periodic evaluation. Rationale/updates are captured in the logs, consistent with EMA's definitions and review expectations for audit trails.

Annex 11 Section; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
Change and Configuration Management (§10); Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	**6-7, 42-43**	Change control is executed under the QMS (42–43): requests, impact/risk assessment, testing, approval, versioning, and release records (with reproducibility checks 6–7). This aligns with EMA GCP guideline A2.10 "Change control".
Periodic Evaluation (§11); Computerised systems should be periodically evaluated to confirm valid state and GMP compliance; evaluations include functionality, deviation records, incidents, performance, reliability, security, validation status	**6A, 7A, 42-43**	Reproducibility audits (6A, 7A) and QMS periodic reviews (42–43) confirm the system remains in a validated state; results and any actions are documented and version-locked. This implements EMA GCP guideline A2.9 "Periodic review".
Security (§12); Physical/logical controls restricting access to authorized persons; methods include passwords, biometrics; extent depends on criticality; access authorization changes recorded; identity of operators entering/changing data recorded with date/time	**3, 21-26, 28**	Access is limited to authorized users via institutional authentication and e-signature gates (3, 21–26); operator identity, UTC time, and signature meaning are linked in the record; optional non-biometric telemetry (Layer 3) may trigger step-up verification but never alone approves/denies. Controls map to EMA security standards and GCP 5.4 "Security and access control".
Electronic Signature (§14); Electronic signatures are expected to: a) have the same impact as handwritten; b) permanently linked to their respective record; c) include the time and date	**3, 14, 20-22**	Electronic signatures are captured with unique user identity + time + meaning, and permanently linked in the session/gate-job records (14, 20–22). Timestamps are system-generated and non-manipulable; full signature information remains accessible (user-held) for review—consistent with EMA's e-signature and timestamp expectations.

Annex 11 Section; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
Business Continuity (§16); For systems supporting critical processes, provisions ensuring continuity in event of breakdown; alternative arrangements (manual/alternative system) documented and tested; recovery time based on risk	**6A, 7A, 42-43**	Zero-custody design plus independent OTS and on-chain receipts enable offline re-verification; reproducibility audits (6A, 7A) and QMS procedures (42–43) ensure reproducibility independent of AuditLog.AI tools.
Archiving (§17); Data may be archived; archived data checked for accessibility, readability, integrity; if system changes, data must remain readable	**14, 17-18, 20, 38-39**	Frozen archives (17–18) preserve readability and integrity; audit and session logs (14, 20) remain verifiable via digest-match (38) and ledger receipts (39). EMA requires retention of dynamic data (e.g., audit trails) in dynamic form—met via NDJSON/JSON logs, accompanying frozen copies and OTS/BTC receipts.

EMA Clinical Trials Guideline (2023) — Supplementary Evidence Mapping

Guideline Section	Dossier Evidence #	Relevance to AuditLog.AI Software
§5.5 Timestamp (UTC + External Standard)	**15–16, 7–7A, 36–38**	AuditLog.AI fulfills the timestamp requirement through PRE/POST execution UTC records (Evidence 15–16: `PRE_20251014T193659Z` / `POST_20251014T193727Z`, Δ=28 s verified timeline) combined with independent external standards — OpenTimestamps proofs (Evidence 7–7A) and Bitcoin anchoring (Evidence 36–38). Together these ensure unambiguous, verifiable UTC timing synchronized to an external, decentralized standard, meeting EMA §5.5 requirements for accuracy, traceability, and time-zone transparency.

Guideline Section	Dossier Evidence #	Relevance to AuditLog.AI Software
§6.6 Control of Data (Recognition of Public Blockchain)	**36–38**	AuditLog.AI anchors anonymized, tamper-evident cryptographic digests of each session log (Evidence 38) onto the Bitcoin mainnet using OP_RETURN payloads (Evidence 36–37: TXID `9a46014d657726798449c-c6282de083e2084afc87aa5f23233903396d73b8d4f`, Block 919082). This implementation provides "verifiability of data (transactions) by an independent (distributed) tamper-proof ledger" explicitly recognized under EMA §6.6 as offering "comparable security to a system maintained by an independent service provider". The blockchain-based audit trail thereby satisfies the EMA's requirement for independent, tamper-proof data verification and integrity assurance.

Section III: TGA / PIC/S PE 009-17 — Harmonized Matrix

Official Reference Files:

`pe-009-17-gmp-guide-xannexes___20251020T193619Z.pdf`,
`Concept Paper on the Revision of Annex 11 of the Guidelines on Good Manufacturing Practice for Medicinal Products  Computerised Systems___20251020T193619Z.pdf` **NOTE:** Australia (TGA) adopts PIC/S PE 009-17 as GMP standard. PIC/S Annex 11 uses titled sections aligning with EMA Annex 11 structure.

PIC/S Annex 11 Section	Dossier Evidence #	Relevance to AuditLog.AI Software
Validation (Project Phase 4. page 170)	**6, 7, 12–14, 42–43, 6A, 7A**	Risk-based validation is demonstrated across hasher + OTS runtime (6–7), VALIS prompts/logs and the AuditLog Generated record (12–14), with formal QMS validation & pre-deployment/production audits (42–43). Reproducibility and stress tests (6A, 7A) evidence suitable test methods/acceptance criteria and lifecycle verification per §4.1–4.8.
Accuracy (Operational Phase 6. page 171)	**4 & 8, 6, 13, 38**	Pre-Hasher Execution Audit (4) establishes the baseline; Post-Hasher Verification (8) confirms 1:1 parity between manifest rows and generated digests; dual-hasher runtime (6) and per-folder VALIS logs (13) provide validated electronic checks; Session Log Digest Match Validation (38) verifies parity at session level—fulfilling the second operator or validated electronic means control.

PIC/S Annex 11 Section	Dossier Evidence #	Relevance to AuditLog.AI Software
Data Storage (Operational Phase 7. page 171)	**18, 20, 36–39, 42–43**	Frozen copies (18) apply read-only + immutable flags for integrity; Session Log (20) ensures accessibility/readability; on-chain receipts and dual-ledger (36–39) add durable, independently verifiable provenance; QMS validation records (42–43) cover restore/periodic checks expected under §7.2.
Audit Trails (Operational Phase 9. page 171)	**20, 33–39, 41**	Session Log (20) and AMPLIFY Ledger state-machine records (33–39) capture date/time, reasoned events, and transitions; Final Anchor Event (41) closes the trail. All artifacts are available in intelligible form and are reviewable—consistent with §9.
Change & Configuration Management (Operational Phase 10. page 171)	**42–43, 6A, 7A**	QMS change control and configuration management are evidenced in pre-public deployment audits and runtime integrity provenance (42–43). Reproducibility audits (6A, 7A) support controlled modification and verification of the validated state.
Periodic Evaluation (Operational Phase 11. page 171)	**6A, 7A, 42–43**	Periodic evaluations are satisfied by scheduled reproducibility runs (6A, 7A) and QMS-tracked reviews (42–43) covering performance/reliability/security and validation status per §11.

PIC/S Annex 11 Section	Dossier Evidence #	Relevance to AuditLog.AI Software
Security (Operational Phase 12. page 172)	**3, 21–26, 20, 18**	Layer 1–2 identity controls: institutional authentication (21) + cryptographic e-signature (3, 22, 25–26). Layer 3 (optional): non-biometric human-activity verification in the Signature Gate (22–26) as a fraud-prevention signal. All signature actions are linked in Session Log (20) with UTC time; frozen archives (18) protect records at rest. Meets access restriction, authorization lifecycle, and operator identity/time recording.
Electronic Signature (Operational Phase 14. page 172)	**3, 14, 20–22, 26**	Electronic signatures have the same impact as hand-written (policy/QMS), are permanently linked to their records via gate_job/session artifacts (14, 20–22, 26), and include date/time (20, 26), satisfying §14(a)–(c).
Business Continuity (Operational Phasepage 16. 172)	**18, 36–39, 42–43**	Continuity is supported by frozen local artifacts (18), independent public anchoring + dual ledger (36–39) for off-site verifiability, and documented contingency/restore validation within QMS audits (42–43), as required by §16.
Archiving (Operational Phase 17. page 173)	**14, 17–18, 20, 38–39**	Authorized VALIS logs per folder (17), frozen archives (18), and session log with cross-references to prior anchors (20) ensure accessibility/readability/integrity; digest-match (38) and dual-ledger (39) preserve retrievability across system changes per §17.

Section IV: PCAOB AS 1215 / AS 1105 — Audit Documentation & Evidence

Official Reference Files:

`auditing_standards_audits_fybeginning_on_or_after_december_15_2024.pdf`, `2024-007-adoptingrelease.pdf`, `pcaob-release-no-2025-004.pdf`

AS 1215 (Audit Documentation) — Evidence Mapping

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶.04; p.60; Requirements; **Documentation Requirement:** "The auditor must prepare audit documentation in connection with each engagement conducted pursuant to the standards of the PCAOB. Audit documentation should be prepared in sufficient detail to provide a clear understanding of its purpose, source, and the conclusions reached"	**14, 20, 33–39**	**Self-documenting record set:** *AuditLog Generated Post-Verification* (14) and *Session Log View* (20) capture purpose, inputs, approver identity, UTC times, digests, and outcome; *AMPLIFY ledger + anchor receipts* (33–39) show the end-to-end conclusion (e.g., `ANCHORED_RECEIPT_WRITTEN`) and source traceability via TXID/OP_RETURN payloads.
¶.06; p.60; Requirements; **Work Performed:** "The auditor must document the procedures performed, evidence obtained, and conclusions reached with respect to relevant financial statement assertions. Audit documentation must clearly demonstrate that the work was in fact performed"	**6–7, 12–14, 15–16, 33–39**	**Work actually performed is provable:** runtime hashing (6), OTS attestation (7), VALIS prompts and per-folder logs (12–13), generated audit record post-verification (14), PRE/POST execution captures (15–16) and the dual ledgers + Bitcoin chain (33–39) together show the procedures, the evidence produced (digests/OTS/TXID) and the final conclusion state.

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶.06A; p.60; Requirements; **Experienced Auditor Test:** "Audit documentation must contain sufficient information to enable an experienced auditor, having no previous connection with the engagement: (a) To understand the nature, timing, extent, and results of the procedures performed, evidence obtained, and conclusions reached, and (b) To determine who performed the work and the date such work was completed as well as the person or persons who reviewed the work and the date of such review"	**14, 20–22, 26, 33–39**	**Reconstructible without oral explanation:** (14) and (20) present the compiled session and chain-of-custody; access/auth and e-signature gating (21–22, 26) identify **who** approved **when** (UTC) and **for what**; the ledger and anchor receipts (33–39) fix timing/extent/results and reviewers/approvers in a durable record.
¶.07; p.60-61; Requirements; **Documentation Factors:** "In determining the nature and extent of the documentation... the auditor should consider... Nature of the auditing procedure; Risk of material misstatement; Extent of judgment required; Significance of the evidence; Responsibility to document conclusion not readily determinable"	**12–13, 18, 42–43**	**Risk-proportionate documentation:** VALIS gating & per-folder output (12–13) detail what is documented and why; frozen, read-only artifacts (18) preserve significant items; QMS/validation and pre-public deployment audits (42–43) evidence the risk-based selection, testing depth, and rationale behind documentation sufficiency.
¶.09; p.61; Requirements; **Presumption if Documentation Absent:** "If... the auditor becomes aware... that audit procedures may not have been performed... the auditor must determine, and if so demonstrate, that sufficient procedures were performed... To accomplish this, the auditor must have persuasive other evidence. Oral explanation alone does not constitute persuasive other evidence"	**33–39, 36–37, 38**	**Persuasive, independent corroboration:** public-chain receipts and payload parity (36–37), session-to-anchor digest match (38), and the append-only AMPLIFY ledger (33–39) provide third-party-verifiable proof of performance and results—removing reliance on oral explanation.

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶.12; p.62; Requirements; **Significant Findings Documentation:** "The auditor must document significant findings or issues, actions taken to address them (including additional evidence obtained), and the basis for the conclusions reached... Significant findings include: (a) Significant accounting matters; (b) Results indicating need for significant modification of planned procedures; (c) Audit adjustments; (d) Disagreements among engagement team; (e) Circumstances causing significant difficulty; (f) Significant changes in assessed audit risk; (g) Matters that could result in modification of auditor's report"	**20, 33–39, 40**	**Issue → action → conclusion, all recorded:** session log (20) and ledgers (33–39) capture significant events and decisions; *LLM3 correction disclosure* (40) documents the issue, the reason, corrective action, and resultant conclusion with dates and author, as required.
¶.14; p.64; Retention of and Subsequent Changes to Audit Documentation; **Retention Period:** The auditor must **retain audit documentation for seven years** from the date the auditor grants permission to use the auditor's report (report release date), unless a longer period is required by law.	**17–18, 20, 36–39**	**Durable retention & retrievability:** frozen archives with file-system immutability (17–18) + session log (20) + Bitcoin mainnet anchoring/receipts (36–39) ensure records remain complete, readable, and retrievable for (≥) the retention period.
¶.15; p.64; Retention of and Subsequent Changes to Audit Documentation; **Assembly Deadline (Documentation Completion Date):** A complete and final set of audit documentation should be assembled for retention (archived) as of a date not more than **14 days** after the report release date.	**15–16, 18, 33–39**	**Timely assembly by design:** PRE/POST evidence (15–16) and frozen artifacts (18) are generated contemporaneously; ledger/receipts (33–39) timestamp completion—demonstrating assembly well within the 14-day window.

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶.16; p.64; Retention of and Subsequent Changes to Audit Documentation; **Post-Assembly Changes:** Audit documentation must **not be deleted or discarded** after the documentation completion date. Any additions must indicate the date, who made them, and the **specific reasons for the changes**.	**17–18, 33–39, 40**	**Immutable baseline + controlled amendments:** frozen, read-only artifacts (17–18) and append-only ledgers (33–39) prevent deletion/obscuring; late additions (40) explicitly show date, author, and reason—preserving the full change history.

AS 1105 (Audit Evidence) — Evidence Mapping

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶.01; p.18; Introduction; **Objective:** "This standard explains what constitutes audit evidence and establishes requirements regarding designing and performing audit procedures to obtain sufficient appropriate audit evidence"	**2, 4, 6–7, 8, 15–16, 20, 36–39**	The core evidence set spans the full lifecycle: zero-custody baseline (2), pre/post inventory & parity checks (4, 8, 15–16), dual-hash + OTS proofs and compiled session record (6–7, 20), and independent, public blockchain anchoring with dual-ledger receipts (36–39), collectively constituting sufficient, appropriate audit evidence for provenance and integrity.
¶.04; p.19; Requirements; **Design Procedures:** "The auditor must design and perform audit procedures in a manner that addresses the assessed risks of material misstatement for each relevant assertion of each significant account and disclosure"	**12–13, 18, 20, 21–26, 28, 33–39**	Procedures and controls are embedded and evidenced: VALIS prompts and per-folder logs (12–13), frozen audit logs (18), session manifest with linkage to prior anchor (20), multi-factor access + human-signature gate (21–26, 28), and ordered state-machine transitions in the AMPLIFY ledger (33–39) enforcing correct sequencing and approvals.

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶.06 ; p.19; Requirements; **Sufficient Appropriate Audit Evidence:** "The auditor must obtain sufficient appropriate evidence on which to base the audit opinion. To be appropriate, evidence must be both relevant and reliable"	**2, 4, 6–7, 8, 20, 36–39, 6A, 7A, 42-43**	Relevance: session-scoped evidence mapped to specific approvals and timestamps (20). Reliability: cryptographic dual-hash + OTS (6–7), pre/post parity (4, 8), immutable anchoring + confirmations (36–39), zero-custody separation (2), and reproducibility audits (6A, 7A, 42-43) demonstrating repeatable verification by independent validators.
¶.10; p.20; Using Information Produced by the Company (IPC); **IPC Reliability Check (Accuracy/Completeness/Detail):** When using information produced by the company as audit evidence, the auditor must evaluate sufficiency and appropriateness by performing procedures to: (1) **Test accuracy and completeness** of the information, or **test controls** over accuracy/completeness (including ITGCs/AAPs where applicable); AND (2) Evaluate whether the information is sufficiently **precise and detailed** for purposes of the audit.	**4, 8, 12–13, 18, 20, 33–39, 38**	Accuracy/completeness: pre/post inventories and parity (4, 8, 38). Tested controls: VALIS enforcement + frozen, read-only logs (12–13, 18). Precision/detail: session_log and session_global include per-artifact hashes, timestamps, approver identity, prior-anchor linkage (20). Dual-ledger writes + ordered states provide control testing evidence (33–39).

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶.10A; p.17; Requirements; **External Electronic Information (Effective Dec 15, 2025):** "When using [external electronic information provided by the company] as audit evidence, the auditor should evaluate whether the information is reliable by: (a) Obtaining an understanding of (i) the source from which the company received the information; and (ii) the company's process by which such information was received, maintained, and processed; (b) Testing the information... or testing controls over receiving, maintaining, and processing the information"	**27, 30, 33, 36–38, 39, 41**	Source/process: gate job (hashes-only) creation (27), incoming anchor receipt (30), AMPLIFY watcher/ledger describing broadcast and confirmation flow (33, 39), final anchor event (41). Testing/ controls: independent explorer views and TX confirmations (36–38) tied to the exact OP_RETURN payload; dual-ledger consistency (39) demonstrates controls over receiving/maintaining/ processing the external info.
AS 1105.10A Policy; p.2; Policy; **Remote Possibility Exception:** "If... the auditor concludes that there is no more than a remote possibility that the information used as audit evidence has been modified in a way that would render it unreliable for purposes of the audit, the PCAOB will not... treat the absence of any separate testing specified in paragraph .10A(b) as noncompliance"	**6–7, 20, 36–39, 6A, 7A, 42–43**	AuditLog.AI's design makes undetected modification remote: (i) strong cryptographic binding of session content (6–7, 20), (ii) public mainnet confirmations + payload parity (36–38), (iii) dual-ledger atomic writes (39), and (iv) documented validation & reproducibility audits (6A, 7A, 42–43). Together these support an auditor's conclusion that additional separate testing may be unnecessary under the Policy's threshold (final judgment remains with the auditor).

Section V: ISA 230 / ISA 500 / ISA 240 (Revised 2025) — International Assurance Alignment

Official Reference Files:

`isa-230.pdf`, `isa-500_en.pdf`, `IAASB-ISA-240-Revised-Fraud.pdf`

ISA 230 (Audit Documentation) — Evidence Mapping

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶7; p.155; Requirements; **Timely Preparation:** "The auditor shall prepare audit documentation on a timely basis"	**14, 15–16, 20, 41**	System-generated **AuditLog** on completion (14) plus **PRE/POST mandatory screenshots** (Δ=28s, 15–16) show contemporaneous capture; **Session Log view** (20) is produced automatically at run-end; **Final Anchor Event** (41) closes the record set within the same runtime, evidencing timely preparation.

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶8; p.156; Requirements; **Experienced Auditor Test:** The auditor shall prepare audit documentation that is sufficient to enable an experienced auditor, having no previous connection with the audit, to understand: (a) The nature, timing and extent of the audit procedures performed; (b) The results of the audit procedures performed, and the audit evidence obtained; (c) Significant matters arising during the audit, the conclusions reached thereon, and significant professional judgments	**20, 33–39, 15–16**	An experienced auditor can reconstruct the work from the **Session Log with approver, UTC, digests** (20), **dual-ledgers / blockchain artifacts** (33–39) and the **PRE/POST pair** (15–16) showing nature, timing, extent, results, conclusions, and who did what/when.
¶9; p.156; Requirements; **Documentation Elements:** (a) The identifying characteristics of the specific items or matters tested; (b) Who performed the audit work and the date such work was completed; (c) Who reviewed the audit work performed and the date and extent of such review	**20, 14, 21–26, 33–39**	**Identifying characteristics & items tested**: session entries + manifest (20). **Who performed & when**: approver identity + UTC in (14) and **Human-Signature Gate / login** (21–26). **Review/approval*****: gate_job creation + ***AMPLIFY ledger state transitions** with timestamps (33–39) record reviewer/approval moments.
¶14; p.157; Requirements; **Assembly Deadline:** The auditor shall assemble the audit documentation in an audit file and complete the administrative process of assembling the final audit file on a timely basis after the date of the auditor's report	**17–20, 41, 42**	**Frozen archives** (17–20) evidence assembly into a complete file; **Final Anchor Event** (41) marks closure; **QMS/Pre-Public Deployment Audit Log** (42) defines and documents the assembly procedure and control.

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶15; p.157; Requirements; **Retention Prohibition:** After the assembly of the final audit file has been completed, the auditor shall not delete or discard audit documentation of any nature before the end of its retention period	**17–20, 39, 40**	**Read-only / immutable** controls on frozen archives (17–20) prevent deletion; **Dual-ledger consistency** (39) detects any divergence; **Post-assembly change log** (40) documents reasons/dates for any permitted additions, satisfying prohibition on alteration/discard.
¶A5; p.158; Application; **Oral Explanation Prohibition:** Oral explanations by the auditor, on their own, do not represent adequate support for the work the auditor performed or conclusions the auditor reached, but may be used to explain or clarify information contained in the audit documentation	**20, 33–39, 36–38, 38**	The dossier is **self-documenting**: **Session Log** (20), **dual ledgers + TXID receipts** (33–39), **public explorer views** (36–38), and **Session-digest-to-anchor match** (38) obviate reliance on oral explanation.
¶A21; p.164; Application; **60-Day Assembly:** An appropriate time limit within which to complete the assembly of the final audit file is ordinarily not more than 60 days after the date of the auditor's report	**17–20, 41, 42–43**	**Frozen archives** (17–20) and **Final anchor** (41) evidence assembly; **QMS controls** (42) set the timeline; **Runtime validation dossier** (43) shows environment in validated state at release, supporting on-time completion.
¶A23; p.164; Application; **5-Year Retention:** The retention period for audit engagements ordinarily is no shorter than five years from the date of the auditor's report	**17–20, 33–39, 36–38, 42**	**Read-only frozen archives** (17–20) + **on-chain permanence/receipts** (33–39, 36–38) provide enduring availability; **QMS** (42) defines retention responsibilities and access during the retention period.

ISA 500 (Audit Evidence) — Evidence Mapping

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶4; p.362; Objective; **Objective:** The objective of the auditor is to design and perform audit procedures in such a way as to enable the auditor to obtain sufficient appropriate audit evidence to be able to draw reasonable conclusions on which to base the auditor's opinion	**4 & 8, 6–7, 12–13, 20, 33–39, 42–43**	The end-to-end pipeline is explicitly designed to obtain sufficient appropriate evidence: pre/post execution audits (4, 8) feed dual-hash + OTS processing (6–7); VALIS controls (12–13) enforce completeness/accuracy; the compiled session log (20) captures results and linkages; AMPLIFY/Bitcoin artifacts (33–39) provide independent persistence; QMS validation/traceability (42–43) documents lifecycle controls.
¶5(b); p.362; Definitions; **Appropriateness Definition:** Appropriateness (of audit evidence) – The measure of the quality of audit evidence; that is, its relevance and its reliability in providing support for the conclusions on which the auditor's opinion is based	**6–7, 15–16, 20, 36–38, 39**	Quality is established by cryptographic integrity (6) + independent time attestation (7); PRE/POST screenshots show correct context and timing (15–16); relevance is bound to the specific session via manifest + metadata (20); reliability is elevated by external, public blockchain anchors (36–38) cross-checked against the dual-ledger (39).
¶5(f); p.362; Definitions; **Sufficiency Definition:** Sufficiency (of audit evidence) – The measure of the quantity of audit evidence. The quantity of the audit evidence needed is affected by the auditor's assessment of the risks of material misstatement and also by the quality of such audit evidence	**4, 8, 12–13, 18, 20, 6A**	Quantity is evidenced by the pre/post hasher audits demonstrating 1:1 parity (4, 8), folder-level VALIS logs that enumerate every input (12–13), frozen archives preserving the full set (18), and the session manifest with per-file digests (20). Stress-test/reproducibility runs (6A) demonstrate capacity and repeatability at scale.

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶6; p.363; Requirements; **Design Procedures:** The auditor shall design and perform audit procedures that are appropriate in the circumstances for the purpose of obtaining sufficient appropriate audit evidence	**4, 6–7, 8, 12–13, 20, 33–39, 42–43**	Procedures are risk-aligned and deterministic: parity checks (4, 8), dual-hash + OTS (6–7), VALIS enforcement (12–13), session compilation with acceptance checks (20), state-machine-controlled anchoring and confirmations (33–39), and QMS validation/controls (42–43).
¶7; p.363; Requirements; **Relevance and Reliability:** When designing and performing audit procedures, the auditor shall consider the relevance and reliability of the information to be used as audit evidence, including information obtained from an external information source	**7, 36–38, 39**	External reliability is provided by OpenTimestamps (7) and public Bitcoin mainnet anchors (36–38); cross-verification against the user + AuditLog.AI dual-ledger (39) evidences that external data agree with internal records.
¶9; p.363; Requirements; **Entity-Produced Information:** When using information produced by the entity, the auditor shall evaluate whether the information is sufficiently reliable for the auditor's purposes, including, as necessary in the circumstances: (a) Obtaining audit evidence about the accuracy and completeness of the information	**4, 8, 12–14, 20, 38**	Entity-produced logs are validated by parity audits (4, 8) and VALIS controls (12–13); the AuditLog generated post-verification record (14) and session manifest (20) capture full lineage; digest-match verification (38) proves that the compiled record exactly corresponds to the anchored payload.
¶A8; p.365; Application; **Sufficiency-Appropriateness Interrelation:** The sufficiency and appropriateness of audit evidence are interrelated. Sufficiency is the measure of the quantity of audit evidence... Appropriateness is the measure of the quality of audit evidence... Obtaining more audit evidence, however, may not compensate for its poor quality	**12–13, 20, 6–7, 36–38**	The system balances quantity (VALIS enumeration and manifest coverage: 12–13, 20) with quality (cryptographic/OTS proofs and public anchors: 6–7, 36–38), showing why more evidence is unnecessary when higher-quality external proofs exist.

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶A9; p.365; Application; **Reliability Factors:** Appropriateness is the measure of the quality of audit evidence; that is, its relevance and its reliability in providing support for the conclusions... The reliability of evidence is influenced by its source and by its nature, and is dependent on the individual circumstances under which it is obtained	**2, 18, 20, 27, 30, 36–38, 39, 7A**	Source/nature are evidenced by zero-custody provenance (2, 27, 30), frozen read-only archives (18) and session context (20); circumstances are independently corroborated on Bitcoin mainnet (36–38) and reconciled via dual-ledger controls (39). OTS reproducibility audits (7A) further support credibility of the external time source.
¶A30-A38; p.368; Application; **Reliability Hierarchy:** External evidence more reliable than internal; documentary evidence more reliable than oral; original evidence more reliable than copies	**36–38, 7, 18, 20, 33–39**	External documentary originals: public TXIDs/ OP_RETURN payloads (36–38) and OTS proofs (7). Internal records: frozen originals and manifest (18, 20). Cross-checks: append-only ledgers and public blockchain confirmations (33–39). This suite meets the reliability hierarchy.
¶A43; p.370; Application; **Single Provider Assessment:** In some situations, there may be only one provider of certain information... the nature and extent of audit procedures that may be appropriate in the circumstances is influenced by the nature and credibility of the source of the information	**33–39, 6A, 7A, 36–38**	Where a single internal provider exists (system logs), controls are tested via dual-ledger atomicity and state transitions (33–39) and by independent external anchors (36–38). Reproducibility campaigns (6A, 7A) provide additional assurance on source credibility and the controls over receiving/ maintaining/processing the information.

ISA 240 (Revised) (Fraud Responsibilities) — Evidence Mapping

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶12; p.10; Introduction; **Professional Skepticism and Professional Judgment:** It is important that the auditor maintain professional skepticism throughout the audit, considering the potential for management override of controls, and recognizing that audit procedures that are effective for detecting error may not be effective in detecting fraud	**15–16, 18, 20, 33–39, 6A, 7A**	Immutable, computer-generated proofs (PRE/POST screenshots with Δ<300s; frozen archives; session log with dual-hash + OTS; dual-ledger + Bitcoin anchors) reduce reliance on oral explanations and support skeptical evaluation; reproducibility audits (6A, 7A) evidence consistent results over time.
¶19; p.12; Requirements; **Professional Skepticism:** In applying ISA 200, the auditor shall maintain professional skepticism throughout the audit, recognizing the possibility that a material misstatement due to fraud could exist	**4 & 8, 20, 36–39, 6A, 7A, 38, 42-43**	Pre/Post-Hasher audits (4, 8) and session log (20) expose any mismatch (38); external, independently verifiable anchors (36–39) plus reproducibility suites (6A, 7A, 42-43) provide corroborative, third-party-verifiable evidence consistent with skeptical inquiry.
¶20; p.12; Requirements; **Remain Alert:** "The auditor shall remain alert throughout the audit for information that indicates that one or more fraud risk factors are present and circumstances that may be indicative of fraud or suspected fraud"	**22–26, 23–24, 33–39**	e-Signature Gate records PASS/FAIL outcomes (22–26) and **blocked attempts** (23–24). State-machine ledger entries (33–39) time-stamp all attempts and outcomes, supporting alerting and detection of anomalous authorization patterns.
¶22; p.12; Requirements; **Document Authenticity:** If conditions identified during the audit cause the auditor to believe that a record or document may not be authentic or that terms in a document have been modified but not disclosed to the auditor, the auditor shall investigate further	**18, 20, 27, 30, 36–38, 38**	Frozen archives (18) + session log (20) enable immediate re-hashing; gate job (27) → incoming receipt (30) → public TXIDs (36–37) + **digest-to-payload parity** (38) allow definitive authenticity checks without raw-data disclosure.

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶29(a)(iv); p.13-14; Requirements; **Management Override Discussion:** Engagement team discussion shall include... An exchange of ideas about... How management may be able to override controls	**3, 21, 22–26, 33–39, 24**	Controls require institutional login (21) **and** Ed25519 e-signature (3, 22); optional Layer-3 human-activity check can be enabled per policy (23-26). Fail-closed event (24) shows override attempts are blocked. Ledger state machine (33–39) prevents out-of-sequence actions.
¶32(a)(i); p.14; Requirements; **Culture and Integrity:** Obtain an understanding of: How management's oversight responsibilities are carried out, such as the entity's culture and management's commitment to integrity and ethical values	**42, 43, 33–39, 20**	QMS and pre-deployment audit (42) + live runtime integrity provenance (43) demonstrate governance; append-only dual-ledgers (33–39) and session log (20) evidence traceable accountability and oversight posture.
¶42; p.17; Requirements; **Respond to Assessed Risks:** The auditor shall design and implement overall responses to address the assessed risks of material misstatement due to fraud at the financial statement level	**6–7, 12–14, 18, 20, 33–39, 6A, 7A**	Risk responses are embedded as controls: dual-hashing + OTS (6–7), VALIS enforcement and post-verification record (12–14), frozen archives (18), linked session log (20), dual-ledger anchoring (33–39), and periodic reproducibility audits (6A, 7A).
¶48-49; p.18; Requirements; **Journal Entry Testing:** The auditor shall design and perform audit procedures to test the appropriateness of journal entries recorded in the general ledger and other adjustments made in the preparation of the financial statements	**4 & 8, 6, 20, 38**	For financial-audit contexts, **manifest-to-hash parity** (4, 8, 6) and **session digest matching** (20, 38) let auditors test that exported journals/adjustments used in procedures are complete, unaltered, and tied to a specific, timestamped evidence set.

Clause; Page; Paragraph; Requirement	Dossier Evidence #	Relevance to AuditLog.AI Software
¶52; p.19; Significant Transactions Outside the Normal Course of Business or Otherwise Appear Unusual; **Business Rationale Evaluation:** For significant transactions that are outside the normal course of business or otherwise appear unusual, the auditor shall **evaluate whether the business rationale (or the lack thereof) suggests they may have been entered into to engage in fraudulent financial reporting or to conceal misappropriation of assets.**	**20, 33–37**	Session metadata (20) captures timing/meaning and links to prior anchors; dual-ledger state history + public TXID/block height (33–37) provides independent timing/provenance to evaluate rationale and detect concealment via after-the-fact edits.
¶68; p.22-23; Requirements; **Documentation:** The auditor shall include in the audit documentation... The significant decisions reached during the engagement team discussion... The identified and assessed risks of material misstatement due to fraud... The overall responses to the assessed risks of material misstatement due to fraud... The nature, timing and extent of the audit procedures performed... The results of the audit procedures	**20, 33–39, 41, 6A, 7A**	Session log (20) + dual-ledger timeline (33–39) document nature/timing/results; final anchor event (41) closes the record; reproducibility evidence (6A, 7A) documents additional procedures and conclusions related to fraud-risk responses.

Annex VI — Dossier Evidence Index (Execution Evidence Cross-Reference)

This annex consolidates all primary runtime evidence numbers referenced across regulatory clauses (FDA, EMA, TGA, PCAOB, ISA).
All files are contained within the **AuditLog.AI — Runtime Execution and System Validation Evidence Dossier** (v27 Oct 2025). Evidence groups are organized by functional sequence — from pre-execution environment validation to final blockchain anchoring and reproducibility verification.

I. Zero-Custody Environment Verification

- **2. PRE Screenshot — AuditLog.AI Folder View**
  Demonstrates pre-execution environment cleanliness and zero-custody architecture. Confirms no pre-existing derivatives prior to run.
- **27. Gate Job (Hashes Only)**
  Shows cryptographic handoff job containing only SHA-256 and RIPEMD-160 digests—no user data transferred.
- **30. AuditLog.AI Incoming Anchor Job Receipt**
  Receipt confirming secure zero-custody transfer and queueing of incoming anchor job.
- **33. Receipt Broadcast View**
  Broadcast confirmation from AuditLog.AI server, showing TXID issuance and state machine transition (QUEUE_TICK → BROADCAST_QUEUED).

II. System Validation and Pre/Post Execution Integrity

- **4. Pre-Hasher Execution State Audit**
  Baseline inventory capture verifying controlled environment before hashing begins.
- **8. Post-Hasher Verification Audit**
  Confirms 1:1 parity between manifest entries and generated digests; validates completeness of processing.
- **15. Pre-Execution Mandatory Screenshot (User-Held)**
  System-captured pre-run record showing system state and timestamps prior to execution.
- **16. Post-Execution Mandatory Screenshot (User-Held)**
  Post-run confirmation within Δ=28 s threshold proving consistent, validated performance.
- **42. AuditLog.AI Quality Management System (QMS) and Pre-Public Deployment Audit Log**
  Documents SDLC and validation activities under Sentinel QMS prior to production release.

- **43. AuditLog.AI Live Runtime Execution Audit Infrastructure Integrity Provenance**
  Demonstrates live audit infrastructure reproducibility and integrity under runtime observation.

III. Cryptographic Proof Generation and Time Attestation

- **6. Dual-Hasher Runtime Execution**
  Execution of SHA-256 + RIPEMD-160 dual-hash generation ensuring tamper-evidence.
- **6A. SHA-256 / RIPEMD-160 Reproducibility & Amplification Audits**
  Independent reproducibility campaigns confirming deterministic hash parity across and amplification to 30,000+ evidence files.
- **7. OpenTimestamps (OTS) Runtime Execution**
  Creation of decentralized timestamp proofs anchored to Bitcoin mainnet.
- **7A. OTS Explanation & Reproducibility Audits**
  Validation of OTS proof reproducibility and independent verification using public tools.

IV. Human Verification and Audit Log Authorization

- **12. VALIS Audit Verification Initial Prompt**
  System prompt requesting human approval before audit log creation.
- **13. VALIS Audit Verification Output (Log per Folder)**
  Generated audit verification logs for each folder, showing enforced VALIS template and compliance flags.
- **14. AuditLog Generated Post-Verification**
  Automatically compiled audit log after human confirmation, recording approver identity, UTC time, and signature meaning.
- **17. VALIS Audit Log per Folder Authorized**
  Authorized, frozen audit log files post-validation, marked human_verified = true.
- **20. Session Log View and Prior Session Anchor Audit Log Reference**
  Composite session manifest linking all prior audit logs and their blockchain TXID, establishing chain-of-custody lineage.

V. Immutable Archival & Anchoring Evidence

- **18. Frozen VALIS Audit Logs**
  Demonstrates read-only and immutability protections applied to all validated audit logs.
- **36. Anchored Transaction – Public Explorer View #1**
  Public blockchain confirmation showing TXID and payload parity on Bitcoin mainnet.
- **37. Anchored Transaction – Public Explorer View #2**
  Independent explorer cross-verification (mempool.space / blockchain.com).

- **38. Session Log Digest Match Validation**
  Confirms hash equivalence between frozen session log and on-chain payload (digest parity).
- **39. Dual-Ledger Consistency Verification**
  Demonstrates atomic append across user ledger and master AMPLIFY_LEDGER (no divergence).
- **41. AuditLogger – Final Anchor Event**
  Captures mandatory audit log entry registering the anchor event.

VI. Human Signature Gate & Authorization Workflow

- **3. Human Verifier — Distinct e-Signature Identification Component 1 of 2**
  Human verifier interface executing Ed25519 personal signature bound to a unique meta_id.
- **21. HMAC (Layer 2) + Reviewer Login**
  Institutional authentication verifying organizational authority and session origin.
- **22. e-Signature Gate (Web UI Access)**
  Multi-layer signing interface combining personal signature, institutional HMAC, and non-biometric vector screen.
- **23. Signature Validation (FAIL Test)**
  Negative-control showing system rejection of invalid or automated signature.
- **24. Gate Job Not Generated by False Signature**
  Demonstrates that failed signature attempts do not generate anchor jobs.
- **25. Signature Validation (PASS Test)**
  Positive-control confirming valid human signature passing multi-layer verification.
- **26. AuditLog.AI Pass Signature Registered – Gate Job Created**
  Record of successful gate job creation following human authorization.
- **28 A & B. Final Human Authorization Blockchain Anchoring**
  Final step showing human-approved signature event resulting in blockchain anchoring via AuditLog.AI broadcast.

Annex VII – Public Verification Provenance

Evidence citations originates from the **AuditLog.AI — Runtime Execution and System Validation Evidence Dossier** published 27 October 2025.

Provenance

- **File Reference:** `Audit-Log.AI_Runtime_Execution_and_System_Validation_Evidence_Dossier_FINAL_METADATA___20251027T231047Z.pdf`
- **SHA-256:** `fc46851b4854ca45798b741c0fb001eaa0945eb73c98795900c87939acb30d8a`
- **RIPEMD-160:** `b0c8b2223eab705cac6bf7801b64945f7ed47022`
- **OTS File:** `Audit-Log.AI_Runtime_Execution_and_System_Validation_Evidence_Dossier_FINAL_METADATA___20251027T231047Z.pdf.hash.ots`
- **OP_RETURN Anchor:** `ORDINAL11|b0c8b2223eab705cac6bf7801b64945f7ed47022|fc46851b` | **Transaction ID:** `a09523a5e311d5e5213cba7cc39ec3a274aa1cc017be369c-fa5786c3677a1540` | **Block:** `921107`
- **Ordinal Anchor:** `ORDINAL11|b0c8b2223eab705cac6bf7801b64945f7ed47022|fc46851b` | **Transaction ID:** `6754818e57d5dcc16a7fccdb1d36b-b213cd39ae4a180e17923387738f38a3f41` | **Block:** `921109`
- **Session_log:** `session_log_AuditLogAI.REG.GlobalSubmission.v4059_20251027T231229.358107Z.json`
- **SHA-256:** `db4451a879e62a1e34a14a6052a442172be6c8798aff163a9564a31beb768d21`
- **RIPEMD-160:** `d51e9af05a7b8f32db2f85ab0a76ea7e71cadede`
- **Session OTS File:** `session_log_AuditLogAI.REG.GlobalSubmission.v4059_20251027T231229.358107Z.hash.ots`
- **Session OP_RETURN Anchor:** `SENTINEL|SESSION|d51e9af05a7b8f32db2f85-ab0a76ea7e71cadede|db4451a8`
- **Transaction ID:** `06028cfbf809665838e437dcad6d01c48d5c4679ebd-be045ea12ed4c311c020e`
- **Date of Existence (UTC):** `2025-10-27T23:14:36Z` *(TXID broadcast time confirming file existence as of Bitcoin block 921094.)*

Public Verification References

Telles, Fernando. AuditLog.AI — Runtime Execution and System Validation Evidence Dossier End-to-End Operational Proof During Regulatory Global Submission. CDA AI Pty Ltd, October 2025. DOI: 10.13140/RG.2.2.28551.25765 Zenodo: 10.5281/zenodo.17460850

Telles, Fernando. Sentinel Protocol v3.1 – Infrastructure Reproducibility and Public Verification Log. CDA AI Pty Ltd, July 2025.
DOI: 10.13140/RG.2.2.29180.65924
Zenodo: 10.5281/zenodo.16607606

Telles, Fernando. Ordinal 06 – Immutable Verification of Infrastructure Audit Log (Ordinal 05) under Sentinel Protocol v3.1. CDA AI Pty Ltd, July 2025.
DOI: 10.13140/RG.2.2.21019.78882
Zenodo: 10.5281/zenodo.16777715
