PUBLISHED MAPPING · SP 800-53 · PART 11 · CNSA 2.0

Every capability traces to *a specific control.*

This document mirrors the procurement packet control table (§04) and adds supplementary rows aligned to published collateral. SBOM (CycloneDX) and audit record schema (JSON Schema) are summarized in the procurement packet (§08 Evidence Artifacts) until standalone machine-readable downloads are published at nuqasm.com.

FRAMEWORKS	MAPPING ROWS	BRANDING	DISTRIBUTION
NIST · FDA · NSA SP 800-53 · Part 11 · CNSA	16 core + extended	Aligned procurement PDF	Public with packet

§ 01 · REGULATORY CONTROL MAPPING

Every capability traces to *a specific control.*

Procurement does not buy features. Procurement buys control satisfaction. The table below maps Nuqasm capabilities to the specific regulatory controls your compliance team is already responsible for.

CONTROL	FRAMEWORK	REQUIREMENT	NUQASM CAPABILITY
AU-2	SP 800-53	Define and log auditable events	Every workload submission, seal, route, execution, and result retrieval generates a structured audit entry.
AU-3	SP 800-53	Content of audit records: what, when, where, source, outcome, identity	Audit record includes submitter identity, timestamp, environment, hardware backend, calibration snapshot, compiler version, execution outcome.
AU-8	SP 800-53	Reliable time stamps synchronized across systems	Ledger timestamps from NTP-synchronized time source. Deterministic capsule identity via SHA3-256 hash over contents.
AU-9	SP 800-53	Audit records protected from unauthorized modification	**Append-only ledger** with cryptographic chain. Tamper-evident capsule archives. No overwrite operations permitted by runtime.
AU-10	SP 800-53	Non-repudiation of actions on regulated records	**ML-DSA-87 signatures** bind submitter identity to workload definition and execution record. Signatures verifiable offline using published FIPS 204 reference implementations.
AU-11	SP 800-53	Audit record retention	Configurable retention: 1 year (Evaluate), 3 years (Standard), 7+ years (Sovereign). Immutable storage with policy-scoped retention per workload.
AU-12	SP 800-53	Automatic audit generation at system level	Runtime generates audit entries at each lifecycle stage without operator action. No opt-out for regulated workloads.
§11.10(c)	PART 11	Protection of records for accurate retrieval	Signed, verifiable archives retrievable offline. Export formats include signed PDF evidence bundle and CSV with signature manifest.
§11.10(d)	PART 11	System access limited to authorized individuals	Identity binding on workload submission. Role-based access to ledger queries (researcher, compliance viewer, auditor, administrator).
§11.10(e)	PART 11	Secure, computer-generated, time-stamped audit trails that do not	**Append-only ledger** preserves full version history. Previous records are never overwritten

CONTROL	FRAMEWORK	REQUIREMENT	NUQASM CAPABILITY
		obscure previous records	or deleted. Every modification generates a new entry with full diff.
§11.200	PART 11	Electronic signatures — uniqueness, verification, indelible link to record	ML-DSA signatures cryptographically bound to named individual. Each signature is unique, offline-verifiable, and indelibly linked to the signed record by hash.
CNSA 2.0	NSA	Quantum-resistant algorithms for National Security Systems	NSS default: **ML-DSA-87** signatures, **ML-KEM-1024** key exchange, SHA-384/512 hashing, AES-256 symmetric. Non-NSS option: ML-DSA-65 / ML-KEM-768.
SP 800-208	NIST	Firmware and software signing	Reproducible builds with signed release manifests. SBOM published per runtime version. LMS/XMSS hash-based signatures available for firmware images.
AU-6	SP 800-53	Audit review, analysis, and reporting	Compliance exports, auditor views, and SIEM-forwarded events support systematic review without altering the append-only ledger.
AU-7	SP 800-53	Audit record reduction and reporting	Optional reduction and reporting views; underlying capsule archives and ledger entries remain complete and immutable.
ML-KEM	CNSA 2.0	Quantum-resistant key encapsulation for enterprise routing	**ML-KEM-1024** for NSS workloads; ML-KEM-768 available for non-NSS regulated deployments. No classical-only TLS paths for enterprise workloads.
Parameters	CONFIGURABLE	Cryptographic parameter policy	CNSA 2.0 default (**ML-DSA-87 / ML-KEM-1024**) for NSS. ML-DSA-65 / ML-KEM-768 available where permitted by organizational crypto policy.

PARAMETER CONFIGURATION NOTE

Nuqasm supports both CNSA 2.0 parameter levels (ML-DSA-87 / ML-KEM-1024) for National Security Systems and the intermediate parameter levels (ML-DSA-65 / ML-KEM-768) for non-NSS regulated environments where the smaller parameters meet FIPS 203/204 compliance at lower computational cost. Default configuration is CNSA 2.0. The parameter choice is a deployment configuration option, not a product change.