

FRAMEWORK MAPPING

NIST AI Risk Management Framework 1.0

Publisher. [NIST](#)

Control mappings. 23 controls

Statement date. 2026-08-03

AI Risk Management Framework. Etch addresses Govern, Map, Measure, and Manage functions through chain signed evidence of role assignments, decisions, and measurements over time.

Control mapping

Every row names a specific control from the framework and describes how Etch addresses it. The response prose commits to what Etch signs on the chain, not to runtime enforcement. Etch is an evidence layer.

Control ref	Control name	How Etch addresses it
Govern 1.1	Legal and regulatory requirements	The extended governance schema records invalidation_conditions on every event. Legal and regulatory constraints are chain signed at write time.
Govern 1.2	Roles and responsibilities	Bounded authority receipts record the identity and scope of each acting party. Every event carries an identifiable signer via authority receipt or signed dissent.
Govern 1.3	AI risk management processes	Session risk score field records the upstream vendor's score at each event. Autonomy level field records L0 through L3 or custom. Both are queryable on chain.
Govern 1.4	Risk management resources	The offline verifier is shipped in the OSS package. An auditor can run air gapped verification without Etch involvement. Resource for risk management is external to the operator.

Control ref	Control name	How Etch addresses it
Govern 1.5	Ongoing monitoring and periodic review	Recoverability measurement, drift detection engine, and corrigibility self audit run on chain state. All measurements are chain signed.
Govern 1.6	Inventories of AI systems	Model card attestation binds model_card_hash, system_prompt_hash, policy_hash, model_id per session. Inventory is queryable back to the specific attestation event.
Govern 1.7	Decommissioning processes	Supersession edge event with intent enum deprecation records decommissioning as a first class chain event.
Govern 2.1	Roles and lines of communication	Signed dissent event provides a second line of defense communication primitive that is chain signed and does not require reaching a supersession.
Govern 3.1	AI risk decisions are transparent	Every AI decision on chain carries a governance record with policy_hash, authority, assumptions, uncertainty, and invalidation_conditions. Decision transparency is chain signed.
Govern 4.1	Organizational teams for AI risk	Authority receipt identity + scope + expiration record the team assignment for each event. Team membership is queryable back to specific approval events.
Govern 5.1	Engaging with AI actors	Cross chain federation records references to external AI actors' chains by derived chain_id. Engagement is cryptographically walkable across boundaries.
Govern 6.1	Third party test and evaluation	The adversarial tamper detection benchmark repository is public MIT licensed and reproducible by any third party. Test and evaluation is external to the operator.
Map 1.1	Context, tasks, and users	Mission field, context field, and scope field on the governance record record the intended context, tasks, and users at each event.

Control ref	Control name	How Etch addresses it
Map 2.1	Documentation of intended uses	Model card attestation binds the intended use text hash. Any deviation from documented use is detectable against the signed record.
Map 3.1	Benefits, costs, and impacts	Signed postmortem records retrospective assessment of outcomes with retroactive confidence downgrade. Impact measurement is chain signed.
Map 4.1	Risks and benefits from third party components	Cross chain federation records upstream and downstream third party chain references. Third party risk posture is walkable on chain.
Measure 1.1	Test, evaluation, verification	The adversarial benchmark repository ships 14 attacks across 5 categories with 100 percent coverage as of the current release. Test evidence is externally reproducible.
Measure 2.1	Test set representativeness	Test corpus is public. Methodology document at the benchmark repository sets out what qualifies as an attack. Community contributions are welcomed via pull request.
Measure 2.5	AI system trustworthiness	Functional continuity tracking walks the DAG backward from any decision to its supporting evidence and reports gaps. Trustworthiness measurement is chain signed.
Measure 2.7	AI system security and resilience	External anchor coverage to Sigstore Rekor and Bitcoin OpenTimestamps. Post quantum hybrid signing envelope (Ed25519 and SLH-DSA-SHA2-128f). Chain integrity survives compromise of the classical signature.
Measure 3.1	AI risk tracking approaches	Drift detection engine tracks risk across 8 dimensions (mission, assumption, confidence, evidence, scope, terminology, authority, context). All drift measurements are chain signed.

Control ref	Control name	How Etch addresses it
Manage 1.1	Response and recovery plans	Explicit stop condition events record halts on chain. Signed postmortem records corrective action with signer identity. Both are first class chain kinds.
Manage 3.1	AI risks and impacts inform response	The retroactive confidence downgrade field on the postmortem event records the revised assessment. Response evidence is chain signed against the originating event.