

VERITROOPER Scout — Framework Crosswalk — Where This Audit's Evidence Maps



Model: Meta-Llama-3.1-70B-Instruct on Generated — OSHA_29CFR_full_2024 — veritrooper v9. Generated 2026-07-13 23:17:27.

This crosswalk shows which accuracy, robustness, and documentation requirements across the **EU AI Act**, the **NIST AI RMF**, and **ISO/IEC 42001** the evidence in this package **maps to** — and which it does not. It is a pointer from requirement to evidence, to speed a review. It **does not** assert conformity with any framework; conformity is a determination for the provider and its assessor.

Regulatory posture (verified 2026-07-09). No harmonised standard for high-risk AI has yet been cited in the Official Journal, so **nothing on the market today confers a presumption of conformity** — any vendor claiming AI Act "compliance" is claiming something that cannot currently be conferred. The Digital Omnibus (Council green light 29 June 2026, OJ publication pending) defers the high-risk obligations to **2 December 2027** for stand-alone systems and **2 August 2028** for AI embedded in regulated products. The general-purpose AI obligations (Chapter V) have applied since **2 August 2025** and were **not** deferred. No regime reviewed requires an independent third-party AI audit. This package is **evidence for** the obligations below; it is not, and cannot be, compliance with them.

EU AI Act (Reg. (EU) 2024/1689)

Reference	Requirement (summary)	VERITROOPER evidence	Artifact
Art. 15(3) — Declared accuracy metrics	The levels of accuracy and the relevant accuracy metrics of a high-risk system shall be declared in the accompanying instructions of use. A binding disclosure, not a recommendation.	A named metric with its definition, the measured level, the question set it was measured on, and a reproducible verdict per question — the content that disclosure requires.	VT-20260601-OSHA-001_Results_Report.pdf · VT-20260601-OSHA-001_System_Card.pdf · certification_report.json
Art. 55(1)(a) — GPAI with systemic risk: documented adversarial testing	Model evaluation using standardised protocols and tools, including documented adversarial testing. In force since 2 Aug 2025 — NOT deferred by the Digital Omnibus.	Negative / hallucination-trap categories are adversarial by construction; every prompt, answer and verdict is retained, and the package is cryptographically signed (with an RFC 3161 trusted timestamp where a network was available at sealing).	VT-20260601-OSHA-001_Results_Report.pdf · VT-20260601-OSHA-001_All_QA_Pairs.pdf · findings.sarif.json
Art. 15 — Accuracy & robustness (cybersecurity not assessed)	Appropriate accuracy levels and robustness across the lifecycle. Art. 15 also covers cybersecurity, which this accuracy/robustness audit does not assess.	Final verified accuracy + per-category accuracy + adversarial (hallucination-trap) results, both arms.	VT-20260601-OSHA-001_Results_Report.pdf · VT-20260601-OSHA-001_System_Card.pdf
Art. 11 / Annex IV §2(g)	Validation & testing procedures, metrics, and dated test logs in the technical file.	Annex IV Testing & Validation Record with dated log and metric definitions.	VT-20260601-OSHA-001_Annex_IV_Test_Record.pdf
Art. 10 — Data & data governance	Examination of data for gaps, shortcomings and representativeness.	Performance-gap / representativeness diagnostic by question category.	VT-20260601-OSHA-001_Gap_Diagnostic.pdf
Art. 72 / Annex IV §9 — Post-market monitoring	A monitoring system tracking performance over the system's life.	Accuracy-drift report across repeated audits of a frozen question panel.	drift_report (when ≥2 audits of a panel exist)
Art. 14 — Human oversight	Human oversight of the deployed system in operation.	NOT covered by this audit. The sign-off here is QMS review of test results, not operational oversight; supply Art. 14 measures separately.	— (provider-supplied)

Texas TRAIGA (HB 149) — in force 1 Jan 2026

Reference	Requirement (summary)	VERITROOPER evidence	Artifact
Affirmative defense	No audit is mandated. The Act gives an affirmative defense for substantial compliance with the NIST AI RMF Generative AI Profile (AI 600-1) via internal review, and for discovering violations through testing, including adversarial or red-team testing.	A dated, signed audit with adversarial categories and reproducible verdicts — the testing record the defense contemplates.	VT-20260601-OSHA-001_Results_Report.pdf · Integrity/manifest.json

Colorado SB26-189 (ADMT) — obligations from 1 Jan 2027

Reference	Requirement (summary)	VERITROOPER evidence	Artifact
Developer documentation + 3-year records	Developers must give deployers documentation of intended uses, known limitations, and human-review instructions; both parties retain compliance records for at least three years. The replaced 2024 Act's audit regime was dropped — no third-party audit is required.	Known-limitations evidence (failure clusters, severity, guardrail recipes) inside a cryptographically signed package (RFC 3161 timestamped where a network was available at sealing) that supports the retention duty.	VT-20260601-OSHA-001_System_Card.pdf · VT-20260601-OSHA-001_Results_Report.pdf · Integrity/

NIST AI RMF 1.0

Reference	Requirement (summary)	VERITROOPER evidence	Artifact
MEASURE 2.3 — Performance measured	System performance is measured and documented in deployment conditions.	Two-arm accuracy measurement on domain material with per-category breakdown.	VT-20260601-OSHA-001_Results_Report.pdf · evidence.json
MEASURE 2.5 — Validity & reliability	Validity and reliability are evaluated and documented.	Independent adjudication of each verdict on both arms; reproducible from stored data.	VT-20260601-OSHA-001_System_Card.pdf · evidence.json
MEASURE 2.7 — Robustness / adversarial	Resilience to adversarial or out-of-distribution inputs is assessed.	Dedicated hallucination-trap category measuring refusal on unsupported questions.	VT-20260601-OSHA-001_Results_Report.pdf (Negative category)
MAP / MANAGE — documentation & traceability	Context, limitations and decisions are documented and traceable.	System card, data card, audit trail, the hash-bound human sign-off once recorded, and the whole package sealed with a standards-based digital signature (plus an RFC 3161 trusted timestamp where a network was available at sealing).	VT-20260601-OSHA-001_System_Card.pdf · VT-20260601-OSHA-001_Data_Card.pdf · audit_trail.jsonl · Integrity/

ISO/IEC 42001:2023 (AIMS)

Reference	Requirement (summary)	VERITROOPER evidence	Artifact
Clause 9 — Performance evaluation	Monitoring, measurement, analysis and evaluation of the AI system.	Measured accuracy/robustness with a repeatable, documented procedure.	VT-20260601-OSHA-001_Results_Report.pdf · VT-20260601-OSHA-001_Annex_IV_Test_Record.pdf
Annex A — AI system verification & validation	The AI system is verified and validated against requirements.	Independent two-arm V&V of answers against ground truth, adjudicated.	VT-20260601-OSHA-001_System_Card.pdf

Reference	Requirement (summary)	VERITROOPER evidence	Artifact
Annex A — Documented information / impact	Documented information on AI system performance and data is maintained.	System card + data card + machine-readable evidence bundle.	VT-20260601-OSHA-001_System_Card.pdf · VT-20260601-OSHA-001_Data_Card.pdf · evidence.json

How to read this

- **Maps to** means the artifact provides evidence relevant to the requirement — a reviewer still has to accept it in context.
- Rows marked **NOT covered** flag requirements this audit does not address (notably operational human oversight); supply those separately.
- ISO/IEC 42001 clause and Annex A references are named by control area; confirm the exact clause numbers against your Statement of Applicability.

Contents (click a section to jump)

- EU AI Act (Reg. (EU) 2024/1689)
- Texas TRAIGA (HB 149) — in force 1 Jan 2026
- Colorado SB26-189 (ADMT) — obligations from 1 Jan 2027
- NIST AI RMF 1.0
- ISO/IEC 42001:2023 (AIMS)
- How to read this

Generated by VERITROOPER as a cross-framework evidence map (EU AI Act · NIST AI RMF · ISO/IEC 42001). This artifact is testing evidence only. It does not by itself constitute, certify, or confer conformity with any framework, and does not replace the conformity assessment or the provider's other obligations. Have counsel review before external use.

