FRAMEWORK MAPPING

SOC 2 (Trust Services Criteria 2017, revised 2022)

Publisher. AICPA

Control mappings. 22 controls

Statement date. 2026-08-03

System and Organization Controls 2. Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Etch addresses Security and Processing Integrity primarily. Availability, Confidentiality, and Privacy are partially addressed through the signing and audit surface documented below.

> **Attestation vs mapping.** This page is a control response mapping and is not a substitute for a formal SOC 2 attestation report. Etch does not hold a formal third party attestation today. Compliance teams reviewing Etch under an active SOC 2 engagement can request the current audit posture via security@etch.systems.

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
`CC1.1`	Integrity and ethical values	Etch chain signs every policy version and every human approval into an append only log. An auditor can read the record of which policy was in force at which time without depending on the operator's ongoing cooperation.
`CC1.4`	Attracting, developing, retaining people	Etch does not address people processes directly. The signed record identifies each acting party by the bounded authority receipt attached to their events, which supports downstream people audits.

Control ref	Control name	How Etch addresses it
`CC2.1`	Information quality supporting internal control	Every event carries a governance record with policy_hash, authority, assumptions, uncertainty, and invalidation conditions. The signed record commits the exact information that supported each decision at the time.
`CC3.4`	Assessing risk and change	The drift detection engine measures policy drift across 8 categories (mission, assumption, confidence, evidence, scope, terminology, authority, context) on every closed epoch. Drift measurements are chain signed.
`CC4.1`	Selection and development of monitoring	The offline verifier walks the entire chain and reports on integrity, epoch structural validity, external anchor coverage, policy drift, corrigibility, and dimensional drift. Runs on demand or on schedule.
`CC5.1`	Selection and development of control activities	Every control activity that touches an AI decision is chain signed. The record includes the tool call, the policy version, the authority, and the outcome.
`CC5.3`	Deployment of policies and procedures	Policy versions are chain signed at deploy time. The policy drift detector alerts when a downstream node is still running a stale policy_hash after an update.
`CC6.1`	Logical access controls	Token scopes segregate mcp:read, mcp:write, and admin:project. Tokens are hashed at rest. Token issuance and revocation are chain signed via the admin API. The bounded authority receipt endpoint verifies per event Ed25519 signatures against a per project pubkey registry.
`CC6.6`	Boundary protection and transmission	All external traffic terminates at TLS 1.2 or higher with strict SNI. Internal service traffic binds 127.0.0.1 only. KMS backed signing keys are decrypted into memory at spawn time and wiped on shutdown.

Control ref	Control name	How Etch addresses it
`CC6.7`	Transmission and physical media	Chain evidence is transmitted over TLS. External anchor evidence is retrievable independently from Sigstore Rekor and Bitcoin OpenTimestamps by the auditor without traversing Etch.
`CC6.8`	Prevention of unauthorized changes	SQL layer append only triggers on every chain table reject UPDATE and DELETE. A silent rewrite attempt raises the trigger and invalidates the chain state detectable by the offline verifier on next walk.
`CC7.1`	Detection of vulnerabilities and changes	The startup orphan tempfile sweep and the release pipeline (pip audit, Sigstore Trusted Publishing, SBOM) address supply chain detection. Chain state drift is caught by the offline verifier's 11 check categories.
`CC7.2`	Detection of anomalies	Recoverability measurement returns time to reconstruct and evidence completeness per session. The corrigibility self audit flags policies with high governance volume and zero dissent as suppression fragility. Both are chain signed so the detection itself is verifiable.
`CC7.3`	Evaluation of security events	The signed postmortem endpoint records the retrospective of any security event with about_event_id, finding, corrective_action, signer, and optional retroactive confidence downgrade. The record is a first class chain kind.
`CC7.4`	Response to identified incidents	Explicit stop condition events record halts on the chain. The offline verifier flags any write that lands after a stop condition in the same session scope.
`CC8.1`	Change management	Every code release is Sigstore attested through PyPI Trusted Publishing. Every deploy snapshots each OSS chain byte identical before and asserts unchanged after so a bad deploy is caught before it can affect customer chains.

Control ref	Control name	How Etch addresses it
`CC9.1`	Risk mitigation of business disruptions	Chain data replicates to a hot standby. The hot cold storage split supports long term archival with Merkle path verification against cold data. Recovery point objective is under 15 minutes for chain writes.
`CC9.2`	Vendor and business partner management	Cross chain federation lets a supplier chain reference a customer chain by derived chain_id, epoch_seq, and event_hash. The reference is cryptographically walkable so the vendor management record survives beyond either party's continued cooperation.
`PI1.1`	Processing integrity: definition of processing	The signed model card attestation binds model_card_hash, system_prompt_hash, policy_hash, and model_id for each session. Processing definition is chain signed at session boundary.
`PI1.4`	Processing integrity: output completeness	The artifact hash endpoint chain signs the SHA 256 of any produced artifact. Auditor can verify the artifact in hand matches the record on chain.
`PI1.5`	Processing integrity: output correctness storage	Idempotency collapse deduplicates retry storms into a single logical operation with an incrementing counter chain. The counter chain preserves the exact retry history for later reconstruction.
`C1.1`	Confidentiality: identification	The chain payload commits hashes, not raw content. Raw content stays outside Etch. Chain integrity survives any downstream redaction of the source content.