QUANTUM CORE INSTITUTE

Standards-first governance for post-quantum cryptography risk

QCI-QS1

Quantum Readiness and Post-Quantum Cryptography Governance Standard

Version	**2.2**
Status	**Published**
Release note	v2.2 adds the AI-cryptographic intersection across QRAF, QASI, and the vendor process, and wires primary citations into the normative references.
Date	June 8, 2026
Owner	Quantum Core Institute
Cite as	Quantum Core Institute. QCI-QS1 Quantum Readiness and Post-Quantum Cryptography Governance Standard. Version 2.2. June 2026.

Rights and reference

QCI-QS1 is published by the Quantum Core Institute as public infrastructure. It may be referenced freely in organizational governance documentation, regulatory submissions, procurement instruments, and vendor assessments, provided that attribution to the Quantum Core Institute is maintained and the version and date are cited.

The standard may not be modified and redistributed, or reproduced in whole for commercial gain, without written consent from the Quantum Core Institute. Any conformance or methodology claim that references QCI-QS1 shall state the version and the edition date relied upon.

Contents

Foreword

This standard defines the minimum governance, inventory, scoring, and third-party oversight requirements for quantum-related cryptographic risk. It is built to be auditable, repeatable, and comparable across institutions.

Version 2.2 adds one capability. It lets the standard govern cryptographic risk that arises from AI systems. AI infrastructure now concentrates high-value cryptographic exposure. Model weights, training data, signed model provenance, and dense machine-to-machine traffic between agents all depend on cryptography that a quantum-capable adversary can target. v2.2 brings that exposure inside the existing structure rather than creating a parallel framework.

> QCI-QS1 governs cryptographic risk arising from AI systems. It does not govern AI risk generally. The additions in v2.2 apply only where AI systems sit inside the declared assessment scope.

Version 2.2 also replaces the prior placeholder normative references with primary sources. Every quantum-safe algorithm, deprecation date, and AI-specific recommendation now traces to a named standard or government publication in Clause 2 and the citation register in Annex E.

1. Scope

This standard specifies requirements for:

- Quantum risk governance and enterprise accountability (QRAF).
- Quantum attack surface and cryptographic dependency inventory (QASI).
- A comparable readiness scoring method (Q-Risk Score).
- Vendor roadmap request and attestation process for third-party risk.
- Board-level reporting and oversight tied to PQC readiness.

This standard applies to systems, data, and third parties where cryptography protects confidentiality, integrity, authenticity, identity, and transaction trust. Where AI systems fall within that scope, the AI-cryptographic provisions marked throughout this standard also apply.

2. Normative references

The following documents inform this standard. This standard does not require adherence to any single external framework. It maps cleanly to them. Algorithm names, deprecation trajectories, and AI-specific recommendations in this standard trace to the sources below. Full detail and status sit in Annex E.

Reference	Document and status
NIST FIPS 203	Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM). Final standard, August 13, 2024.
NIST FIPS 204	Module-Lattice-Based Digital Signature Algorithm (ML-DSA). Final standard, August 13, 2024.

Reference	Document and status
NIST FIPS 205	Stateless Hash-Based Digital Signature Standard (SLH-DSA). Final standard, August 13, 2024.
NIST IR 8547 ipd	Transition to Post-Quantum Cryptography Standards. Initial Public Draft, November 12, 2024. The 2030 deprecation and 2035 disallowance dates are draft and not yet binding.
NSA CNSA 2.0	Commercial National Security Algorithm Suite 2.0. NSA, 2022. New National Security System acquisitions support CNSA 2.0 from January 1, 2027.
NSA/CISA/FBI CSI	AI Data Security: Best Practices for Securing Data Used to Train and Operate AI Systems. Cybersecurity Information Sheet, May 22, 2025. Recommends quantum-resistant digital signatures for training data and model parameters.
OpenSSF OMS	OpenSSF Model Signing Specification. Industry specification, not a government standard. A PKI- and algorithm-agnostic model-signing framework. Referenced as an example mechanism only.

This standard also assumes the context of enterprise risk governance frameworks, information security management programs, and vendor risk management practices already in use by the adopting organization.

3. Terms and definitions

Quantum risk. Exposure created by quantum computing progress that may compromise current cryptographic protections or accelerate adversarial capabilities.

Post-quantum cryptography (PQC). Cryptographic algorithms designed to resist attacks from quantum computers.

Cryptographic dependency. Any use of cryptography within systems, products, integrations, identity infrastructure, or vendor services that supports confidentiality, integrity, authenticity, or nonrepudiation.

Data longevity. The duration for which data must remain confidential or verifiable to maintain compliance, operational safety, or business value.

Harvest now, decrypt later (HNDL). An adversary pattern in which encrypted data is collected now for potential decryption later when capabilities improve.

Crypto agility. The ability to change cryptographic algorithms with bounded, repeatable effort and without replacing the platform that uses them.

ML-KEM. Module-Lattice-Based Key-Encapsulation Mechanism. Standardized by NIST as FIPS 203.

ML-DSA. Module-Lattice-Based Digital Signature Algorithm. Standardized by NIST as FIPS 204.

SLH-DSA. Stateless Hash-Based Digital Signature Algorithm. Standardized by NIST as FIPS 205.

Cryptographic Bill of Materials (CBOM). A machine-readable inventory of an organization or product’s cryptographic assets, including algorithms, libraries, keys, certificates, and protocols.

AI system. A system that trains, fine-tunes, stores, serves, or coordinates machine-learning models, including training pipelines, model registries, inference endpoints, and multi-agent communication architectures.

AI artifact. A cryptographically protected asset produced or consumed by an AI system, including model weights and parameters, training datasets, model registry entries and signatures, and inter-agent message streams.

Part A. Normative requirements

4. Governance and accountability requirements (QRAF core)

4.1 Governance ownership

1. The organization shall assign an executive sponsor accountable for quantum readiness.
2. The organization shall appoint a Quantum Risk Owner responsible for program execution.
3. The board or designated board committee shall receive quantum readiness reporting at least quarterly.

4.2 Required governance artifacts

The organization shall maintain the following artifacts:

- A quantum risk policy statement that defines scope and oversight.
- A quantum risk register section within the enterprise risk register.
- A PQC readiness roadmap with milestones and owners.
- A QASI inventory with coverage reporting.
- A Q-Risk Score snapshot produced at least quarterly.
- A third-party evidence pack, including vendor attestations, for defined critical suppliers.
- A board briefing insert, included in the quarterly risk pack.

4.3 Risk appetite and escalation

1. The organization shall define escalation triggers tied to quantum readiness exceptions.
2. The organization shall require remediation plans for exceptions that exceed risk appetite.
3. The organization shall identify who can accept exceptions and for how long.

4.4 AI-cryptographic incident scenarios (where AI systems are in scope)

New in v2.2. Where AI systems with material cryptographic dependencies fall within the assessment scope, the organization shall include the following scenarios in its incident response procedures and tabletop evidence. These scenarios are assessed under QRAF Domain D7 (incident and resilience).

1. Provenance forgery (D7-AI-1). Response to forged model provenance, model artifact signatures, or attestations made possible by a broken or deprecated signature scheme. Coverage shall address re-signing of critical artifacts with a quantum-safe signature algorithm.
2. Harvested AI asset exposure (D7-AI-2). Identification and response to HNDL exposure of model weights, model parameters, or training data protected in transit or at rest by quantum-vulnerable key exchange or key-wrapping.
3. Inter-agent downgrade (D7-AI-3). Detection and response to downgrade or silent fallback events on machine-to-machine and agent-to-agent channels that remove quantum-safe protection.

> Scope guard. These scenarios assess cryptographic incidents arising from AI systems. They do not assess model behavior, output safety, or AI risk generally. They apply only where AI systems are in scope. Anchors: NSA/CISA/FBI AI Data Security CSI, FIPS 204, FIPS 205, NIST IR 8547 ipd.

5. Inventory and visibility requirements (QASI)

5.1 Minimum inventory coverage

1. The organization shall inventory all critical systems and critical data flows that rely on cryptography.
2. The organization shall maintain an inventory coverage metric.
3. The organization shall name a system owner for each inventoried system.

5.2 Minimum required QASI fields

For each in-scope system, the organization shall capture at minimum:

- System identifier, system name, business criticality, system owner.
- Data classification and data longevity requirement.
- Cryptographic functions used, for example TLS, signing, encryption at rest, key exchange.
- Algorithms in use, where known.
- Cryptographic libraries, where known, and version where available.
- Key management method, for example HSM, KMS, internal PKI, local keys.
- Certificate dependencies and identity dependencies.
- External interfaces and third-party dependencies.
- PQC support status or roadmap status.
- Crypto agility status.
- Evidence reference for validation.

New in v2.2. For each in-scope system classified as an AI system, the organization shall additionally capture the conditional field group below. A non-AI system records an AI artifact class of “none” and the group has no scoring effect.

AI field (conditional)	Description	Example
AI artifact class	Type of AI artifact the system holds or moves.	Model weights
Artifact sensitivity horizon	Years the artifact must stay confidential, or its provenance must stay trustworthy.	7 years
Model signing and provenance scheme	Signature scheme protecting model artifacts, registries, and attestations.	ECDSA P-256
Inter-agent channel protection	Protection on machine-to-machine and agent-to-agent traffic.	Classical TLS
AI artifact key-wrapping	Mechanism that wraps symmetric keys protecting AI artifacts at rest.	RSA-wrapped

5.3 QASI risk flags

The organization shall define and track risk flags. At minimum, flags shall include:

- Long-lived confidentiality requirements protected by non-PQC public-key mechanisms without an approved migration plan.
- Critical vendor dependencies without a PQC roadmap and attestation response.
- Unknown or unmanaged certificate inventories for critical trust chains.
- Systems without a named owner or without evidence references.
- **New in v2.2.** AI artifact with a sensitivity horizon beyond the planned migration date, protected by quantum-vulnerable signing or key-wrapping, with no approved migration plan.

6. Comparable scoring requirements (Q-Risk Score)

6.1 Scoring structure

The organization shall compute a Q-Risk Score from 0 to 100 using five pillars:

- Governance and accountability (20).
- Crypto visibility and QASI completeness (20).
- Data longevity and exposure management (20).
- PQC migration readiness and crypto agility (25).
- Third-party readiness (15).

6.2 Maturity scale

Each pillar shall be scored 0 to 5 using this maturity scale: 0 Unaware. 1 Aware. 2 Defined. 3 Implementing. 4 Managed. 5 Assured.

6.3 Comparability controls

1. An institution shall not score above 60 unless QASI coverage exceeds a defined threshold for critical systems.
2. An institution shall not score above 70 unless critical vendors have provided roadmap responses and attestations, or exceptions are documented with a mitigation plan.
3. An institution shall not score above 80 unless crypto agility has been demonstrated via test evidence for at least one critical trust pathway.

6.4 AI-cryptographic posture in Pillar 5 (where AI systems are in scope)

New in v2.2. Pillar weights do not change. Where a critical vendor supplies AI platform, ML infrastructure, model registry, or key management used for AI artifacts, the vendor's AI-cryptographic posture is in scope for Pillar 5 and is assessed through the vendor questions in Clause 7 and the Vendor Roadmap Request Pack.

6.5 Reporting cadence

The organization shall produce and archive the Q-Risk Score quarterly, including deltas and evidence references.

7. Third-party oversight requirements (Vendor Roadmap Request Pack)

7.1 Applicability

The organization shall issue vendor roadmap requests to suppliers that materially affect:

- Identity and trust (PKI, certificate issuance, signing).
- Secure communications (TLS termination, VPN, secure remote access).
- Key management and cryptographic enforcement.
- Confidentiality of regulated or long-lived data.
- Transaction integrity and nonrepudiation.
- **New in v2.2.** AI platform, ML infrastructure, model registry, or key management used with AI artifacts.

7.2 Minimum vendor request contents

The vendor request pack shall include:

- A standardized question set covering cryptographic footprint, PQC roadmap, crypto agility, testing and assurance, customer obligations, and disclosure practices.
- For AI platform suppliers, the AI-cryptographic question group (Vendor Roadmap Request Pack, Section G).
- An attestation format requiring officer-level signature or equivalent authorized signatory.
- A requirement for evidence attachments where available.

7.3 Vendor exception handling

1. The organization shall maintain a vendor exception register for suppliers that fail to respond or provide inadequate roadmaps.
2. Each exception shall include a remediation plan, compensating controls, and an exit strategy, where feasible.
3. The board briefing insert shall include the top vendor exceptions for critical suppliers.

8. Board reporting requirements (Board Briefing Insert)

8.1 Mandatory board insert elements

The board insert shall include:

- Current Q-Risk Score and change since last quarter.
- QASI coverage metrics.
- Top exposures tied to data longevity and crypto dependencies, including AI artifact exposures where AI systems are in scope.
- Vendor readiness and exceptions list for critical suppliers.
- A short list of management actions completed and actions planned.
- Any requests for board decisions or risk acceptance.

8.2 Board oversight expectations

The board shall require named accountability for quantum readiness, evidence-driven reporting rather than narrative-only reporting, and third-party readiness treated as a governance topic rather than a procurement topic.

Part B. Implementation guidance

9. Practical implementation guidance

9.1 The 90-day establishment sequence

- Weeks 1 to 2: Assign owners, define scope, identify critical systems, define coverage threshold.
- Weeks 3 to 6: Build QASI inventory for critical systems, validate with engineering owners. Where AI systems are in scope, capture the conditional AI fields.
- Weeks 7 to 9: Map data longevity and HNDL exposure, prioritize remediation targets.
- Weeks 10 to 12: Run vendor request pack, score Q-Risk, deliver board insert with a first roadmap.

9.2 Crypto agility proof, minimum viable

A crypto agility proof should show algorithm negotiation or configuration change capability, operational steps documented and repeatable, a rollback plan, and performance and latency impact measured in a realistic environment.

9.3 AI-cryptographic priorities (where AI systems are in scope)

Sequence the highest-sensitivity AI flows first. Re-sign critical model artifacts with a quantum-safe signature algorithm, move model weight distribution and training data ingestion to hybrid key exchange, and update key management to wrap AI artifact keys with ML-KEM. Existing AES-256 data does not need re-encryption. The key protection mechanism is what requires updating.

9.4 What auditors like to see

Evidence links from every claim to a ticket, report, export, or configuration artifact. Defined scope boundaries with rationale. Exception handling with approvals and expiry dates.

Component specifications

The following sections provide the operational detail for the six integrated components. The normative requirements in Part A take precedence where any difference appears.

QRAF. Quantum Risk Governance and Assessment Framework

Purpose

QRAF prevents a predictable failure mode. Quantum risk gets treated as future cryptography work until it becomes present operational exposure. QRAF forces the organization to assign ownership, measure exposure, and prove progress using evidence rather than optimism.

Scope

QRAF covers quantum-driven risk that can create operational, financial, legal, or strategic exposure, including PQC migration readiness, cryptographic dependency and data longevity exposure, third-party and supply-chain quantum risk, shadow quantum activity, incident readiness for HNDL scenarios, and governance and reporting obligations. Where AI systems are in scope, QRAF also covers cryptographic risk arising from those AI systems.

Governance model

QRAF assigns responsibility on the principle that unassigned risk does not get managed. Required roles span the board (oversight and risk appetite), an executive sponsor (accountable owner, typically CISO or CIO), a Quantum Risk Owner (program lead), a risk committee (cross-functional steering), procurement and vendor risk, architecture and engineering, and legal and compliance.

QRAF assessment domains

QRAF assesses eight domains. Each uses maturity levels and evidence requirements.

Domain	What it measures	Typical failure mode
D1. Governance and accountability	Ownership, oversight cadence, risk appetite.	“It’s IT’s problem.”
D2. Crypto asset visibility	What crypto exists and where.	“We do not know what we use.”
D3. Data longevity exposure	What must stay secret and for how long.	“We assumed short shelf life.”
D4. PQC migration readiness	Plan, prioritization, engineering capacity.	“We are waiting on vendors.”
D5. Third-party exposure	Supplier readiness and attestations.	“Outsourced risk is still ours.”
D6. Identity and trust dependencies	Certificates, PKI, IAM, signing.	“Certificate sprawl.”

Domain	What it measures	Typical failure mode
D7. Incident and resilience	Detection, response, crypto agility. Where AI systems are in scope, coverage of AI-cryptographic incident scenarios D7-AI-1 through D7-AI-3.	"No playbook." For AI systems: "The model registry trusts a signature that quantum capability can forge."
D8. Assurance and auditability	Evidence, testing, reporting.	"Slides instead of proof."

AI-cryptographic incident scenarios (D7, where AI systems are in scope). D7 assessment shall confirm incident coverage of the three scenarios defined in Clause 4.4:

- D7-AI-1 Provenance forgery. Forged model provenance or signatures from a broken or deprecated signature scheme. Coverage includes re-signing critical artifacts with a quantum-safe algorithm.
- D7-AI-2 Harvested AI asset exposure. HNDL exposure of harvested model weights, parameters, or training data protected by quantum-vulnerable key exchange or key-wrapping.
- D7-AI-3 Inter-agent downgrade. Downgrade or silent fallback on machine-to-machine and agent-to-agent channels that removes quantum-safe protection.

> These scenarios assess cryptographic incidents arising from AI systems. They do not assess model behavior or AI risk generally.

Maturity model

Use five levels. 0 Unaware (no owner, no inventory, no roadmap). 1 Aware (talk exists, evidence does not). 2 Defined (roadmap exists, execution uneven). 3 Implementing (migration underway, metrics tracked). 4 Managed (crypto agility exists, vendors controlled). 5 Assured (tested, audited, repeatable, board-ready).

Evidence standard

QRAF requires evidence, not intent. Each assessed claim must link to at least one artifact, such as system inventories, SBOM crypto libraries, key and certificate inventories, PQC pilot results, vendor attestations, or incident runbooks and tabletop exercises.

Assessment workflow

A standard cycle, repeated quarterly: initiate, inventory (build QASI), analyze (map data longevity and crypto dependencies), score (Q-Risk snapshot), plan (roadmap and vendor actions), execute (prioritized controls and migrations), assure (test crypto agility, produce evidence pack), and report (board insert plus risk register updates).

QASI. Quantum Attack Surface and Crypto Dependency Inventory

Purpose

QASI is the cryptographic inventory required to answer, with evidence, whether the organization is exposed. It maps cryptography use, trust dependencies, and data longevity to systems and vendors. Inventory material systems first. Prioritize coverage of material systems over exhaustive precision. Validate each row with an owner.

QASI table template

Copy this structure into a spreadsheet or database. Add rows per system.

Field	Description	Example
System ID	Unique ID.	PAY-001
System name	Common name.	Payments API
Business criticality	High, Medium, Low.	High
System owner	Accountable leader.	VP Eng
Data classification	Public, Internal, Confidential, Regulated.	Regulated
Data longevity required	Years data must remain confidential.	10 years
Crypto functions used	TLS, signing, encryption at rest, PKI, tokens.	TLS, signing
Algorithms in use	RSA, ECC, AES, SHA, and so on.	RSA-2048, ECC P-256
Crypto libraries	OpenSSL, BoringSSL, libsodium, and so on.	OpenSSL 3.x
Key management	HSM, KMS, local, mixed.	Cloud KMS
Certificate dependencies	Internal PKI, public CA, both.	Public CA
Identity dependencies	SSO, IAM, OIDC, SAML.	OIDC
External interfaces	APIs, VPN, partner links.	Partner API
Vendor dependencies	Critical suppliers for crypto or comms.	Cloud provider
PQC support status	None, roadmap, pilot, available.	Roadmap
Crypto agility	Ability to swap algorithms quickly.	Partial
Exposure type	Confidentiality, integrity, authenticity.	Confidentiality
Harvest-now risk	Low, Medium, High.	High
Compensating controls	Segmentation, rotation, minimization.	Tokenization
Target remediation date	Milestone date.	2026-12
Evidence link	Artifact reference.	Ticket, report

AI systems only (new in v2.2). Capture these fields in addition for any system classified as an AI system. A non-AI system records an AI artifact class of “none.”

AI field	Description	Example
AI artifact class	Model weights, training dataset, model registry, inference endpoint, inter-agent channel, none.	Model weights
Artifact sensitivity horizon	Years the artifact must stay confidential or its provenance trustworthy.	7 years
Model signing scheme	None, RSA/ECDSA, ML-DSA, SLH-DSA, hybrid.	ECDSA P-256
Inter-agent channel protection	None, classical TLS, hybrid TLS with ML-KEM.	Classical TLS
AI artifact key-wrapping	RSA-wrapped, ECC-wrapped, ML-KEM-wrapped, hybrid.	RSA-wrapped

QASI risk flags

Add a Flag column and mark when true:

- RSA or ECC used for long-lived confidentiality with no roadmap.
- High data longevity with unclear crypto coverage.
- Vendor cannot attest to PQC roadmap.
- Certificate sprawl with unknown owners.
- Hard-coded crypto primitives or rigid hardware dependencies.
- Unknown crypto libraries, unknown versions, or missing SBOM coverage.
- **New in v2.2.** AI artifact with a sensitivity horizon beyond the planned migration date, protected by quantum-vulnerable signing or key-wrapping, with no approved migration plan.

QASI output artifacts

System coverage percentage. Count of high-longevity datasets on non-PQC paths. Count of critical vendors missing roadmap or attestation. Count of AI artifacts flagged under the v2.2 flag. Top 10 remediation targets.

Q-Risk Score. Comparable Readiness Snapshot

Purpose

Q-Risk Score is a comparable readiness snapshot rather than a forecast. It measures whether the organization is getting meaningfully safer and how it compares to peers using the same rubric.

Score structure

Total score 0 to 100, derived from five pillars.

Pillar	Weight	What good looks like
P1. Governance and accountability	20	Board cadence, owned roadmap, evidence.
P2. Crypto visibility and QASI completeness	20	Inventory coverage, validated owners.
P3. Data longevity and exposure management	20	Long-lived data mapped and prioritized.
P4. PQC migration readiness and crypto agility	25	Migration underway, agility proven.
P5. Third-party readiness	15	Critical vendors attested, contracts updated.

Scoring method

Each pillar is scored 0 to 5, then scaled by weight. Pillar score percent equals (Level divided by 5) times weight. Q-Risk Score equals the sum of pillar percent values.

Bands and interpretation

0 to 19 Exposed (no credible readiness posture). 20 to 39 Behind (plans exist, execution weak). 40 to 59 Mobilizing (execution started, uneven). 60 to 79 Advancing (measurable progress, gaps known). 80 to 100 Defensible (evidence-backed, repeatable posture).

Comparability controls

Require QASI coverage threshold before scoring above 60. Require vendor attestations for critical suppliers before scoring above 70. Require crypto agility test evidence before scoring above 80.

Pillar 5 AI-cryptographic posture (new in v2.2). Pillar weights do not change. Where a critical vendor supplies AI platform, ML infrastructure, model registry, or key management used for AI artifacts, the vendor's AI-cryptographic posture is in scope for Pillar 5 and is assessed through the Vendor Roadmap Request Pack Section G.

Reporting format

A one-page scorecard, quarterly: score and band, movement since last quarter, top three risk reducers delivered, top three exposures still open, and the vendor exceptions list.

Vendor Roadmap Request Pack

When to send

Send to all vendors that provide or materially touch identity, PKI, certificates, key management, network security, VPN, secure remote access, cloud infrastructure and managed databases, messaging, payments, transaction signing, custody, any platform storing high-longevity confidential data, and any AI platform, ML infrastructure, model registry, or key management used with AI artifacts.

Standard questions

Use these in an RFI format. Require evidence attachments.

A. Product scope and crypto footprint. B. PQC roadmap and milestones. C. Crypto agility and upgrade path. D. Testing and assurance. E. Customer obligations and support. F. Disclosures and incident readiness.

G. AI platform cryptographic posture (new in v2.2, where applicable). For suppliers of AI platforms, ML infrastructure, model registries, or key management used with AI artifacts:

No.	Question
G1	Does your AI platform, model registry, or key management service rely on quantum-vulnerable digital signatures, such as RSA or ECDSA, for model artifact signing, attestation, or provenance today?
G2	Do you support quantum-safe model signing using ML-DSA or SLH-DSA, applied through a model-signing framework such as the OpenSSF Model Signing specification or an equivalent? Provide dates and milestones.
G3	Do you support hybrid key exchange with ML-KEM for service-to-service and agent-to-agent communication in your platform?
G4	Do you provide a Cryptographic Bill of Materials covering AI artifacts and their dependencies, and will you update it on material cryptographic change?
G5	Does your key management support ML-KEM key encapsulation for wrapping symmetric keys that protect AI artifacts at rest?

Vendor attestation format

Designed to be signable by an officer. The vendor attests to identification of customer-facing cryptographic functions, an up-to-date algorithm and library inventory, a documented PQC roadmap with target dates, a supported transition path including hybrid modes, migration guidance, disclosure of material cryptographic risks, and acknowledgement that customers may rely on the attestation for oversight.

How to use responses

Accept vendor roadmap (keeps momentum, but roadmaps can slip). Contractualize milestones (creates enforceability, adds procurement friction). Dual-source or exit plan (reduces concentration risk, adds operational complexity). Compensating controls (buys time, can become fragile permanent fixtures).

Board Briefing Insert

Why this is in the board pack

Quantum risk is a timeline and dependency problem. If data must stay confidential for years, cryptography decisions today matter. If vendors control crypto upgrades, third-party controls are not optional. If the organization cannot inventory crypto dependencies, it cannot credibly claim readiness.

Board oversight objectives

Every quarter the board should require ownership (a named accountable executive), visibility (QASI coverage and top exposures), progress (PQC roadmap milestones delivered), vendors (attestations collected plus an exceptions list), and assurance (evidence of testing, including crypto agility proof points).

What we are measuring right now

- Q-Risk Score and movement since last quarter.
- QASI coverage as a percentage of critical systems inventoried.
- High-longevity data exposure: count of systems on a non-PQC path, including AI artifacts where AI systems are in scope.
- Vendor readiness: percentage of critical vendors attested, plus top exceptions.
- Crypto agility status: Not proven, Partial, or Proven.

Third-party oversight statement

Third-party risk does not transfer. It compounds. Any supplier that cannot provide a credible PQC roadmap and attestation becomes a managed exception, with an exit plan or compensating controls.

Annex A. QASI template

Informative. The fields in Clause 5.2 are required. Use the full field table in the QASI component above, and capture the AI systems-only sub-block for any system classified as an AI system.

Annex B. Q-Risk Score worksheet

Informative. The computation in Clause 6 is required. Score each pillar 0 to 5, then weight.

Pillar	Weight	Weighted contribution
Governance and accountability	20	
Crypto visibility and QASI completeness	20	
Data longevity and exposure management	20	
PQC readiness and crypto agility	25	
Third-party readiness	15	
Total	**100**	

Computation: (Level divided by 5) times Weight.

Annex C. Vendor roadmap request pack

Informative. The minimum content in Clause 7.2 is required. Use question sections A through F for all critical suppliers, and Section G for suppliers of AI platforms, ML infrastructure, model registries, or key management used with AI artifacts. Include the attestation format requiring an authorized signatory.

Annex D. Board briefing insert

Informative. The elements in Clause 8.1 are required. The quarterly insert states the Q-Risk Score and delta, QASI coverage, top exposures, vendor readiness and exceptions, crypto agility status, actions delivered and planned, board decisions requested, and exceptions requiring acknowledgement.

Annex E. Citation register

Every normative claim in this standard traces to a primary source below. Secondary and analytical inputs are listed separately and are not cited for any normative claim.

Ref	Source	Use and status
S1	NIST FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM). NIST, August 13, 2024.	Final standard. Anchors key encapsulation, hybrid key exchange, and key-wrapping (Clauses 5, 6, 9).
S2	NIST FIPS 204, Module-Lattice-Based Digital Signature Algorithm (ML-DSA). NIST, August 13, 2024.	Final standard. Anchors quantum-safe model signing (Clauses 4.4, 7).
S3	NIST FIPS 205, Stateless Hash-Based Digital Signature Standard (SLH-DSA). NIST, August 13, 2024.	Final standard. Anchors the hash-based signing alternative (Clauses 4.4, 7).
S4	NIST IR 8547 ipd, Transition to Post-Quantum Cryptography Standards. NIST, Initial Public Draft, November 12, 2024.	Initial Public Draft. The 2030 deprecation and 2035 disallowance dates are not yet binding. Cited as a trajectory, not a mandate.
S5	NSA Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). NSA, 2022.	Binding for National Security Systems. New NSS acquisitions support CNSA 2.0 from January 1, 2027. Anchors parameter sets and the federal-adjacent vendor timeline.
S6	NSA, CISA, FBI and allied agencies, AI Data Security: Best Practices for Securing Data Used to Train and Operate AI Systems. CSI, May 22, 2025 (U/OO/157249-25).	Government guidance. Recommends quantum-resistant digital signatures to authenticate training datasets and model parameters. Primary anchor for the AI-specific scope.
S7	OpenSSF Model Signing (OMS) Specification. Open Source Security Foundation, 2025.	Industry specification, not a government standard. A PKI- and algorithm-agnostic model-signing framework, not itself a post-quantum mechanism. Referenced as an example mechanism only.
Input	Cloud Security Alliance, Harvest Now, Decrypt Later: Quantum Risk to AI Infrastructure. CSA, May 18, 2026.	Analytical input only. Secondary, AI-assisted, no-modify license. Not cited for any normative claim.

Annex F. Revision history

Version	Date	Changes
2.2	June 8, 2026	Adds the AI-cryptographic intersection across the standard: QRAF Domain D7 incident scenarios (Clause 4.4), conditional QASI fields and risk flag (Clauses 5.2 and 5.3), Pillar 5 AI-cryptographic posture (Clause 6.4) and Vendor Roadmap Request Pack Section G (Clause 7). Replaces placeholder normative references with primary sources and adds the citation register (Annex E). No pillar weight changes and no change to the comparability caps at 60, 70, and 80. No new domain, no new pillar, and no standalone AI document. First published edition (June 2026).

Version	Date	Changes
2.1	Prior	Normative standard prior to the AI-cryptographic intersection additions. Established QRAF, QASI, Q-Risk Score, the Vendor Roadmap Request Pack, and the Board Briefing Insert.

Quick comparison table

A one-line summary of each component and its trade-offs.

Component	What it is	Output	Pros	Cons
QRAF	Governance and assessment framework.	Owners, cadence, evidence rules.	Board-ready and auditable.	Feels heavy without clear quick wins.
QASI	Inventory of crypto dependencies and attack surface.	System-level rows with evidence.	Turns unknowns into a plan.	Requires coordination across teams.
Q-Risk Score	Comparable snapshot.	0 to 100 score plus movement.	Enables benchmarking and momentum.	Temptation to game it without controls.
Vendor Pack	Third-party standard request and attestation.	Responses plus signed statement.	Forces vendor accountability.	Some vendors resist or stall.
Board Insert	Quarterly oversight insert.	One-page governance summary.	Keeps board engaged without noise.	Requires disciplined evidence collection.

Quantum Core Institute. Standards-first governance for post-quantum cryptography risk.