Executive Summary (1 page)

L4 Witness Protocol v0.2 — Outcome Traceability Standard for AI Act Evidence

Submission context:	Regulation (EU) 2024/1689 (AI Act)
Primary mapping:	Article 50 (Transparency) + Article 14 (Human oversight)
Document type:	Technical submission (implementation-oriented)
Author:	Ivan Kotov — Systems Architect | Independent Researcher (Brussels, Belgium)
Contact:	+32485228195 | kotovivan78@gmail.com
Date:	2026-01-21

1) Problem addressed (audit gap)

Operational enforcement of AI Act obligations requires **verifiable evidence** that transparency disclosures and human oversight controls were actually executed during system operation (including reasonably foreseeable misuse). In practice, audits often face either claims without evidence, or non-standard log dumps that are difficult to verify and may expose sensitive information.

2) Proposed solution (what the protocol is)

L4 Witness Protocol specifies an open, audit-ready evidence layer for AI system operation. It defines:

- **Witness Record**: structured event model (JSON Schema).
- **Evidence Envelope**: cryptographic commitments (hash chain) and signatures.
- **Conformance profile**: MUST/SHOULD requirements for a minimal evidence set.

Goal: enable independent verification of compliance-relevant actions **without** requiring disclosure of proprietary prompts, weights, or internal business logic.

3) Regulatory mapping (evidence targets)

Article 50 — Transparency (evidence targets)

- Disclosure that the user is interacting with an AI system (timestamp, channel, context).
- Marking/labeling of AI-generated or manipulated content where applicable (event + applicable policy/rule ID).
- Role attribution fields to distinguish provider vs deployer responsibilities when relevant.

Article 14 — Human oversight for high-risk systems (evidence targets)

- Oversight assignment (responsible natural person role/authority for the session or decision point).
- Information shown to the overseer at the decision boundary (decision-support snapshot metadata).
- Intervention capability and use (override/correction/refusal/safe-stop events, with reason codes).
- Traceable linkage between intervention and the affected output (record IDs).

4) What is delivered (attachments)

- This 1-page Executive Summary (for triage/printing/forwarding).
- Normative specification (PDF): definitions, conformance criteria, threat model, security considerations.
- JSON Schema package (versioned): Witness Record + Evidence Envelope schemas.

5) Integration and audit workflow (how it is used)

Implementers emit Witness Records at defined control points (disclosure, generation, marking, oversight decision, intervention, stop). Records are sealed into Evidence Envelopes (hash chaining + signatures). Auditors verify integrity (chain continuity, signatures) and check completeness against the conformance profile (required events present; coherent timestamps; consistent role attribution).

6) Security, confidentiality, and scope boundaries

- Selective disclosure: sensitive payloads may be committed via hashes while retaining verifiability.
- Tamper-evidence reduces post-hoc editing risk ("compliance after the incident").
- Not a substitute for conformity assessment or full technical documentation; not an identity system.

7) Request to the European AI Office

Please consider this submission for technical review as an implementation-oriented evidence standard supporting enforcement of Article 50 and Article 14 obligations under Regulation (EU) 2024/1689.

Design rationale (non-normative)

Explicit bridge: c = a + b → accountability (a) + verifiable procedures (b) = auditable outcome evidence (c).

Hidden bridges: Ashby (requisite variety) → multiple control-point events; Cover & Thomas (channel reliability) → compact, standardized evidence records.

Earth paragraph: An audit trail is like an ECG: not a narrative, but a signal that should not be drawable after the fact. The witness chain is the signal.

References: Regulation (EU) 2024/1689 (AI Act). Repository set (technical reference):

github.com/Kot141078/advanced-global-intelligence
github.com/Kot141078/sovereign-entity-recursion
github.com/Kot141078/ester-reality-bound

`Reference Source: GitHub Commit 7a376cf (2026-01-21)`