FRAMEWORK MAPPING

HITRUST CSF v11

Publisher. HITRUST

Control mappings. 23 controls

Statement date. 2026-08-03

Common Security Framework. Etch addresses the audit logging control family, integrity control family, and cryptography control family primarily.

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
`01.b`	Access control policy	Token scope model (mcp:read, mcp:write, admin:project) enforces separation of duties. Token issuance and revocation are chain signed via the admin API.
`01.d`	User access management	Bounded authority receipt binds identity, scope, and expiration for each acting party. User access is queryable per event.
`01.j`	User authentication	Every event on the chain is authenticated by Ed25519 signature verified against the per project pubkey registry. Individual event authentication is walkable offline.
`01.q`	User identification and authentication	Every event carries an identifiable signer via authority receipt or signed dissent. Unique identity is chain signed at event level.

Control ref	Control name	How Etch addresses it
`01.t`	Session time out	Authority receipt expiration field bounds each signer's effective window. Any event signed after the expiration instant is rejected server side before append and is detectable by the offline verifier on later walks.
`01.v`	Information access restriction	Session scope chain view emits a scoped bundle without exposing the full project chain.
`01.x`	Mobile computing and communications	TLS 1.2 or higher on all external traffic. HSM attestation for mobile signer scenarios via tpm2 or yubikey.
`03.a`	Cryptographic controls	SHA 256 Merkle chain per epoch. Hybrid Ed25519 and SLH-DSA-SHA2-128f envelope. Post quantum resistance from day 1.
`03.b`	Key management	KMS encrypted signing keys under a KEK loaded at boot from hardware. HSM attestation for enterprise BYOK deployments.
`05.d`	Audit logging	The chain is the audit log substrate. Every signed event kind is chain signed and externally anchored.
`05.e`	Protection of audit logs	SQL layer append only triggers reject UPDATE and DELETE. External anchoring to Sigstore Rekor and Bitcoin OpenTimestamps.
`05.f`	Audit log review	The offline verifier walks chain state and reports on 11 check categories. Review is continuous.
`05.g`	Audit trails	Custody export bundle produces a session scoped self authenticating slice. FRE 902 and eIDAS regime aligned.
`05.h`	Clock synchronization	Every chain row carries a monotonic ts field. Epoch close timestamps are chain signed.

Control ref	Control name	How Etch addresses it
`05.i`	Information integrity	SHA 256 Merkle chain per epoch. Hybrid signing envelope. External anchoring. Post hoc modification detectable.
`05.j`	Non repudiation and signature	Every closed epoch signed with hybrid Ed25519 and SLH-DSA-SHA2-128f. Bounded authority receipt binds per event identity to Ed25519 signature.
`06.g`	Compliance with legal requirements	Custody export bundle regimes cover FRE 902 (11, 13, 14) and eIDAS qualified. Legal compliance evidence is chain signed.
`07.a`	Business continuity management	Chain data replicates to hot standby. Hot cold storage split supports long term archival with Merkle path verification.
`08.a`	Change management	Every deploy asserts byte identical customer chains before and after. Bad deploys are caught before they affect customer state.
`09.aa`	Audit log content and format	Chain payload commits hashes not raw content. Row shape is documented and stable. Payload cannot silently change.
`09.ab`	Audit log storage	Hot tier stores current epochs. Cold tier stores archived epochs with Merkle path verification against hot.
`09.ad`	Fault logging	Explicit stop condition endpoint records halts on chain. The verifier flags any post halt write.
`10.a`	System acquisition	Every code release Sigstore attested via PyPI Trusted Publishing. SBOM available under NDA.