FOR PROCUREMENT · SECURITY · COMPLIANCE REVIEW

Cryptographic execution provenance for *regulated* quantum workloads.

A signed, verifiable record of every quantum circuit your teams execute — with the audit content, retention, and non-repudiation your regulators already require for classical computation. Vendor-neutral across IBM Quantum, IonQ, and air-gapped hardware. Built on published NIST and NSA standards.

SIGNATURE	KEY EXCHANGE	CONTROLS MAPPED	RETENTION
ML-DSA-87	ML-KEM-1024	12	7 yr+
FIPS 204 · CNSA 2.0	FIPS 203 · CNSA 2.0	SP 800-53 · Part 11	configurable

§ 01 · WHAT NUQASM DOES

The control gap your auditor will find — *before they find it.*

Regulated enterprises are beginning to run material quantum workloads on cloud-hosted QPUs. The controls around those workloads look more like best-effort observability than formal evidence suitable for auditors and regulators. NIST SP 800-53, 21 CFR Part 11, and CNSA 2.0 define audit, integrity, and non-repudiation requirements that apply to any regulated electronic record — including those produced by quantum computation. Today, those requirements cannot be satisfied by standard cloud quantum platforms. Nuqasm closes this gap.

What we deliver

A signed, append-only ledger of quantum execution records — cryptographically binding submitter identity, workload definition, hardware backend, calibration state, and results into a single verifiable artifact. Retrievable by your compliance team. Verifiable offline by your auditor. Aligned to the controls your organization already enforces.

The four things this packet contains

CONTROL MAPPING

Line-by-line mapping of Nuqasm capabilities to NIST SP 800-53 AU controls, 21 CFR Part 11 sections, and CNSA 2.0 algorithm requirements.

DEPLOYMENT OPTIONS

Three control environments — Evaluate, Standard, Sovereign — with specific compliance attributes, data residency, and certification status for each.

COMMERCIAL TERMS

Published price ranges anchored to the cost of the alternative (compliance FTE labor). No per-seat pricing. Multi-year discounts for FedRAMP-authorized deployments.

EVIDENCE ARTIFACTS

Reference to SBOM manifest, reproducible build attestations, audit record schema, and engagement model for security and compliance reviewers.

Who this packet is for

This document is produced specifically for procurement, security, and compliance reviewers evaluating Nuqasm for deployment in regulated environments. It contains the information these teams need to make a buy/no-buy decision without a sales conversation. Technical reviewers seeking deeper implementation detail should request a briefing with engineering; commercial reviewers seeking a pilot scope should request a scoping call. Both paths are noted at the end of this document.

The summary claim — and what backs it

Nuqasm produces cryptographic execution provenance for quantum workloads that satisfies the audit, integrity, and non-repudiation requirements already codified in the frameworks your organization enforces for classical systems. The cryptographic primitives are published NIST standards (FIPS 203, FIPS 204) at CNSA 2.0 parameter levels. The audit

record content and retention map to NIST SP 800-53 Rev. 5 Audit & Accountability controls. The electronic records and signature architecture aligns to 21 CFR Part 11 §11.10 and §11.200. This packet documents each of these alignments in detail.

§ 02 · WHAT YOUR AUDITOR WILL ASK

Quantum execution is *in scope* for controls your organization already enforces.

Four regulatory frameworks — each already in force at most regulated organizations — impose specific requirements on electronic records produced by quantum computation. Those requirements cannot be satisfied by cloud quantum provider logging alone.

NIST SP 800-53 Rev. 5 — Audit & Accountability

Your ATO boundary requires comprehensive, tamper-protected, time-correlated audit records with non-repudiation. AU-2 requires defined auditable events. AU-3 specifies required content including identity, timestamp, source, and outcome. AU-8 requires synchronized time stamps. AU-9 requires protection from modification. AU-10 requires non-repudiation. AU-11 requires retention. AU-12 requires system-level audit generation. Cloud quantum providers today emit account-level API logs — they do not produce experiment-level records you can attribute to a named individual and prove have not been modified.

21 CFR Part 11 — Electronic Records & Signatures

FDA-regulated organizations must maintain secure, computer-generated, time-stamped audit trails that record creation, modification, and deletion of electronic records without obscuring previous versions (§11.10(e)). Each action must be uniquely attributable to an individual via secure credentials (§11.10(d), §11.200). Today, quantum-derived results arrive as JSON payloads delivered to customer buckets — with no Part 11–style audit trail over the full experiment lifecycle.

CNSA 2.0 — Post-Quantum Cryptographic Baseline

New National Security System acquisitions must be CNSA 2.0–compliant by January 1, 2027. That means ML-DSA-87 signatures (FIPS 204), ML-KEM-1024 key establishment (FIPS 203), AES-256 symmetric encryption, SHA-384/512 hashing, and SP 800-208 firmware signing. Most quantum tooling does not yet implement these algorithms at NSS parameter levels. The gap widens as the January 2027 deadline approaches.

The synthesis question

> “Prove this quantum workload ran as approved, on validated hardware, in a known calibration state — and that the results you cite are the results it produced.”

Most organizations cannot answer this question with evidence today. They reconstruct from partial logs. They assemble spreadsheets. They hope the documentation holds up. The absence of enforcement action to date is not an exemption — the underlying requirements apply to any electronic record that informs a regulated decision.

SUPPORTING DOCUMENT

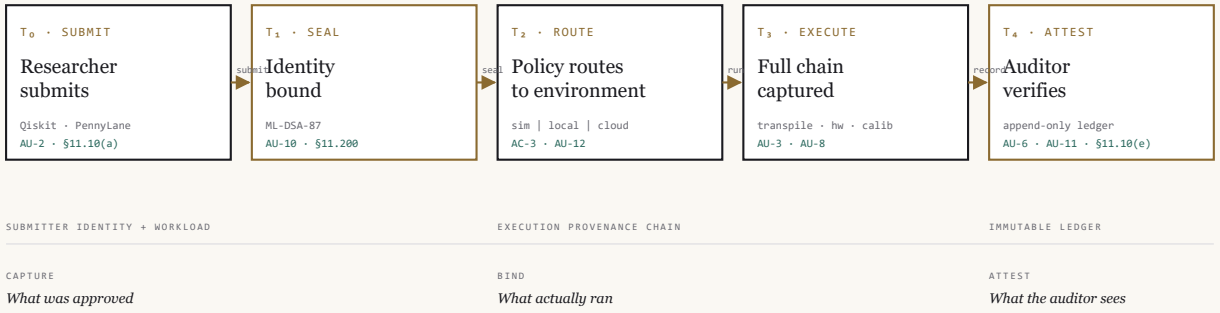
A full analytical assessment, *“Execution Provenance Gaps in Regulated Quantum Computing Environments,”* maps each of these frameworks to concrete quantum workflows on IBM Quantum, Amazon Braket, Azure Quantum, and D-Wave Leap. Available on request.

§ 03 · HOW NUQASM CLOSES THE GAP

One system of record. *Every workload. Every environment.*

Nuqasm captures a cryptographically bound execution record at every stage of the quantum computation lifecycle — from the moment a researcher submits a workload to the moment an auditor verifies what ran. The record is signed, time-stamped, immutable, and complete.

FIG.01 — COMPLIANCE LIFECYCLE · FIVE STAGES · CONTROLS SATISFIED



The single claim this architecture makes

At any point after an execution, an authorized reviewer can produce a signed record showing: **who** submitted the workload, **what** was approved for execution, **when** it ran, **where** it ran, on **what hardware in what calibration state**, and **what results it produced** — with every element cryptographically bound and independently verifiable offline using published NIST standards. No other quantum tooling produces this artifact today.

§ 04 · 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).

CONTROL	FRAMEWORK	REQUIREMENT	NUQASM CAPABILITY
§11.10(e)	PART 11	Secure, computer-generated, time-stamped audit trails that do not obscure previous records	**Append-only ledger** preserves full version history. Previous records are never overwritten 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.

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.

§ 05 · CONTROL ENVIRONMENTS

Three deployment modes. *One trust boundary.*

Nuqasm separates the execution environment from the source of truth. Policy declares where a workload may run. The runtime enforces it. The audit record is identical regardless of environment. Your compliance team reviews one ledger, not three.

Simulator — evaluation and workflow validation

Data residency	Local only, never leaves the host workstation
Network requirements	Offline-capable. Zero external calls in air-gap mode.
Audit retention	Local ledger, 1-year retention, exportable
Applicable certifications	Inherits host system ATO and certifications
Typical use case	Validate sealing workflow, train compliance staff, reproduce historical results for audit review

Sovereign (UQBench Appliance) — air-gapped hardware deployment

Deployment form	Desk-side hardware appliance with integrated 15-qubit QPU. USB-C / JTAG connectivity.
Data residency	Facility-local. No cloud dependency. No telemetry. No license pings.
Network requirements	Air-gap enforced by architecture. Suitable for SCIF deployment.
Audit retention	Append-only ledger on device, configurable 7+ years, export to approved media
Applicable certifications	DISA STIG (in progress). Architecture compatible with NIST SP 800-53 High baseline.
Typical use case	Classified programs, National Security Systems, environments where cloud connectivity is not approvable

Managed — cloud routing with federated audit

Deployment form	Nuqasm runtime routes sealed workloads to managed QPU providers (IBM Quantum, IonQ)
Data residency	Provider regions (configurable) with Nuqasm-side capture of full execution record
Network requirements	ML-KEM-1024 quantum-resistant key establishment. No classical-only TLS paths.
Audit retention	Federated ledger with provider-independent records, 3-year default retention
Applicable certifications	FedRAMP Moderate (in progress, targeting via 20x path). SOC 2 Type 2 (in progress).
Typical use case	Production quantum workloads in regulated enterprises where provider QPUs are approved and cloud connectivity is permitted

CERTIFICATION STATUS SUMMARY

FEDRAMP MODERATE

In progress

▲ 20x authorization path

SOC 2 TYPE 2

In progress

▲ 12-month observation

DISA STIG

In progress

▲ Sovereign deployment

PART 11 VALIDATION

Ready

• IQ / OQ / PQ available

SBOM / REPRODUCIBLE BUILDS

Shipped

• Every release

CNSA 2.0 PARAMETERS

Shipped

• Default configuration

§ 06 · PRICING & ACCESS

Priced below *the compliance labor it replaces.*

> ### Pricing anchor
>
> Quantum execution provenance is currently handled — where it is handled at all — by 0.5 to 1 FTE of compliance analyst time per program, at roughly $120,000 to $180,000 per year in fully-loaded labor cost. Nuqasm is priced below that alternative at every tier.

TIER	ANNUAL PRICE	INCLUDES
Evaluate	$0 NO CONTRACT	20-qubit simulator, full sealing workflow, Qiskit / PennyLane / OpenQASM support, local ledger with 1-year retention, 2 compliance users. For compliance and security teams assessing the control gap. No procurement friction.
Standard	$80K – $120K PER YEAR	Simulator + cloud routing environments, 3-year audit retention, 5 compliance users, quarterly compliance reports, SOC 2 Type 2 evidence, full control mapping documentation. Suitable for financial institutions, research labs with federal funding, enterprise R&D under regulatory oversight.
Sovereign	$150K – $250K + UQBENCH CAPEX FROM $200K	All environments including UQBench air-gapped appliance, 7+ year audit retention, unlimited compliance users, custom audit report templates, dedicated compliance liaison, CNSA 2.0 default configuration, classified-network compatibility, full procurement documentation package. UQBench appliance CapEx from $200K with $50K annual maintenance.

Pricing principles

- **No per-seat pricing for researchers.** Price scales with control environments, not people. A program with 50 quantum researchers pays the same as one with 5.
- **Multi-year contracts available at discount** for FedRAMP-authorized deployments (10–15% for 3-year, 15–20% for 5-year).
- **Pilot programs available** for qualifying organizations, typically 90 days, converted to annual contract upon successful pilot close.
- **Government pricing** available via GSA schedule and SBIR contract vehicles.

Engagement model

Standard and Sovereign tier engagements include a dedicated customer success contact with direct access to engineering, quarterly compliance review calls, and priority response on audit inquiries. Sovereign tier includes an

assigned compliance liaison for procurement documentation, validation packages (IQ/OQ/PQ), and regulatory response support during audits or IG inquiries.

What's not included

Quantum hardware access to IBM Quantum or IonQ is billed separately by the provider. Nuqasm does not resell QPU time. Custom integration work beyond the published API is available as a professional services engagement at $250/hour or fixed-fee scoping.

REQUEST COMMERCIAL ENGAGEMENT

For quote requests, contract templates, or pilot scoping — contact commercial@nuqasm.com or use the pilot scoping door at nuqasm.com/#access.

§ 07 · DEPLOYMENT BY REGULATORY CONTEXT

For the compliance team that *already owns these frameworks*.

Defense, intelligence, and national security programs

Primary frameworks: CNSA 2.0, NIST SP 800-53 High baseline, NIAP protection profiles. Deployment: Sovereign (UQBench) with managed air-gap, classified-network compatible. Typical buyer: program security officer, authorizing official, information system security manager (ISSM). Evidence delivered: signed execution records with CNSA 2.0 parameter signatures, retention aligned to program classification, STIG-compatible configuration.

Financial services and market infrastructure

Primary frameworks: SR 11-7 (Federal Reserve model risk management), FFIEC handbook, MiFID II Article 17 (algorithmic trading controls), SOC 2 Type 2, SOX IT general controls. Deployment: Managed (cloud routing) with federated audit, Standard control environment. Typical buyer: head of model risk, chief compliance officer, operational risk lead. Evidence delivered: model execution provenance for model risk committee review, reproducibility attestation for challenger model validation.

Life sciences and clinical research

Primary frameworks: 21 CFR Part 11, EU GMP Annex 11, ICH E6(R3) GCP, ICH E9 (statistical principles). Deployment: Managed or Sovereign based on data classification. Typical buyer: head of quality, validation lead, Part 11 subject matter expert, CSV (computer system validation) lead. Evidence delivered: IQ/OQ/PQ validation package, Part 11–compliant audit trail, electronic signature attestation suitable for FDA submission.

National laboratories and federally funded research

Primary frameworks: DOE Order 205.1C, FISMA, NIST SP 800-53 Moderate baseline, DOE SC quantum computing user program requirements. Deployment: Sovereign (on-premise) or Managed (cloud routing to approved QPUs). Typical buyer: cybersecurity program manager, designated approving authority (DAA), quantum computing user facility lead. Evidence delivered: audit records aligned to lab's existing FISMA boundary, execution provenance for DOE peer review.

Cross-context value

Organizations operating across multiple regulatory contexts (e.g., a bank with both SR 11-7 model risk governance and SOC 2 Type 2 reporting, or a pharmaceutical company with Part 11 clinical trial workflows and SR 11-7 model risk for internal financial models) can use a single Nuqasm deployment to produce audit artifacts aligned to each framework simultaneously. The underlying audit record is identical; only the export format and reporting template changes per framework.

§ 08 · EVIDENCE ARTIFACTS

What your security team can *verify independently*.

Nuqasm publishes verifiable evidence for every claim in this packet. Reviewers do not need to trust Nuqasm's assertions — they can reproduce the verification themselves using published open-source tooling.

Cryptographic verification

Every `.qcap` capsule and every audit record is signed with ML-DSA-87 (FIPS 204) at the CNSA 2.0 parameter level. Signatures are verifiable offline using the **liboqs** reference implementation from the Open Quantum Safe project (github.com/open-quantum-safe/liboqs) without any Nuqasm-provided tooling. Public keys for the Nuqasm signing hierarchy are published at nuqasm.com/keys with a separate attestation chain rooted in a published certificate policy.

Supply chain transparency

SBOM (Software Bill of Materials) is published in CycloneDX 1.5 format for every runtime release. Machine-readable `sbom.json` at nuqasm.com is planned; until then, SBOM scope, format, and signing posture are summarized in this packet for procurement review. Release manifests are signed with SP 800-208 compliant stateful hash-based signatures (LMS). Build reproducibility is verified via Nix-based deterministic builds; reviewers can rebuild any release from published source and verify hash equivalence.

Audit record schema

The audit record schema is defined in JSON Schema format with accompanying documentation. Machine-readable `audit-schema.json` at nuqasm.com is planned; until then, field definitions and control annotations are summarized in this packet for security and compliance reviewers. Each field maps to the regulatory control it supports. The schema is versioned; schema changes require a major version bump and are documented in release notes.

Third-party assessments

SOC 2 Type 2 report (in progress) will be available under NDA upon completion of the 12-month observation period. Penetration testing report from a qualified 3PAO is available under NDA for Standard and Sovereign tier evaluations. FedRAMP Moderate authorization (in progress via 20x path) will be listed on the FedRAMP Marketplace upon completion.

Supporting documentation

Three analytical and technical documents support the claims in this packet:

- *Execution Provenance Gaps in Regulated Quantum Computing Environments* — regulatory framework assessment available on request
- *Nuqasm Audit Record Schema v2.0* — JSON Schema with control mapping annotations; public download planned at nuqasm.com — narrative in this packet until published.
- *Nuqasm Cryptographic Architecture* — technical specification of signing hierarchy, key management, and verification procedures, available on request under NDA for Standard and Sovereign tier evaluations

Reproducible verification walkthrough

Three-step independent verification

1. Download any sealed `.qcap` archive from the Evaluate tier. **2.** Download the Nuqasm signing public key from the published key hierarchy. **3.** Use liboqs to verify the ML-DSA-87 signature over the archive contents. The verification succeeds using only published NIST standards and published open-source tooling — no Nuqasm code required.

§ 09 · ENGAGEMENT PATHS

Three doors. *Pick the one that fits your role.*

Compliance, security, and procurement teams work on different clocks with different evidence requirements. Each path below leads to the specific artifact or conversation that matches your role — without forced sales pressure.

PATH 01 · PROCUREMENT REVIEW

You have this document. Share it with procurement, legal, and security. If additional documentation is needed — commercial terms, signed NDA, SOC 2 executive summary — email commercial@nuqasm.com with the specific artifact requested.

`commercial@nuqasm.com`

PATH 02 · TECHNICAL BRIEFING

30-minute call with engineering covering architecture, cryptographic implementation, audit record schema, and integration with your existing SIEM. No commercial conversation — technical verification only.

`engineering@nuqasm.com`

PATH 03 · PILOT SCOPING

45-minute commercial conversation with engineering lead and customer success. We map your regulatory context to our deployment options and size a 90-day pilot with defined success criteria.

`pilots@nuqasm.com`

PATH 04 · AUDITOR ENGAGEMENT

For internal audit or external regulator teams reviewing a customer's Nuqasm deployment. We provide direct reviewer access to the audit record schema, verification procedures, and control mapping documentation.

`audit@nuqasm.com`

Typical pilot structure

A 90-day pilot engagement begins with a scoping call to identify the customer's regulatory context and target quantum workloads. Week 1–2: deployment of the Evaluate tier and compliance team onboarding. Week 3–6: production workload integration with the Standard or Sovereign tier. Week 7–10: audit export and reporting validation with the customer's compliance and audit teams. Week 11–12: pilot review and conversion to annual contract. Pilot fees are typically waived for qualifying organizations in defense, life sciences, or regulated financial services.

Reference check availability

Reference calls with existing Nuqasm customers are available for Standard and Sovereign tier evaluations upon execution of a mutual NDA. Customer references are typically available in defense, national laboratory, and regulated financial services contexts. Contact commercial@nuqasm.com to schedule.

Contact summary

COMMERCIAL & PROCUREMENT

`commercial@nuqasm.com`

TECHNICAL & ENGINEERING

`engineering@nuqasm.com`

Pricing, contract terms, GSA schedule, SBIR vehicles, multi-year agreements

Architecture review, integration planning, cryptographic verification, SIEM integration

PILOT SCOPING

pilots@nuqasm.com

90-day pilot scoping, regulatory context mapping, success criteria definition

AUDIT ENGAGEMENT

audit@nuqasm.com

Auditor access, regulatory response support, verification documentation for reviewers

---