ENCRYPTORIUM

APPLIED CRYPTOGRAPHY

Post-Quantum Readiness Assessment

Cryptographic inventory, risk scoring, migration roadmap

Version 1.0

2026-04

Encryptorium

Contents

OVERVIEW

Executive summary

This document is a structured framework for evaluating an organization's readiness to migrate from quantum-vulnerable cryptography to post-quantum cryptography (PQC). It covers seven domains: cryptographic inventory, data sensitivity, standards compliance, migration readiness, vendor and supply chain dependencies, timeline assessment, and governance.

The framework produces two outputs: a domain-level maturity score (1 to 5) for each of the seven domains, and a weighted overall score that maps to a risk category (Critical, High, Moderate, or Low). The scoring rubrics aim to produce consistent results across assessors.

Who should use this: CISOs, security architects, compliance officers, IT leaders, and consultants evaluating quantum risk for their organization or clients.

What you get: A scored assessment with per-domain and overall risk ratings, per-domain maturity scores that identify which areas to address first, and specific guidance on what to do next.

How to use it: Work through each domain section. For each question, read the rubric and select the score (1 to 5) that best matches your organization. Enter scores in the companion spreadsheet (one tab per domain, score dropdowns for each question, auto-calculated domain averages and weighted overall score on the Dashboard tab). If a question does not apply to your organization, leave the score cell blank and the average will adjust automatically.

Complete this assessment collaboratively. Involve representatives from security, IT operations, software development, and procurement. No single person has visibility across all seven domains.

GUIDE

How to use this guide

Assessment process

The assessment follows four phases:

1. **Inventory.** Document what cryptographic algorithms, protocols, keys, and certificates your organization uses. This is Domain 1, and it feeds into every other domain.
2. **Score.** Work through all seven domains. Answer each question using the 1 to 5 rubric. Enter scores in the companion spreadsheet.
3. **Prioritize.** Review domain-level scores to identify where the largest gaps are. Domains with scores of 1 or 2 need immediate attention.
4. **Plan.** Use your results to build a migration roadmap. The "Next steps" section at the end of this guide provides recommendations by risk category.

Scoring mechanics

Each question uses a 1 to 5 scale:

Score	Meaning
1	No awareness or preparation
2	Aware but no action taken
3	Initial steps taken, partial coverage
4	Significant progress, most areas addressed
5	Complete coverage, documented, actively managed

Each question includes a rubric with specific criteria for each score level. Choose the level that best matches your current state. If you fall between two levels, choose the lower one.

Domain scores are the average of all question scores within that domain. The overall score is a weighted average of domain scores. Weights reflect each domain's relative importance to migration readiness (see "Scoring methodology" for the full weight table).

The overall score maps to a risk category:

Overall score	Risk category
1.0 to 2.0	Critical: immediate action required
2.1 to 3.0	High: significant gaps, prioritize remediation within 6 to 12 months
3.1 to 4.0	Moderate: targeted improvements needed
4.1 to 5.0	Low: well-prepared, maintain and monitor

Time estimate

Plan for 2 to 4 hours for organizations with some existing cryptographic documentation. Organizations starting from scratch should expect 4 to 6 hours, or may split the assessment across two sessions (domains 1-3 in the first session, domains 4-7 in the second).

Who should participate

- **Security team:** Owns the overall assessment. Leads domains 1, 2, 3, and 6.
- **IT operations:** Contributes to domains 1 (infrastructure cryptography), 4 (migration capability), and 5 (vendor dependencies).
- **Development teams:** Contributes to domains 1 (application-level cryptography), 4 (crypto-agility, CI/CD readiness).
- **Procurement:** Contributes to domain 5 (vendor PQC roadmaps, contract requirements).
- **Leadership/governance:** Contributes to domains 6 (timeline decisions) and 7 (policy, budget, ownership).
- **Compliance and legal:** Contributes to domains 3 (regulatory requirements) and 7 (policy, risk register). In healthcare, include the privacy officer.

When participants disagree on a score, discuss the evidence behind each proposed score. If agreement cannot be reached, score the lower value. The assessment is more useful when it identifies gaps than when it inflates progress.

If you cannot assemble a cross-functional group, the security team can complete an initial pass and then validate scores with other teams.

A note on standards references

This assessment references several government and standards-body publications (CNSA 2.0, NCSC guidance, BSI recommendations). CNSA 2.0 timelines are mandatory for US national security systems (NSS) and are not directly binding on commercial enterprises. We reference them throughout as planning benchmarks because they represent the most concrete public timeline for PQC migration. Where your sector has its own regulatory requirements, those take precedence. IETF protocol drafts (hybrid TLS, ML-KEM in TLS 1.3) are referenced as active standardization work; specific draft numbers and status will change as these proceed through the standards process.

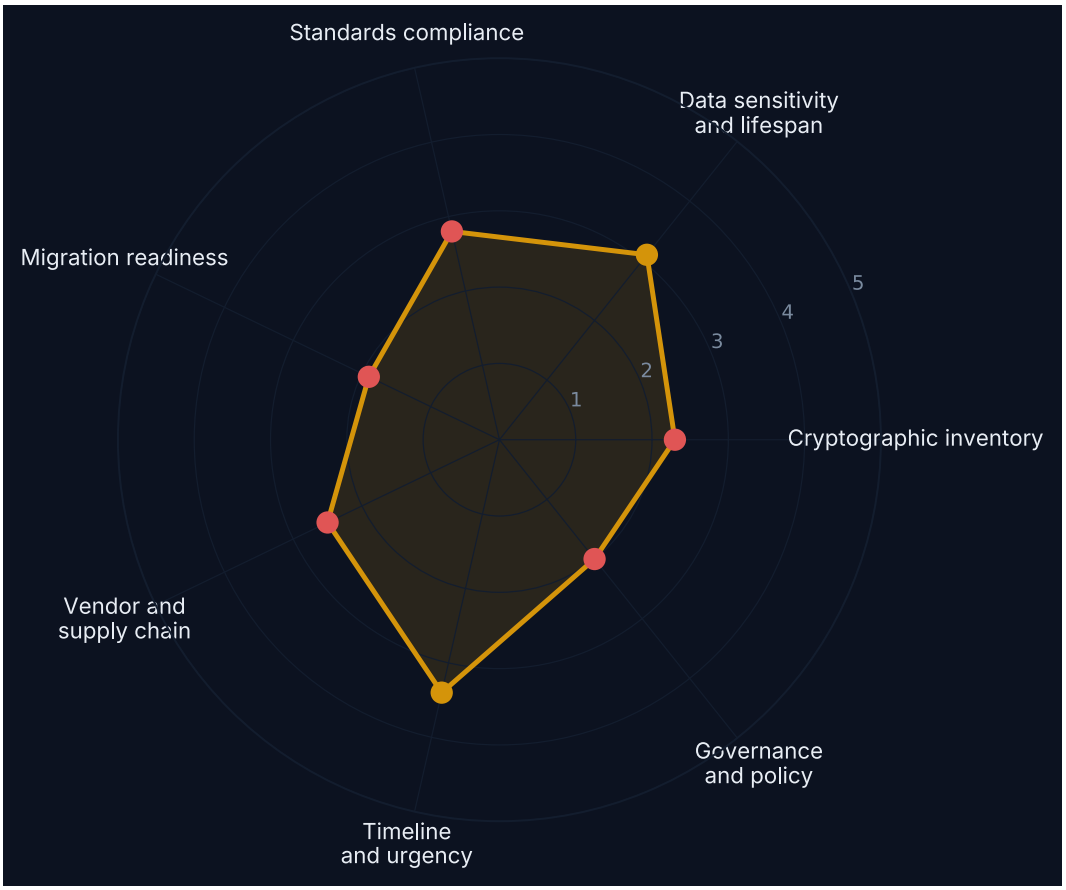
Cloud-native organizations

For organizations where the cloud provider manages most cryptography (TLS termination, key management, certificate issuance), answer questions about algorithm inventory, PKI, and key management in terms of what the provider uses and their PQC migration roadmap. "Does your organization maintain a cryptographic inventory?" includes understanding what your provider manages on your behalf. "Can your PKI support hybrid certificates?" becomes "does your cloud PKI provider's roadmap include hybrid certificate support?"

SAMPLE OUTPUT

Example: domain score visualization

The radar chart below shows an example domain score profile. Your completed assessment will produce a similar visualization highlighting strengths and gaps across all seven domains.



DOMAIN 1

Cryptographic inventory

Weight: 20% | 9 questions

Overview

Identifies what cryptographic algorithms, protocols, keys, and certificates are in use across the organization. A complete inventory is the prerequisite for any migration effort.

Why this matters

Organizations cannot migrate cryptographic dependencies they have not identified. NIST SP 1800-38B (Migration to Post-Quantum Cryptography), an NCCoE practice guide in preliminary draft, identifies cryptographic discovery as the first phase of any PQC transition. Without an inventory, risk assessment is guesswork and migration planning is impossible. The CycloneDX Cryptography Bill of Materials (CBOM) specification provides a standardized format for documenting cryptographic assets.

Quick self-assessment

Level	Description
1	No inventory exists. The organization does not know what cryptographic algorithms or protocols are in use.
2	Some awareness of major systems (e.g., TLS, VPN) but no documented inventory. Knowledge is informal and person-dependent.
3	Partial inventory covers primary systems. Primary applications and protocols are documented, but coverage gaps remain in legacy systems, embedded devices, or third-party dependencies.
4	Documented inventory covers most cryptographic dependencies across applications, infrastructure, and key management. Regular review process exists.
5	Automated, continuously updated inventory using standardized formats (e.g., CycloneDX CBOM). Integrated into CI/CD and change management. Covers all layers including hardware, firmware, and supply chain.

Assessment questions

Question 1: Does your organization maintain a documented inventory of cryptographic algorithms in use?

Score	Criteria
1	No inventory exists.
2	Informal awareness of some algorithms (e.g., 'we use AES'), but nothing documented.
3	Partial inventory lists major algorithms by system (e.g., TLS 1.2 with RSA-2048, AES-256-GCM).
4	Complete inventory documents algorithms, key lengths, and protocols across most systems.
5	Automated inventory with CycloneDX CBOM or equivalent. Updated continuously via scanning tools.

NIST CSF 2: ID.AM-01, ID.AM-02 | SP 800 53: CM-8, SC-12 | ISO 27001: A.8.24

CNSA 2: Cryptographic inventory required before migration

Question 2: Are cryptographic protocol versions (TLS, SSH, IPsec, etc.) documented across your infrastructure?

Score	Criteria
1	Protocol versions are unknown.
2	General awareness (e.g., 'we use TLS') but specific versions are not tracked.
3	Major internet-facing services have documented protocol versions. Internal services are partially covered.
4	Protocol versions documented for most services. Deprecated versions (TLS 1.0/1.1, SSHv1) identified.
5	All protocol versions documented and monitored. Automated alerts for deprecated protocol use. Upgrade schedule maintained.

NIST CSF 2: ID.AM-01, PR.DS-02 | SP 800 53: CM-8, SC-8, SC-23 | ISO 27001: A.8.24

CNSA 2: Protocol version awareness for migration planning

Question 3: Do you know where RSA, ECDSA, ECDH, and other quantum-vulnerable algorithms are used?

Score	Criteria
1	No knowledge of where specific algorithms are deployed.
2	Know that RSA/ECC are used for TLS and code signing, but no system-level mapping.
3	Quantum-vulnerable algorithms identified in primary systems (web servers, VPN, PKI).
4	Mapping covers applications, infrastructure, key management, and most third-party integrations.
5	Complete mapping of quantum-vulnerable algorithm usage with dependency analysis. Automated detection of new deployments.

NIST CSF 2: ID.AM-01, ID.RA-01 | SP 800 53: SC-12, SC-13, RA-5 | ISO 27001: A.8.24

CNSA 2: Identify quantum-vulnerable algorithms for replacement

Question 4: Is there a certificate and key management inventory?

Score	Criteria
1	No centralized awareness of certificates or keys.
2	Some certificates tracked (e.g., public web TLS), but internal and code-signing certificates are not inventoried.
3	Certificate inventory covers most externally-facing assets. Key management practices are documented for primary systems.
4	Centralized certificate lifecycle management. Key inventory covers encryption, signing, and authentication keys.
5	Automated certificate and key lifecycle management with expiry alerts, rotation policies, and audit trails. HSM inventory included.

NIST CSF 2: ID.AM-02, PR.DS-01 | SP 800 53: SC-12, SC-17 | ISO 27001: A.8.24

CNSA 2: Key management readiness for PQC key sizes

Question 5: Does the inventory cover embedded systems, IoT devices, and firmware?

Score	Criteria
1	Embedded and IoT cryptography is not considered.
2	Aware that embedded devices use cryptography, but no inventory.
3	Major embedded platforms identified (e.g., industrial controllers, medical devices), but firmware crypto is not analyzed.
4	Embedded and IoT cryptographic dependencies documented for most device classes. Firmware update capabilities assessed.
5	Complete embedded inventory including firmware-level cryptographic dependencies, update mechanisms, and hardware security module capabilities.

NIST CSF 2: ID.AM-01, ID.AM-03 | SP 800 53: CM-8, SA-4 | ISO 27001: A.8.24, A.7.4

CNSA 2: Firmware/software signing with LMS/XMSS by 2025 per CNSA 2.0

Question 6: How frequently is the cryptographic inventory reviewed and updated?

Score	Criteria
1	Never reviewed; no inventory exists.
2	Inventory was created once but has not been updated.
3	Reviewed annually or when major changes occur.
4	Reviewed quarterly. Updates triggered by system changes and vulnerability disclosures.
5	Continuously updated via automated scanning. Changes trigger review workflows. Integrated into change management.

NIST CSF 2: ID.AM-01, ID.IM-04 | SP 800 53: CM-8(3), PM-5 | ISO 27001: A.8.24

Question 7: Does your organization use automated tools to discover cryptographic usage across systems?

Score	Criteria
1	No automated discovery. Inventory is entirely manual or nonexistent.
2	Aware that scanning tools exist (e.g., CryptoSense, Keyfactor Command, custom scripts) but none deployed.
3	Automated scanning covers some systems. Results feed into a manual inventory process.
4	Automated scanning deployed across most infrastructure. Results integrated into the cryptographic inventory.
5	Continuous automated discovery integrated into CI/CD and infrastructure provisioning. New deployments automatically scanned and cataloged.

NIST CSF 2: ID.AM-01, DE.CM-09 | SP 800 53: CM-8(3), RA-5, SI-7 | ISO 27001: A.8.24
CNSA 2: Automated discovery supports migration planning | DORA: Article 9(1): ICT asset identification

Question 8: Are cryptographic dependencies between systems mapped (e.g., which applications depend on which key management services)?

Score	Criteria
1	No understanding of inter-system cryptographic dependencies.
2	Aware that systems share cryptographic dependencies (e.g., multiple apps use the same CA), but not documented.
3	Major dependency chains identified (e.g., application servers depend on specific HSMs, databases use shared key wrap keys).
4	Dependency mapping covers most systems. Impact analysis available for key infrastructure components (CA, HSM, KMS).
5	Complete cryptographic dependency graph maintained. Impact analysis automated. Migration sequencing informed by dependency order.

NIST CSF 2: ID.AM-04, ID.RA-03 | SP 800 53: CM-8, SA-4, CP-2 | ISO 27001: A.8.24
CNSA 2: Dependency mapping required for migration sequencing

Question 9: Do you have visibility into the cryptographic algorithms used by cloud-managed services (cloud KMS, managed TLS, cloud HSM)?

Score	Criteria
1	No visibility into cloud provider cryptographic choices.
2	Aware that cloud providers manage cryptography on your behalf, but specific algorithms unknown.
3	Cloud KMS and managed TLS configurations documented for primary cloud accounts. Algorithm choices known for major services.
4	Cryptographic configurations documented across all cloud providers. Customer-managed key options evaluated.
5	Complete cloud cryptographic visibility including managed service defaults, customer-managed key configurations, and provider PQC roadmap alignment.

NIST CSF 2: ID.AM-01, ID.AM-05 | SP 800 53: CM-8, SC-12, SA-9 | ISO 27001: A.8.24, A.5.23 | CNSA 2: Cloud crypto visibility for migration planning | DORA: Article 28: ICT third-party risk

Standards references

- NIST SP 1800-38B, Section 3: Cryptographic Discovery
- CycloneDX CBOM Specification v1.6
- CISA Post-Quantum Cryptography Initiative: Inventory Phase

What organizations typically miss

Most organizations underestimate the breadth of their cryptographic footprint. TLS and VPN configurations are usually known, but cryptographic dependencies in databases, message queues, file encryption, code signing, IoT firmware, and third-party SaaS integrations are frequently missed.

DOMAIN 2

Data sensitivity and lifespan

Weight: 15% | 7 questions

Overview

Evaluates the sensitivity of data protected by current cryptographic mechanisms and its required confidentiality lifespan. This determines exposure to harvest-now, decrypt-later (HNDL) attacks.

Why this matters

Adversaries with access to network traffic or encrypted stores can capture ciphertext today and decrypt it once a cryptographically relevant quantum computer (CRQC) becomes available. Data with long confidentiality requirements (medical records, state secrets, financial data, intellectual property) is at risk now, not when quantum computers arrive. CNSA 2.0 and NCSC guidance both identify data classification as a critical input to migration prioritization.

Quick self-assessment

Level	Description
1	No classification of data by sensitivity or lifespan. No awareness of harvest-now, decrypt-later risk.
2	General data classification exists (e.g., public/internal/confidential) but is not linked to cryptographic protection or lifespan analysis.
3	High-sensitivity data categories identified. Some analysis of which data requires long-term confidentiality (10+ years).
4	Data classification includes cryptographic protection mapping and lifespan analysis. HNDL risk assessed for sensitive categories.
5	Complete data lifecycle management with cryptographic protection requirements. HNDL risk quantified per data class. Migration priority derived from lifespan analysis.

Assessment questions

Question 1: Does your organization classify data by sensitivity level with defined confidentiality requirements?

Score	Criteria
1	No data classification scheme exists.
2	Basic classification (e.g., public/internal/confidential) exists but is inconsistently applied.
3	Data classification is applied to most assets. Sensitivity levels have defined handling requirements.
4	Classification includes specific confidentiality timeframes (e.g., 'confidential for 10 years post-creation').
5	Mature data lifecycle management with automated classification, defined retention periods, and regular review.

NIST CSF 2: ID.AM-07, PR.DS-01 | SP 800 53: RA-2, SC-28 | ISO 27001: A.5.12, A.5.13
CNSA 2: Data classification drives migration prioritization | DORA: Article 13: Data classification

Question 2: Have you identified data categories with long-term confidentiality requirements (10+ years)?

Score	Criteria
1	No analysis of data lifespan requirements.
2	Aware that some data is long-lived, but no formal identification.
3	Key long-lived data categories identified (e.g., medical records, financial archives, IP).
4	Long-lived data mapped to specific systems and cryptographic protections.
5	Complete mapping of long-lived data with quantified risk exposure based on estimated CRQC timelines.

NIST CSF 2: ID.AM-07, ID.RA-01 | SP 800 53: RA-2, SC-28 | ISO 27001: A.5.12
CNSA 2: Long-lived data prioritized for early migration

Question 3: Is your organization aware of harvest-now, decrypt-later (HNDL) risk?

Score	Criteria
1	No awareness of HNDL as a threat vector.
2	Concept is known at the security leadership level but not assessed.
3	HNDL risk discussed in threat models. General understanding of which data categories are exposed.
4	HNDL risk formally assessed. High-value data flows analyzed for interception exposure.
5	HNDL risk quantified and incorporated into risk register. Network traffic analysis identifies exposed data flows. Mitigation timeline established.

NIST CSF 2: ID.RA-01, ID.RA-02 | SP 800 53: RA-3, RA-5 | ISO 27001: A.5.7 | CNSA 2: HNDL is the primary driver for early action

Question 4: Are data-at-rest encryption mechanisms mapped to the data they protect?

Score	Criteria
1	No mapping between encryption mechanisms and data assets.
2	Know that databases and file systems use encryption, but specific mechanisms are not mapped to data classes.
3	Major data stores mapped to encryption mechanisms (e.g., 'customer DB uses AES-256, TDE with RSA key wrap').
4	Most data-at-rest encryption mapped including key management mechanisms and algorithm details.
5	Complete mapping with automated discovery. Key hierarchy documented. Quantum-vulnerable key wrapping mechanisms identified.

NIST CSF 2: PR.DS-01 | SP 800 53: SC-28, SC-12 | ISO 27001: A.8.24

CNSA 2: Data-at-rest encryption to transition to CNSA 2.0 algorithms (AES-256); key wrapping with ML-KEM-1024 by 2030

Question 5: Are data-in-transit protections assessed for quantum vulnerability?

Score	Criteria
1	No assessment of transit encryption against quantum threats.
2	Aware that TLS and VPN use quantum-vulnerable key exchange, but no formal assessment.
3	Primary data flows assessed. Internet-facing TLS and VPN configurations reviewed for quantum-vulnerable algorithms.
4	Internal and external data flows assessed. Key exchange mechanisms (RSA, ECDH) identified across most transit protections.
5	Complete transit encryption assessment with protocol-level detail. Hybrid key exchange evaluation underway or deployed for high-priority flows.

NIST CSF 2: PR.DS-02 SP 800 53: SC-8, SC-13 ISO 27001: A.8.24
CNSA 2: Key establishment with ML-KEM-1024 by 2030 per CNSA 2.0

Question 6: Is data-at-rest encryption assessed at the key hierarchy level (envelope encryption, key wrapping, backup encryption)?

Score	Criteria
1	No understanding of key hierarchy for data-at-rest encryption.
2	Aware that encryption uses key hierarchies (e.g., data encryption keys wrapped by master keys), but not assessed.
3	Key hierarchy documented for major data stores. Master key algorithms identified (e.g., RSA key wrap for TDE).
4	Key hierarchy assessed across most systems including backup and archive encryption. Quantum-vulnerable key wrap algorithms flagged.
5	Complete key hierarchy analysis. All layers assessed for quantum vulnerability. Migration plan addresses each layer from root keys down.

NIST CSF 2: PR.DS-01 SP 800 53: SC-12, SC-28 ISO 27001: A.8.24
CNSA 2: Key wrapping mechanisms must transition to quantum-resistant algorithms

Question 7: Are data-in-transit protections differentiated by sensitivity level and network segment (internal east-west, external north-south)?

Score	Criteria
1	No differentiation of transit protection by data sensitivity or network segment.
2	External traffic uses TLS. Internal traffic encryption is inconsistent or absent.
3	External traffic encrypted with documented configurations. Internal east-west encryption deployed for some sensitive segments (e.g., service mesh TLS, database connections).
4	Transit protection mapped by network segment and data sensitivity. API gateway, service mesh, and internal service encryption configurations documented.
5	Complete transit protection matrix by data sensitivity and network segment. Internal and external traffic encryption aligned to quantum risk priority. High-sensitivity internal flows prioritized for PQC migration.

NIST CSF 2: PR.DS-02, PR.IR-01 | SP 800 53: SC-8, SC-8(1) | ISO 27001: A.8.24, A.8.20

CNSA 2: Network encryption to transition to CNSA 2.0 algorithms; timelines vary by equipment category (networking 2026, niche/large systems 2030)

Standards references

- NSA CNSA 2.0: Data-at-rest timeline (ML-KEM-1024 for key establishment by 2030; AES-256 for symmetric encryption)
- NCSC: Preparing for quantum-safe cryptography (November 2020)
- ETSI TR 103 619: Quantum-Safe Cryptography; Migration Strategies

What organizations typically miss

Organizations often have data classification policies but do not connect them to cryptographic protection analysis. The gap is not knowing which data classes are protected by quantum-vulnerable algorithms and how long that protection needs to last. Healthcare, financial, and government data frequently has confidentiality requirements exceeding 20 years.

DOMAIN 3

Standards compliance

Weight: 10% | 6 questions

Overview

Measures alignment with published post-quantum cryptography standards and guidance from NIST, NSA (CNSA 2.0), NCSC, BSI, and ETSI.

Why this matters

NIST finalized the first PQC standards in August 2024: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA). CNSA 2.0 sets mandatory timelines for US national security systems. Organizations that track these standards can plan migration around stable, vetted algorithms rather than reacting to ad hoc vendor announcements. Compliance with these standards is increasingly expected by auditors and regulators.

Quick self-assessment

Level	Description
1	No awareness of PQC standards or guidance.
2	Aware that NIST has published PQC standards, but no organizational response.
3	Relevant standards identified. Internal briefings or assessments reference FIPS 203/204/205 and CNSA 2.0.
4	Standards requirements mapped to organizational systems. Gap analysis performed. Migration timelines matched to CNSA 2.0.
5	Active standards tracking across NIST, IETF, NCSC, and sector-specific regulators. Organizational migration plan matched to published timelines. Participating in industry working groups.

Assessment questions

Question 1: Is your organization aware of the NIST post-quantum cryptography standards (FIPS 203, 204, 205)?

Score	Criteria
1	No awareness of NIST PQC standards.
2	Heard of 'post-quantum' but cannot name specific standards.
3	Security team is aware of FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA).
4	Standards reviewed in detail. Implications for organizational systems assessed.
5	Standards tracked actively. Internal documentation maps FIPS requirements to organizational cryptographic usage. NIST Round 4 outcome (HQC selected March 2025) tracked for future standardization.

NIST CSF 2: GV.RM-01 | SP 800 53: SC-13 | ISO 27001: A.8.24

CNSA 2: CNSA 2.0 approves ML-KEM-1024, ML-DSA-87, LMS/XMSS; SLH-DSA (FIPS 205) is not CNSA 2.0 approved

Question 2: Has your organization assessed alignment with published PQC migration timelines (e.g., CNSA 2.0, NCSC guidance)?

Score	Criteria
1	No awareness of CNSA 2.0.
2	Aware that CNSA 2.0 exists, but timelines not reviewed.
3	CNSA 2.0 timelines reviewed. Aware of category-based dates (e.g., LMS/XMSS for firmware signing by 2025, ML-KEM-1024 for key establishment by 2030).
4	Organizational migration plan references CNSA 2.0 timelines. Gap analysis identifies which deadlines are at risk.
5	Migration milestones matched to CNSA 2.0 and other relevant guidance (NCSC, BSI). Regular progress reviews against published timelines.

NIST CSF 2: GV.RM-01, GV.RM-02 | SP 800 53: SC-13, PM-9 | ISO 27001: A.8.24, A.5.36

CNSA 2: Category-based timelines: firmware/software signing (LMS/XMSS) by 2025, key establishment (ML-KEM-1024) by 2030, exclusive use by 2031 (NSS), full transition by 2035

Question 3: Are sector-specific regulatory requirements for PQC migration identified?

Score	Criteria
1	No awareness of sector-specific PQC requirements.
2	Aware that regulators may issue PQC guidance, but none tracked.
3	Key regulatory bodies identified (e.g., PCI DSS for payments, HIPAA for healthcare, FedRAMP for government).
4	Sector-specific PQC requirements documented. Compliance timeline established.
5	Active engagement with sector regulators. Participating in industry consultations on PQC requirements. Compliance plan reviewed by legal and audit teams.

NIST CSF 2: GV.OC-03 | SP 800 53: SC-13, SA-9 | ISO 27001: A.5.31, A.5.36
CNSA 2: Sector-specific timelines may be earlier than CNSA 2.0 defaults | DORA: Article 5: ICT risk management governance

Question 4: Does your organization track IETF post-quantum protocol standards (hybrid TLS, post-quantum key exchange)?

Score	Criteria
1	No awareness of IETF PQC work.
2	Aware that TLS and other protocols will need PQC updates, but not tracking specific drafts.
3	Key IETF drafts identified (e.g., hybrid key exchange, ML-KEM in TLS 1.3).
4	IETF PQC work tracked. Evaluation of hybrid key exchange approaches underway.
5	Active tracking of IETF PQC standardization. Testing hybrid TLS implementations. Providing feedback to working groups or participating in interoperability testing.

NIST CSF 2: GV.RM-01 | SP 800 53: SC-8, SC-13 | ISO 27001: A.8.24 | CNSA 2: Protocol-level migration required

Question 5: Is there a process for incorporating new PQC standards into organizational policy as they are published?

Score	Criteria
1	No process for standards adoption.
2	Standards adoption is ad hoc, triggered by audits or incidents.
3	Informal process exists. New standards are reviewed when the security team becomes aware of them.
4	Defined process for evaluating and adopting new cryptographic standards. Designated owner for PQC standards tracking.
5	Formal standards adoption process integrated into governance framework. Automatic alerts for new publications. Review and adoption timeline defined (e.g., assess within 90 days of publication).

NIST CSF 2: GV.RM-01, GV.PO-01 | SP 800 53: SC-13, SA-8 | ISO 27001: A.5.1, A.8.24

Question 6: Has your organization mapped sector-specific compliance requirements to specific systems and begun collecting compliance evidence?

Score	Criteria
1	No mapping of compliance requirements to systems.
2	General awareness of which regulations apply, but no system-level mapping.
3	Key systems mapped to applicable compliance frameworks. Evidence collection is informal.
4	Compliance requirements mapped to systems with documented evidence. Gap analysis identifies where cryptographic controls fall short.
5	Automated compliance evidence collection. Cryptographic control status tracked per system per framework. Audit-ready documentation maintained.

NIST CSF 2: GV.OC-03, ID.GV-01 | SP 800 53: CA-2, CA-7, SC-13 | ISO 27001: A.5.31, A.5.35, A.5.36

CNSA 2: Evidence collection supports audit readiness for CNSA 2.0 deadlines

DORA: Article 5: ICT risk management governance, Article 6: ICT risk management framework

Standards references

- NIST FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)
- NIST FIPS 204: Module-Lattice-Based Digital Signature Algorithm (ML-DSA)
- NIST FIPS 205: Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)
- NSA CNSA 2.0 Cybersecurity Advisory (September 2022, updated April 2024)
- NCSC: Next steps in preparing for post-quantum cryptography (November 2023, updated August 2024)
- BSI TR-02102-1: Cryptographic Mechanisms (PQC recommendations)

What organizations typically miss

Many organizations are aware of "post-quantum cryptography" as a concept but have not read the actual standards or mapped CNSA 2.0 timelines to their own systems. The gap between awareness and actionable compliance is where most organizations stall.

DOMAIN 4

Migration readiness

Weight: 20% | 10 questions

Overview

Assesses the organization's technical capability to transition from quantum-vulnerable algorithms to post-quantum alternatives. Covers crypto-agility, key management flexibility, PKI readiness, and testing infrastructure.

Why this matters

Identifying risk is only useful if the organization can act on it. Migration readiness determines how quickly and safely an organization can deploy post-quantum algorithms once the decision is made. Crypto-agility, the ability to swap cryptographic algorithms without redesigning systems, is the single most important technical enabler. Organizations with rigid cryptographic dependencies face multi-year migration timelines.

Quick self-assessment

Level	Description
1	No consideration of cryptographic migration. Algorithms are hardcoded throughout systems.
2	Aware that migration will be needed, but no assessment of migration capability.
3	Some systems evaluated for crypto-agility. Pilot testing of PQC algorithms initiated.
4	Migration capability assessed across most systems. Crypto-agility improvements underway. PQC testing environment established.
5	Crypto-agile architecture deployed. PQC algorithms tested and validated. Migration playbook documented with rollback procedures.

Assessment questions

Question 1: Are cryptographic algorithms configurable rather than hardcoded in your systems?

Score	Criteria
1	Algorithms are hardcoded. No configuration capability.
2	Some systems allow algorithm configuration (e.g., TLS cipher suites), but most are fixed.
3	Major systems have configurable cryptography. Some legacy or embedded systems remain hardcoded.
4	Most systems support algorithm configuration. Crypto-agility is a design requirement for new systems.
5	Crypto-agile architecture across all systems. Algorithm changes require configuration updates, not code changes. Centralized cryptographic policy enforcement.

NIST CSF 2: PR.DS-01, PR.DS-02 | SP 800 53: SC-12, SC-13, SA-8 | ISO 27001: A.8.24

CNSA 2: Crypto-agility is prerequisite for meeting migration timelines

Question 2: Can your PKI infrastructure support post-quantum or hybrid certificates?

Score	Criteria
1	PKI capabilities unknown or not assessed for PQC readiness.
2	Aware that PKI will need updating, but no assessment performed.
3	PKI vendor contacted about PQC roadmap. Basic understanding of hybrid certificate support timelines.
4	PKI readiness assessed. Migration path identified. Testing hybrid certificates in non-production environment.
5	PKI supports hybrid or post-quantum certificates. Testing complete. Rollout plan in place.

NIST CSF 2: PR.DS-01 | SP 800 53: SC-12, SC-17 | ISO 27001: A.8.24

CNSA 2: PKI must support ML-DSA-87 certificates; large PKI systems have until 2030 per CNSA 2.0

Question 3: Has your organization tested any post-quantum algorithms (ML-KEM, ML-DSA, SLH-DSA) in a lab or staging environment?

Score	Criteria
1	No PQC testing performed.
2	Aware of PQC algorithms but no testing initiated.
3	Initial testing of one or more PQC algorithms in an isolated lab environment.
4	PQC algorithms tested in staging environments that mirror production. Performance impact measured.
5	PQC algorithms validated in staging and pilot production. Performance baselines established. Compatibility with existing systems confirmed.

NIST CSF 2: PR.DS-01, PR.IP-12 | SP 800 53: SC-13, SA-11 | ISO 27001: A.8.24 | CNSA 2: Testing required before deployment | DORA: Article 11: ICT system testing

Question 4: Is there a process for evaluating the performance impact of PQC algorithm migration?

Score	Criteria
1	Performance impact not considered.
2	Aware that PQC algorithms have different performance characteristics (larger keys, different latency) but not measured.
3	Performance benchmarks reviewed from published literature (e.g., NIST PQC performance data).
4	Organization-specific performance testing underway. Latency, bandwidth, and CPU impact measured for critical systems.
5	Performance testing complete across all targeted systems. Capacity planning incorporates PQC overhead. Optimization strategies identified.

NIST CSF 2: PR.DS-01 | SP 800 53: SC-13, SA-8 | ISO 27001: A.8.24

Question 5: Do your key management systems support the new key sizes and formats required by PQC algorithms?

Score	Criteria
1	Key management capabilities not assessed for PQC.
2	Aware that PQC keys are larger (e.g., ML-KEM-768 public key is 1,184 bytes vs. 32 bytes for X25519), but impact not evaluated.
3	Key management system evaluated for PQC compatibility. Known limitations identified.
4	Key management upgrades planned or underway to support PQC key sizes. HSM vendor roadmap reviewed.
5	Key management systems support PQC key formats. HSMs updated or replaced. Key generation, storage, and distribution tested with PQC algorithms.

NIST CSF 2: PR.DS-01 | SP 800 53: SC-12 | ISO 27001: A.8.24 | CNSA 2: Key management must support PQC key sizes

Question 6: Is there a rollback plan if a PQC migration causes operational issues?

Score	Criteria
1	No rollback planning.
2	General awareness that rollback may be needed, but no plan.
3	Rollback approach discussed. Major systems have identified fallback configurations.
4	Documented rollback procedures for each migration phase. Tested in staging.
5	Rollback procedures tested and validated. Hybrid deployment (classical + PQC) maintained during transition to enable safe rollback.

NIST CSF 2: PR.IP-12, RC.RP-01 | SP 800 53: CP-2, CP-10 | ISO 27001: A.8.24, A.5.30 | DORA: Article 11: ICT system testing

Question 7: Are development and deployment pipelines ready to incorporate PQC libraries and configurations?

Score	Criteria
1	No consideration of PQC in development pipelines.
2	Aware that PQC libraries will be needed (e.g., liboqs, AWS-LC, BoringSSL PQC), but not evaluated.
3	PQC libraries evaluated. Compatibility with build systems assessed.
4	PQC libraries integrated into development environments. CI/CD pipelines can build and test with PQC configurations.
5	PQC library management automated. Dependency scanning includes PQC readiness checks. Cryptographic policy enforced in CI/CD.

NIST CSF 2: PR.DS-01, PR.IP-12 | SP 800 53: SA-8, SA-15 | ISO 27001: A.8.24, A.8.25

Question 8: Has your organization assessed cryptographic migration readiness for OT, ICS, or SCADA environments?

Score	Criteria
1	OT/ICS environments not considered in PQC planning.
2	Aware that OT/ICS systems use cryptography, but migration constraints not assessed.
3	Major OT/ICS platforms identified. Unique constraints documented (safety requirements, long equipment lifecycles, air-gapped networks).
4	OT/ICS cryptographic dependencies inventoried. Vendor firmware update capabilities assessed. Migration approach accounts for safety and availability constraints.
5	OT/ICS PQC migration plan developed with input from operational teams. Vendor PQC roadmaps verified. Parallel testing completed without disrupting operations.

NIST CSF 2: PR.DS-01, ID.AM-01 | SP 800 53: SC-12, SC-13, SA-4 | ISO 27001: A.8.24
CNSA 2: OT systems subject to same migration timelines

Question 9: Does your organization have an incident response capability for cryptographic failures (e.g., newly discovered algorithm vulnerability, key compromise)?

Score	Criteria
1	No cryptographic incident response capability.
2	General incident response process exists, but no specific procedures for cryptographic failures.
3	Cryptographic incidents recognized as a category. Response involves manual assessment and ad hoc remediation.
4	Cryptographic IR playbook documents response procedures for algorithm deprecation, key compromise, and certificate revocation. Communication plan defined.
5	Tested cryptographic IR capability. Tabletop exercises completed for scenarios including emergency algorithm rotation. Response time targets defined and monitored.

NIST CSF 2: RS.RP-01, RS.AN-01 | SP 800 53: IR-4, IR-5, SC-12 | ISO 27001: A.5.24, A.5.26

DORA: Article 17: ICT-related incident management

Question 10: Has your organization planned for hybrid deployment (running classical and post-quantum algorithms simultaneously during transition)?

Score	Criteria
1	No consideration of hybrid deployment.
2	Aware of hybrid approaches (e.g., hybrid TLS, composite certificates) but not evaluated.
3	Hybrid deployment strategy discussed. Understood that hybrid provides backward compatibility during transition.
4	Hybrid deployment plan documented for primary systems. Testing hybrid TLS or hybrid key exchange in staging.
5	Hybrid deployment validated and ready for production. Backward compatibility confirmed. Transition from hybrid to PQC-only planned with defined triggers.

NIST CSF 2: PR.DS-01, PR.DS-02 | SP 800 53: SC-8, SC-12, SC-13 | ISO 27001: A.8.24

CNSA 2: Hybrid acceptable during transition; CNSA 2.0 timelines are category-based (software signing, networking, PKI each have different dates); exclusive use by 2031 (NSS)

Standards references

- NIST SP 1800-38B: Migration to Post-Quantum Cryptography
- NIST IR 8547: Transition to Post-Quantum Cryptography Standards (draft, November 2024)
- IETF RFC 9370: Multiple Key Exchanges in the Internet Key Exchange Protocol

What organizations typically miss

Crypto-agility is often assumed but rarely tested. Organizations discover during migration that algorithms are hardcoded in configuration files, embedded in firmware, or baked into vendor appliances that cannot be updated. PKI infrastructure is a common bottleneck: many CAs do not yet support post-quantum or hybrid certificates.

DOMAIN 5

Vendor and supply chain

Weight: 15% | 7 questions

Overview

Evaluates the organization's understanding of and influence over cryptographic dependencies in third-party software, hardware, and services.

Why this matters

Most organizations do not implement cryptography directly. They depend on operating systems, cloud providers, SaaS platforms, network appliances, and embedded device vendors for cryptographic capabilities. If a vendor does not support PQC migration, the organization cannot migrate that dependency regardless of its own readiness. Supply chain cryptographic risk is a growing focus of CISA guidance and the CycloneDX CBOM specification.

Quick self-assessment

Level	Description
1	No awareness of vendor cryptographic dependencies.
2	Recognize that vendors handle most cryptography, but no assessment of vendor PQC readiness.
3	Critical vendors identified (OS, cloud, network, PKI). Some vendors contacted about PQC roadmaps.
4	Vendor PQC readiness assessed for critical dependencies. Procurement criteria updated to include PQC requirements.
5	Complete vendor PQC assessment. Contractual PQC requirements in place. Alternative vendors identified for non-compliant dependencies. CycloneDX CBOM requested from critical suppliers.

Assessment questions

Question 1: Have you identified which of your vendors and suppliers have cryptographic dependencies?

Score	Criteria
1	No identification of vendor cryptographic dependencies.
2	General awareness that vendors handle cryptography, but no specific mapping.
3	Critical vendors with cryptographic dependencies identified (cloud providers, OS, PKI, VPN/firewall vendors).
4	Complete mapping of vendor cryptographic dependencies across categories (SaaS, IaaS, hardware, firmware).
5	Automated vendor cryptographic dependency tracking. CycloneDX CBOM received from critical suppliers.

NIST CSF 2: GV.SC-01, GV.SC-04 | SP 800 53: SA-9, SR-3 | ISO 27001: A.5.19, A.5.21
CNSA 2: Vendor dependencies constrain migration timeline | DORA: Article 28: ICT third-party risk

Question 2: Have you assessed your critical vendors' PQC migration readiness and roadmaps?

Score	Criteria
1	No vendor PQC assessment.
2	Assume vendors will handle PQC, but none contacted.
3	Critical vendors contacted about PQC roadmaps. Some responses received.
4	PQC readiness assessed for most critical vendors. Roadmaps compared to organizational migration timeline.
5	All critical vendors assessed. PQC roadmaps documented and tracked. Escalation process for vendors behind schedule.

NIST CSF 2: GV.SC-04, GV.SC-05 | SP 800 53: SA-9, SR-6 | ISO 27001: A.5.19, A.5.22
CNSA 2: Vendor roadmaps must align with CNSA 2.0 timelines
DORA: Article 28: ICT third-party risk, Article 30: Key contractual provisions

Question 3: Do procurement and vendor management processes include PQC readiness criteria?

Score	Criteria
1	No PQC criteria in procurement.
2	Aware that PQC should be a procurement consideration, but not implemented.
3	PQC readiness included as a discussion point in vendor evaluations for security-critical purchases.
4	PQC readiness criteria defined in procurement policies. New vendors assessed for cryptographic agility.
5	PQC readiness is a contractual requirement. Existing contracts reviewed and amended. SLA includes PQC migration timelines.

NIST CSF 2: GV.SC-02, GV.SC-05 | SP 800 53: SA-4, SA-9, SR-3 | ISO 27001: A.5.19, A.5.20 | DORA: Article 28: ICT third-party risk, Article 30: Key contractual provisions

Question 4: Are there contingency plans for vendors that cannot or will not migrate to PQC in your required timeline?

Score	Criteria
1	No contingency planning.
2	Recognize the risk, but no alternatives identified.
3	Alternative vendors identified for the most critical dependencies.
4	Contingency plans documented for critical vendor dependencies. Migration to alternatives assessed for feasibility and cost.
5	Contingency plans tested. Alternative solutions validated. Budget allocated for vendor transitions where necessary.

NIST CSF 2: GV.SC-04, GV.SC-07 | SP 800 53: SA-9, CP-2 | ISO 27001: A.5.19, A.5.30 | DORA: Article 28: ICT third-party risk

Question 5: Can you request or generate a Cryptographic Bill of Materials (CBOM) for your critical vendor products?

Score	Criteria
1	No awareness of CBOM.
2	Aware of the CBOM concept but no requests made.
3	CBOM requested from one or more critical vendors. Understanding of CycloneDX CBOM format.
4	CBOMs received from critical vendors. Internal CBOM generation capability for proprietary software.
5	CBOM integrated into vendor management and risk assessment. Automated CBOM analysis for cryptographic vulnerability detection.

NIST CSF 2: GV.SC-04, ID.AM-02 | SP 800 53: SR-3, SR-4, CM-8 | ISO 27001: A.5.19
CNSA 2: CBOM provides visibility for migration planning | DORA: Article 28: ICT third-party risk

Question 6: Do you have visibility into the cryptographic algorithms used by your cloud providers for managed services?

Score	Criteria
1	No visibility into cloud provider cryptographic implementations.
2	Assume cloud providers use strong encryption, but specific algorithms unknown.
3	Documented which cloud services handle cryptography on your behalf (managed databases, KMS, load balancers, CDN). Default algorithms identified for major services.
4	Cloud provider cryptographic configurations documented across all providers. Customer-managed key options evaluated. Provider PQC roadmaps requested.
5	Complete cloud cryptographic transparency. Provider PQC roadmaps tracked and compared to organizational timeline. Contractual requirements for PQC migration in place.

NIST CSF 2: GV.SC-04, ID.AM-05 | SP 800 53: SA-9, SC-12, SC-13 | ISO 27001: A.5.23, A.8.24
CNSA 2: Cloud provider migration timelines affect organizational compliance
DORA: Article 28: ICT third-party risk, Article 29: Preliminary assessment

Question 7: Have third-party libraries and frameworks been assessed for cryptographic dependencies and PQC readiness?

Score	Criteria
1	No assessment of third-party library cryptographic dependencies.
2	Aware that libraries like OpenSSL, BoringSSL, and language-specific crypto modules handle cryptography, but versions and capabilities not tracked.
3	Major cryptographic libraries identified and versions documented. PQC support timelines reviewed for key libraries.
4	Third-party library cryptographic dependencies mapped across applications. Upgrade paths to PQC-capable versions identified.
5	Automated dependency scanning flags cryptographic libraries and their PQC readiness. Upgrade schedule aligned with library release cycles and organizational migration timeline.

NIST CSF 2: GV.SC-04, ID.AM-02 | SP 800 53: SA-4, SR-3, SI-2 | ISO 27001: A.5.19, A.8.24 | CNSA 2: Library PQC support required for implementation | DORA: Article 28: ICT third-party risk

Standards references

- CycloneDX CBOM Specification v1.6 (supply chain cryptographic transparency)
- CISA Post-Quantum Cryptography Initiative (vendor engagement guidance)
- NIST SP 1800-38B, Section 4: Vendor and Third-Party Considerations

What organizations typically miss

Organizations assume vendors will handle the PQC transition without verifying roadmaps or timelines. Cloud providers, OS vendors, and network appliance manufacturers are at different stages of PQC readiness. Contractual requirements for PQC support are rare; most organizations have no leverage to accelerate vendor migration.

DOMAIN 6

Timeline and urgency

Weight: 10% | 6 questions

Overview

Assesses the organization's understanding of quantum computing threat timelines and how they relate to the organization's specific risk horizon.

Why this matters

Quantum threat timelines are uncertain, but the window for action is not. Migration to post-quantum cryptography takes years, not months. Organizations must begin planning based on conservative timeline estimates rather than waiting for certainty. The "harvest-now, decrypt-later" threat means that for long-lived sensitive data, the threat is already active regardless of when a cryptographically relevant quantum computer (CRQC) arrives.

Quick self-assessment

Level	Description
1	No awareness of quantum computing timeline or its relevance to cryptographic security.
2	Vaguely aware that quantum computers may affect encryption 'someday,' but no organizational assessment.
3	Timeline awareness at the security leadership level. Understand that migration takes years and should begin now.
4	Organization-specific risk horizon defined based on data sensitivity, regulatory requirements, and estimated CRQC timelines.
5	Quantified risk model incorporating multiple CRQC timeline scenarios. Migration timeline accounts for organizational complexity and vendor dependencies.

Assessment questions

Question 1: Does your organization have a stated position on quantum computing risk timelines?

Score	Criteria
1	No organizational position on quantum risk.
2	Individual awareness exists, but no organizational stance.
3	Security leadership has a working estimate (e.g., 'CRQC possible within 10-15 years; migration should start now').
4	Documented organizational position on quantum risk timeline. Communicated to relevant stakeholders.
5	Risk timeline model with multiple scenarios (optimistic, expected, conservative). Regularly updated based on published research and industry consensus.

NIST CSF 2: GV.RM-01, ID.RA-01 | SP 800 53: RA-3, PM-9 | ISO 27001: A.5.7

CNSA 2: CNSA 2.0 provides the baseline timeline for NSS

Question 2: Has your organization estimated how long its PQC migration will take?

Score	Criteria
1	No migration timeline estimated.
2	Assume migration is a 'someday' task with no time estimate.
3	Rough estimate exists (e.g., '3-5 years for full migration'). Major phases identified.
4	Detailed migration timeline with milestones, dependencies, and resource requirements.
5	Migration timeline validated against vendor roadmaps, regulatory deadlines, and organizational change capacity. Regularly reviewed and adjusted.

NIST CSF 2: GV.RM-02 | SP 800 53: PM-9, SA-8 | ISO 27001: A.5.8

CNSA 2: Migration duration must fit within CNSA 2.0 deadlines

Question 3: Is the 'harvest-now, decrypt-later' timeline factored into your urgency assessment?

Score	Criteria
1	HNDL not considered in timeline planning.
2	HNDL acknowledged but not factored into prioritization.
3	HNDL risk influences prioritization of high-sensitivity data protection.
4	Migration timeline for high-sensitivity data adjusted based on HNDL risk. These systems are prioritized for early migration.
5	HNDL risk quantified for each data class. Migration sequencing optimized to address highest HNDL exposure first.

NIST CSF 2: ID.RA-01, ID.RA-04 | SP 800 53: RA-3 | ISO 27001: A.5.7

CNSA 2: HNDL risk is the primary argument for immediate action

Question 4: Are there defined milestones and deadlines for your PQC migration?

Score	Criteria
1	No milestones or deadlines.
2	Vague intention to 'start migrating,' but no dates.
3	Initial milestones defined (e.g., 'complete inventory by Q2 2026, begin pilot by Q4 2026').
4	Detailed milestones with owners, deadlines, and success criteria for each migration phase.
5	Milestones tracked in project management system. Regular progress reviews. Deadlines matched to CNSA 2.0 and regulatory timelines.

NIST CSF 2: GV.RM-02 | SP 800 53: PM-9, PM-4 | ISO 27001: A.5.8

CNSA 2: Milestones should reference CNSA 2.0 category-based dates: firmware/software signing (LMS/XMSS) by 2025, key establishment (ML-KEM-1024) by 2030, exclusive use by 2031 (NSS)

Question 5: Does executive leadership understand and support the migration timeline?

Score	Criteria
1	No executive awareness.
2	Executive awareness is limited to general 'quantum threat' mentions.
3	Executive briefing delivered. General support for migration planning.
4	Executive sponsor identified. Budget allocated for migration activities.
5	Board-level reporting on PQC migration progress. Migration funded as a strategic initiative with dedicated resources.

NIST CSF 2: GV.RR-01, GV.OC-01
SP 800 53: PM-1, PM-2
ISO 27001: A.5.1, A.5.4
DORA: Article 5: ICT risk management governance

Question 6: Does your organization track specific regulatory and contractual deadlines that affect PQC migration timing?

Score	Criteria
1	No tracking of external deadlines.
2	Aware that regulations and contracts may impose crypto requirements, but no specific deadlines tracked.
3	Key regulatory deadlines identified (e.g., CNSA 2.0 milestones, sector mandates). Major contracts reviewed for cryptographic requirements.
4	Regulatory and contractual deadlines documented and mapped to migration phases. Compliance gaps identified.
5	Automated tracking of regulatory deadlines. Contract review process flags cryptographic obligations. Migration timeline incorporates all external deadline constraints.

NIST CSF 2: GV.OC-03, GV.RM-02
SP 800 53: PM-9, SA-4
ISO 27001: A.5.31, A.5.36
CNSA 2: CNSA 2.0 milestones: firmware/software signing (LMS/XMSS) 2025, key establishment (ML-KEM-1024) 2030, digital signatures (ML-DSA-87) by category, exclusive use 2031/2035
DORA: Article 5: ICT risk management governance

Standards references

- NSA CNSA 2.0: Mandatory PQC adoption timelines for national security systems
- NCSC: Timelines for migration to post-quantum cryptography (March 2025)
- BSI Technical Guideline TR-02102-1 (recommendation timelines)

What organizations typically miss

Organizations tend toward one of two extremes: dismissing quantum as too far away to matter, or panic-buying solutions without understanding timelines. The productive middle ground is understanding that the migration window (3-7 years for most enterprises) should start now because migration itself takes time, not because quantum computers are imminent.

DOMAIN 7

Governance and policy

Weight: 10% | 7 questions

Overview

Evaluates the organizational governance structures, policies, and resource allocation supporting PQC migration.

Why this matters

Technical readiness without governance support results in stalled migrations. PQC migration requires sustained investment over multiple years, cross-functional coordination (security, IT, development, procurement, legal), and clear ownership. Organizations without governance structures in place tend to start multiple initiatives that lose momentum when priorities shift.

Quick self-assessment

Level	Description
1	No PQC governance. Quantum risk is not on the organizational agenda.
2	PQC mentioned in security discussions, but no formal ownership or policy.
3	PQC migration assigned to a team or individual. Initial policy drafted.
4	Formal PQC governance structure with cross-functional representation. Policy approved. Budget allocated.
5	PQC governance integrated into enterprise risk management. Regular board-level reporting. Dedicated program with multi-year funding.

Assessment questions

Question 1: Is there a designated owner or team responsible for PQC migration?

Score	Criteria
1	No designated owner.
2	Informal responsibility assumed by the security team, but no formal assignment.
3	Specific team or individual assigned. Role documented.
4	Dedicated PQC program manager or working group with cross-functional representation.
5	PQC program office established with clear charter, authority, and reporting structure.

NIST CSF 2: GV.RR-01, GV.RR-02 | SP 800 53: PM-2, PM-10 | ISO 27001: A.5.2, A.5.4

DORA: Article 5: ICT risk management governance

Question 2: Does your organization have a cryptographic policy that addresses PQC?

Score	Criteria
1	No cryptographic policy exists.
2	Cryptographic policy exists but does not mention PQC or quantum risk.
3	Cryptographic policy updated to acknowledge PQC. High-level guidance included.
4	PQC-specific policy defines approved algorithms, migration requirements, and timelines.
5	PQC policy integrated into enterprise security framework. Regular review cycle. Enforcement mechanisms in place.

NIST CSF 2: GV.PO-01, GV.PO-02 | SP 800 53: SC-13, PL-1 | ISO 27001: A.5.1, A.8.24

CNSA 2: Policy should reference CNSA 2.0 approved algorithms: ML-KEM-1024, ML-DSA-87, LMS/XMSS, AES-256, SHA-384/SHA-512

DORA: Article 5: ICT risk management governance

Question 3: Is budget allocated specifically for PQC migration activities?

Score	Criteria
1	No budget for PQC.
2	PQC activities funded ad hoc from existing security budget.
3	Some budget earmarked for PQC assessment and planning.
4	Dedicated budget for PQC migration covering assessment, testing, deployment, and vendor changes.
5	Multi-year PQC budget approved. Funding covers full migration lifecycle including contingency.

NIST CSF 2: GV.RR-04 | SP 800 53: PM-3 | ISO 27001: A.5.4 | DORA: Article 5: ICT risk management governance

Question 4: Is PQC risk included in enterprise risk management processes?

Score	Criteria
1	PQC not in risk registers.
2	Quantum risk acknowledged informally, but not in formal risk management.
3	PQC risk added to risk register. Basic likelihood and impact assessment.
4	PQC risk quantified and regularly reviewed. Mitigation activities tracked.
5	PQC risk integrated into enterprise risk framework with regular board-level reporting. Risk appetite defined.

NIST CSF 2: GV.RM-01, GV.RM-02 | SP 800 53: RA-3, PM-9 | ISO 27001: A.5.7, A.5.8
DORA: Article 6: ICT risk management framework

Question 5: Is there cross-functional coordination for PQC migration (security, IT, development, procurement, legal)?

Score	Criteria
1	No cross-functional coordination.
2	Security team working in isolation on PQC.
3	Initial engagement with IT and development teams. Awareness building across functions.
4	Cross-functional working group established. Regular meetings and shared roadmap.
5	Integrated PQC program with representation from all relevant functions. Shared accountability and aligned priorities.

NIST CSF 2: GV.RR-01, GV.OC-04 | SP 800 53: PM-1, PM-2 | ISO 27001: A.5.2, A.5.4
DORA: Article 5: ICT risk management governance

Question 6: Does your organization have a policy for responding to cryptographic vulnerabilities, including algorithm deprecation and emergency key rotation?

Score	Criteria
1	No cryptographic vulnerability response policy.
2	General vulnerability management exists, but no specific procedures for cryptographic failures.
3	Cryptographic vulnerabilities recognized as a category in the vulnerability management process. Ad hoc response for past incidents (e.g., Heartbleed).
4	Cryptographic vulnerability response policy defines procedures for algorithm deprecation, key compromise, and emergency rotation. Roles and escalation paths documented.
5	Tested cryptographic vulnerability response policy. Tabletop exercises completed. Response time SLAs defined. Lessons from past crypto incidents (Heartbleed, SHA-1 deprecation) incorporated.

NIST CSF 2: RS.RP-01, RS.AN-01, GV.PO-01 | SP 800 53: IR-4, IR-8, SC-12 | ISO 27001: A.5.24, A.5.26, A.8.24
DORA: Article 17: ICT-related incident management

Question 7: Is there a PQC training and awareness program for staff beyond the security team?

Score	Criteria
1	No PQC training or awareness program.
2	Security team has self-educated on PQC, but no organizational training.
3	Awareness briefings delivered to IT leadership and development leads. PQC included in security awareness materials.
4	Structured training program covers PQC concepts, migration impacts, and role-specific responsibilities for IT, development, and procurement staff.
5	Organization-wide PQC awareness. Role-specific training with assessment. Training updated as standards evolve. External training or certification for key personnel.

NIST CSF 2: GV.RR-03, PR.AT-01 | SP 800 53: AT-2, AT-3 | ISO 27001: A.6.3

DORA: Article 13(6): ICT security awareness training

Standards references

- NIST SP 1800-38B: Governance and Planning for PQC Migration
- ISO/IEC 27001:2022: Cryptographic controls (A.8.24)
- CISA Quantum Readiness: Federal Agency Guidance (governance framework)

What organizations typically miss

PQC migration is often treated as a purely technical initiative without governance backing. This leads to unfunded mandates, unclear ownership, and competing priorities. The most common failure mode is not technical inability but organizational inability to sustain a multi-year migration program.

METHODOLOGY

Scoring methodology

The 1 to 5 maturity scale

Score	Level
1	No awareness or preparation
2	Aware but no action taken
3	Initial steps taken, partial coverage
4	Significant progress, most areas addressed
5	Complete coverage, documented, actively managed

Domain weights

Domain	Weight
1. Cryptographic inventory	20%
2. Data sensitivity and lifespan	15%
3. Standards compliance	10%
4. Migration readiness	20%
5. Vendor and supply chain	15%
6. Timeline and urgency	10%
7. Governance and policy	10%

Domains 1 (Cryptographic inventory) and 4 (Migration readiness) carry the highest weight because they represent the two most actionable dimensions: knowing what you have and being able to change it.

Overall score formula

The overall score is a weighted average of domain scores:

```
Overall = (Domain 1 avg x 0.2) + (Domain 2 avg x 0.15) + (Domain 3 avg x 0.1) + (Domain 4 avg x 0.2) + (Domain 5 avg x 0.15) + (Domain 6 avg x 0.1) + (Domain 7 avg x 0.1)
```

Risk categories

Score range	Category	Meaning
1.0 to 2.0	Critical	Immediate action required. The organization has significant unaddressed quantum risk exposure.
2.1 to 3.0	High	Significant gaps exist. Prioritize remediation within the next 6-12 months.
3.1 to 4.0	Moderate	Progress has been made. Targeted improvements needed in specific domains.
4.1 to 5.0	Low	Well-prepared. Maintain current practices and monitor standards updates.

Boundary convention. Scores that fall exactly on a boundary (2.0, 3.0, 4.0) belong to the lower category. A score of exactly 2.0 is Critical, not High. A score of exactly 3.0 is High, not Moderate. The companion workbook uses the same convention.

Critical domain override. If any single domain scores 2.0 or below (Critical), the overall risk category is automatically elevated to at least High, regardless of the weighted average. A single Critical domain indicates a fundamental gap that the weighted average can mask. For example, an organization with no cryptographic inventory (Domain 1 = 1.0) but strong governance (Domain 7 = 5.0) might produce a weighted average in the Moderate or Low range. The override prevents this misrepresentation.

PQCMM maturity model mapping

The PKI Consortium Post-Quantum Cryptography Maturity Model (PQCMM) provides an alternative maturity scale. The table below maps approximate PQRA score ranges to PQCMM levels.

PQCMM level	Name	Approximate PQRA range	Description
0	Unaware	N/A	Organization has no awareness of quantum computing threats to cryptography. Not reachable in PQRA scoring (minimum score is 1.0).
1	Aware	1.0 to 1.5	Organization recognizes quantum computing as a future threat to current cryptography.
2	Prepared	1.5 to 2.5	Organization has begun planning and assessment activities.
3	Capable	2.5 to 3.5	Organization can execute PQC migration for primary systems.
4	Mature	3.5 to 4.5	Organization has systematic PQC migration underway with governance support.
5	Leading	4.5 to 5.0	Organization has completed or nearly completed PQC migration with continuous monitoring.

This mapping is approximate. PQCMM is an emerging maturity model from the PKI Consortium, not yet a universally established benchmark. The PQRA measures organizational readiness across seven domains using a weighted scoring model. The PQCMM measures maturity progression along a single path. Use this mapping as a cross-reference, not an equivalence.

Interpreting domain scores

Look at domain scores individually, not just the overall score. An organization with an overall score of 3.5 (Moderate) might have a Domain 1 score of 1.5 (Critical) and a Domain 7 score of 4.5 (Low). The overall score masks a serious gap in cryptographic inventory. Domain-level analysis is where the actionable findings are.

RECOMMENDATIONS

Next steps

Your assessment results point to specific actions. Use the recommendations below based on your overall risk category.

Critical (1.0 to 2.0)

Start with Domain 1: build a cryptographic inventory. You cannot plan a migration without knowing what needs to migrate. Assign an owner for PQC readiness (Domain 7). Brief executive leadership on the risk and the timeline (Domain 6). These three actions create the foundation for everything else.

Recommended actions:

- Conduct a cryptographic discovery exercise across all systems
- Classify data by sensitivity and confidentiality lifespan
- Assign a PQC migration owner with cross-functional authority
- Brief executive leadership and request dedicated budget
- Set a target date for completing the initial assessment

High (2.1 to 3.0)

You have awareness but lack execution. Focus on the domains with the lowest scores. Common priorities at this stage: completing the cryptographic inventory, assessing vendor PQC readiness, and establishing a migration timeline with milestones.

Recommended actions:

- Complete and document the cryptographic inventory
- Map data classification to cryptographic protections
- Contact critical vendors about PQC roadmaps
- Begin PQC algorithm testing in a lab environment
- Establish migration milestones matched to CNSA 2.0 timelines
- Formalize PQC governance with budget and ownership

Moderate (3.1 to 4.0)

You have made progress. Focus on closing specific gaps. Common priorities at this stage: improving crypto-agility, testing PQC algorithms in staging environments, establishing vendor contingency plans, and updating procurement criteria.

Recommended actions:

- Improve crypto-agility in systems with hardcoded algorithms
- Test PQC algorithms in staging environments that mirror production

- Measure performance impact of PQC algorithms on your workloads
- Update procurement policies to include PQC readiness criteria
- Develop rollback procedures for each migration phase
- Request CycloneDX CBOMs from critical suppliers

Low (4.1 to 5.0)

You are well-prepared. Focus on maintaining your position and closing any remaining gaps. Common priorities at this stage: automating cryptographic inventory updates, validating rollback procedures, beginning pilot production deployments, and participating in industry standards work.

Recommended actions:

- Begin pilot production deployment of PQC algorithms for high-priority systems
- Validate rollback procedures with production-like testing
- Automate cryptographic inventory with CI/CD integration
- Engage with IETF working groups or industry PQC initiatives
- Review and update the assessment quarterly

When to seek external help

Consider engaging a cryptographic security consultant if:

- Your organization scores Critical or High and lacks internal PQC expertise
- You need help building a cryptographic inventory across complex infrastructure
- You require an independent assessment for regulatory or audit purposes
- You are evaluating vendor PQC claims and need technical validation
- Your migration plan involves custom cryptographic implementations

A structured assessment like this one identifies gaps and priorities. For organizations that need hands-on migration support, an external assessment can verify scores against technical evidence and provide implementation guidance.

LIMITATIONS

Limitations

This assessment is a structured self-evaluation. It has inherent limitations:

- **Self-reported scores.** Scores depend on the assessor's knowledge and honesty. An organization cannot accurately score what it does not understand. Involve multiple stakeholders to reduce blind spots.
- **Point-in-time snapshot.** The assessment captures the organization's posture at the time of completion. Cryptographic risk changes as systems are deployed, vendors update products, and standards evolve.
- **No technical validation.** This assessment does not scan networks, test configurations, or verify claims. It measures organizational awareness and process maturity, not technical correctness. A score of 5 on the inventory domain means the organization believes it has a complete inventory, not that the inventory has been independently verified.
- **General-purpose weights.** The domain weights reflect a reasonable default for most organizations. Specific sectors or regulatory environments may need different weighting. A defense contractor subject to CNSA 2.0 deadlines may weight timeline and urgency higher. A healthcare organization with 50-year data retention requirements may weight data sensitivity higher.
- **Quantum timelines are uncertain.** The assessment helps organizations prepare for a threat with uncertain timing. No one knows when a cryptographically relevant quantum computer capable of breaking RSA-2048 or ECDH-P256 will exist. The assessment assumes that preparation is warranted regardless of the exact timeline, based on the multi-year duration of enterprise cryptographic migrations.
- **Not a compliance certificate or audit instrument.** This framework identifies organizational gaps and priorities. It does not replace a technical cryptographic security review, penetration test, or architecture assessment. Treat the results as a prioritization tool, not an attestation of security posture.

APPENDIX A

Standards reference table

This table maps each assessment domain to the relevant published standards and guidance documents.

Standard	Domain 1	Domain 2	Domain 3	Domain 4	Domain 5	Domain 6	Domain 7
NIST FIPS 203 (ML-KEM)			X	X			
NIST FIPS 204 (ML-DSA)			X	X			
NIST FIPS 205 (SLH-DSA)			X	X			
NIST SP 1800-38B	X			X	X		X
NIST IR 8547				X			
NSA CNSA 2.0		X	X			X	
NCSC Quantum-Safe Cryptography		X	X			X	
BSI TR-02102-1			X			X	
ETSI TR 103 619		X					
CycloneDX CBOM v1.6	X				X		
CISA PQC Initiative	X				X		X
ISO/IEC 27001:2022 (A. 8.24)							X
IETF RFC 9370				X			
IETF hybrid TLS drafts			X	X			

Standard descriptions:

- **NIST FIPS 203 (ML-KEM):** Module-Lattice-Based Key-Encapsulation Mechanism. The primary NIST-standardized PQC key encapsulation mechanism. Replaces RSA and ECDH for key establishment. Three parameter sets: ML-KEM-512, ML-KEM-768 (recommended), ML-KEM-1024.
- **NIST FIPS 204 (ML-DSA):** Module-Lattice-Based Digital Signature Algorithm. The primary NIST-standardized PQC algorithm for digital signatures. Replaces RSA and ECDSA for signing. Three parameter sets: ML-DSA-44, ML-DSA-65 (recommended), ML-DSA-87.

- **NIST FIPS 205 (SLH-DSA):** Stateless Hash-Based Digital Signature Algorithm. A conservative, hash-based alternative to ML-DSA. Larger signatures but based on well-understood hash function security. Suitable for use cases where lattice-based assumptions are considered too new.
- **NIST SP 1800-38B:** Migration to Post-Quantum Cryptography. NCCoE practice guide (preliminary draft) covering cryptographic discovery, migration planning, and implementation. Organized by migration phase. Not a finalized standard; treat as structured guidance.
- **NIST IR 8547 (draft, November 2024):** Transition to Post-Quantum Cryptography Standards. Provides transition guidance and deprecation timelines for classical algorithms.
- **NSA CNSA 2.0:** Commercial National Security Algorithm Suite 2.0. Mandatory PQC adoption timelines for US national security systems (NSS). Approved algorithms: ML-KEM-1024 (key establishment), ML-DSA-87 (digital signatures), LMS and XMSS (firmware and software signing), AES-256, SHA-384, and SHA-512. SLH-DSA (FIPS 205) is not CNSA 2.0 approved. CNSA 2.0 deadlines apply directly only to NSS; this assessment references them as planning benchmarks for enterprise organizations, not as universal mandates. Organizations outside the NSS scope should treat CNSA 2.0 timelines as indicative of the direction, not as binding requirements.
- **NCSC PQC guidance:** UK National Cyber Security Centre publications on post-quantum cryptography. Key documents: "Preparing for quantum-safe cryptography" (November 2020), "Next steps in preparing for post-quantum cryptography" (November 2023, updated August 2024), and "Timelines for migration to post-quantum cryptography" (March 2025). The 2025 timelines guidance defines three migration phases: discovery and planning by 2028, high-priority migration by 2031, and complete migration by 2035.
- **BSI TR-02102-1:** German Federal Office for Information Security technical guideline on cryptographic mechanisms. Includes PQC recommendations and transition timelines.
- **ETSI TR 103 619:** European Telecommunications Standards Institute report on quantum-safe cryptography migration strategies. Provides a framework for evaluating migration approaches.
- **CycloneDX CBOM v1.6:** Cryptography Bill of Materials specification. A standardized format for documenting cryptographic assets, algorithms, protocols, and dependencies. Part of the CycloneDX software supply chain standard.
- **CISA PQC Initiative:** US Cybersecurity and Infrastructure Security Agency guidance on post-quantum cryptography readiness. Covers inventory, vendor engagement, and federal agency preparation.
- **ISO/IEC 27001:2022 (A.8.24):** Information security management system standard. Control A.8.24 addresses cryptographic controls and should be updated to reflect PQC requirements.
- **IETF RFC 9370:** Multiple Key Exchanges in the Internet Key Exchange Protocol (IKEv2). Enables hybrid key exchange for IPsec VPNs.
- **IETF hybrid TLS drafts:** In-progress specifications for hybrid key exchange in TLS 1.3, combining classical (X25519) and post-quantum (ML-KEM) key exchange.

APPENDIX B

Glossary

CBOM (Cryptography Bill of Materials): A machine-readable inventory of cryptographic assets used in a software or hardware product. The CycloneDX CBOM specification (v1.6) defines a standardized format. A CBOM documents algorithms, protocols, key sizes, certificates, and cryptographic dependencies.

CNSA 2.0 (Commercial National Security Algorithm Suite 2.0): NSA-published guidance that defines the approved cryptographic algorithms and mandatory adoption timelines for US national security systems. Approved algorithms: ML-KEM-1024, ML-DSA-87, LMS, XMSS, AES-256, SHA-384, SHA-512. SLH-DSA is not CNSA 2.0 approved. Published September 2022, updated April 2024 (FAQ Ver. 2.1, December 2024).

CRQC (Cryptographically Relevant Quantum Computer): A quantum computer with sufficient qubits and low enough error rates to break current public-key cryptographic algorithms (RSA, ECC) using Shor's algorithm. Estimated timelines for CRQC availability range from 2030 to 2040, depending on the source.

Crypto-agility: The ability of a system to swap cryptographic algorithms through configuration changes rather than code changes. A crypto-agile system can migrate from RSA to ML-KEM by updating a configuration file or policy, without modifying application code.

ECDH (Elliptic Curve Diffie-Hellman): A key agreement protocol based on elliptic curve cryptography. Widely used for TLS key agreement (as ECDHE). Vulnerable to quantum attack via Shor's algorithm.

ECDSA (Elliptic Curve Digital Signature Algorithm): A digital signature algorithm based on elliptic curve cryptography. Used in TLS, code signing, and blockchain systems. Vulnerable to quantum attack via Shor's algorithm.

Grover's algorithm: A quantum algorithm that provides a quadratic speedup for searching unsorted databases. Applied to cryptography, it halves the effective security of symmetric algorithms: AES-128 drops to 64-bit security, AES-256 drops to 128-bit security. CNSA 2.0 requires AES-256 to maintain adequate security margins against quantum attack. Unlike Shor's algorithm, Grover's does not completely break symmetric cryptography; it makes shorter key lengths insufficient.

HNDL (Harvest Now, Decrypt Later): An attack strategy where an adversary captures encrypted data today with the intention of decrypting it in the future using a quantum computer. Data with long confidentiality requirements is already at risk from this attack, regardless of when a CRQC becomes available.

HQC (Hamming Quasi-Cyclic): A code-based key encapsulation mechanism selected by NIST as the Round 4 winner in March 2025. Provides algorithm diversity from the lattice-based ML-KEM by relying on different mathematical hardness assumptions (decoding random linear codes). Draft standard expected 2026, finalization around 2027.

HSM (Hardware Security Module): A physical device that manages and protects cryptographic keys and performs cryptographic operations. HSMs may need firmware or hardware updates to support PQC key sizes and algorithms.

Hybrid key establishment: A key establishment mechanism that combines a classical key agreement (e.g., X25519) with a post-quantum key encapsulation (e.g., ML-KEM-768). The resulting shared secret is secure as long as either algorithm remains unbroken. This provides protection against quantum attack while maintaining compatibility with classical systems.

KEM (Key Encapsulation Mechanism): A cryptographic primitive that allows one party to securely generate a shared secret and transmit it to another party using the recipient's public key. Unlike interactive key agreement (e.g., Diffie-Hellman), a KEM is a one-directional operation. ML-KEM and HQC are both KEMs. KEMs are the PQC replacement for the key exchange component of protocols like TLS and IKEv2.

Lattice-based cryptography: A family of cryptographic algorithms based on the mathematical hardness of lattice problems. ML-KEM (FIPS 203) and ML-DSA (FIPS 204) are both lattice-based. This is currently the most efficient approach to PQC, with the smallest key and ciphertext sizes among PQC algorithm families.

LMS (Leighton-Micali Signature Scheme): A stateful hash-based digital signature scheme standardized in NIST SP 800-208. Mandated by CNSA 2.0 for firmware and software signing alongside XMSS. Stateful means each signing key can only produce a finite number of signatures, and the signer must track state to avoid reusing signature indices. Key reuse is catastrophic (reveals the private key). Suitable for firmware signing where the number of signatures is bounded and predictable.

ML-DSA (Module-Lattice-Based Digital Signature Algorithm): NIST FIPS 204. The primary standardized PQC digital signature algorithm. Based on the CRYSTALS-Dilithium scheme. Three parameter sets: ML-DSA-44 (NIST security level 2), ML-DSA-65 (level 3, recommended), ML-DSA-87 (level 5).

ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism): NIST FIPS 203. The primary standardized PQC key encapsulation mechanism, used for key establishment. Based on the CRYSTALS-Kyber scheme. Three parameter sets: ML-KEM-512 (NIST security level 1), ML-KEM-768 (level 3, recommended), ML-KEM-1024 (level 5).

NIST PQC security levels: NIST defines five security levels for PQC algorithms, based on the difficulty of attacking the best known classical algorithm at equivalent strength. Level 1: at least as hard as AES-128. Level 2: at least as hard as SHA-256 collision finding. Level 3: at least as hard as AES-192. Level 4: at least as hard as SHA-384 collision finding. Level 5: at least as hard as AES-256. ML-KEM-768 and ML-DSA-65 are Level 3 (recommended for general use). CNSA 2.0 requires Level 5 (ML-KEM-1024, ML-DSA-87).

PKI (Public Key Infrastructure): The framework of policies, hardware, software, and procedures for creating, managing, distributing, storing, and revoking digital certificates. Enterprise PKI (e.g., Microsoft AD CS) and public CAs (e.g., Let's Encrypt, DigiCert) both need PQC migration. PKI is frequently the largest single bottleneck in PQC migration because certificate formats, chain validation, and revocation mechanisms all need updating.

PQC (Post-Quantum Cryptography): Cryptographic algorithms designed to be secure against both classical and quantum computers. PQC algorithms run on classical hardware; they do not require quantum computers to operate.

QKD (Quantum Key Distribution): A method of distributing encryption keys using quantum mechanical properties (typically photon polarization) to detect eavesdropping. QKD is distinct from PQC: it uses quantum hardware for key distribution, while PQC uses classical algorithms designed to resist quantum attack. NCSC does not recommend QKD for general enterprise use due to hardware requirements, distance limitations, and the availability of PQC alternatives. This assessment covers PQC, not QKD.

RSA: A public-key cryptographic algorithm used for key transport and digital signatures. Named after its inventors (Rivest, Shamir, Adleman). Widely deployed in TLS, PKI, and code signing. Vulnerable to quantum attack via Shor's algorithm.

Shor's algorithm: A quantum algorithm that can efficiently factor large integers and compute discrete logarithms. It breaks RSA, DSA, ECDSA, ECDH, and other public-key algorithms that depend on these mathematical problems. Requires a CRQC to execute at cryptographically relevant scale.

SLH-DSA (Stateless Hash-Based Digital Signature Algorithm): NIST FIPS 205. A PQC digital signature algorithm based on hash functions. Based on the SPHINCS+ scheme. Conservative security assumptions (relies on hash function security rather than lattice assumptions). Larger signatures than ML-DSA, ranging from 7,856 bytes (SLH-DSA-128s) to 49,856 bytes (SLH-DSA-256f) depending on security level and speed/size tradeoff.

TLS (Transport Layer Security): The standard protocol for encrypted communication over networks. TLS 1.3 is the current version. PQC migration for TLS involves replacing the key agreement mechanism (currently ECDH/X25519) with a PQC KEM (ML-KEM) or hybrid scheme, and replacing signature algorithms (RSA/ECDSA) with PQC signatures (ML-DSA/SLH-DSA) for certificate verification.

X25519: An elliptic curve Diffie-Hellman key agreement function using Curve25519. Widely used in TLS 1.3 for key agreement. Produces 32-byte public keys. Vulnerable to quantum attack. Commonly combined with ML-KEM-768 in hybrid key establishment schemes.

XMSS (eXtended Merkle Signature Scheme): A stateful hash-based digital signature scheme standardized in RFC 8391. Like LMS, it is mandated by CNSA 2.0 for firmware and software signing. Stateful: the signer must track which one-time signature indices have been used. Provides strong security guarantees based only on hash function security. Suitable for environments where signature count is bounded and state can be reliably managed (e.g., firmware update signing).

APPENDIX C

Compliance framework mapping

This appendix maps each assessment question to relevant compliance frameworks. Use this mapping to connect PQRA findings to your existing compliance programs and audit requirements.

Frameworks mapped

- **NIST CSF 2.0:** Cybersecurity Framework 2.0. Function and category identifiers (e.g., ID.AM-01 for asset management).
- **NIST SP 800-53:** Security and Privacy Controls. Control identifiers (e.g., SC-12 for cryptographic key establishment).
- **ISO 27001:2022 Annex A:** Information security controls. Control identifiers (e.g., A.8.24 for use of cryptography).
- **CNSA 2.0:** NSA Commercial National Security Algorithm Suite 2.0. Applicable requirements and timelines.
- **DORA:** Digital Operational Resilience Act (EU). Applicable articles for financial sector organizations.

Domain 1: Cryptographic inventory

ID	Question (abbreviated)	NIST CSF 2.0	SP 800-53	ISO 27001	CNSA 2.0	DORA
CI-1	Documented algorithm inventory	ID.AM-01, ID.AM-02	CM-8, SC-12	A.8.24	Inventory required	
CI-2	Protocol versions documented	ID.AM-01, PR.DS-02	CM-8, SC-8, SC-23	A.8.24	Protocol awareness	
CI-3	Quantum-vulnerable algorithm mapping	ID.AM-01, ID.RA-01	SC-12, SC-13, RA-5	A.8.24	Identify for replacement	
CI-4	Certificate and key inventory	ID.AM-02, PR.DS-01	SC-12, SC-17	A.8.24	Key management readiness	
CI-5	Embedded/IoT/ firmware coverage	ID.AM-01, ID.AM-03	CM-8, SA-4	A.8.24, A.7.4	Firmware signing by 2025	
CI-6	Inventory review frequency	ID.AM-01, ID.IM-04	CM-8(3), PM-5	A.8.24		
CI-7	Automated discovery tooling	ID.AM-01, DE.CM-09	CM-8(3), RA-5, SI-7	A.8.24	Supports migration planning	Art. 9(1)
CI-8	Dependency mapping	ID.AM-04, ID.RA-03	CM-8, SA-4, CP-2	A.8.24	Migration sequencing	
CI-9	Cloud crypto visibility	ID.AM-01, ID.AM-05	CM-8, SC-12, SA-9	A.8.24, A.5.23	Cloud migration planning	Art. 28

Domain 2: Data sensitivity and lifespan

ID	Question (abbreviated)	NIST CSF 2.0	SP 800-53	ISO 27001	CNSA 2.0	DORA
DS-1	Data classification with confidentiality	ID.AM-07, PR.DS-01	RA-2, SC-28	A.5.12, A.5.13	Drives prioritization	Art. 13
DS-2	Long-term confidentiality data	ID.AM-07, ID.RA-01	RA-2, SC-28	A.5.12	Early migration	
DS-3	HNDL awareness	ID.RA-01, ID.RA-02	RA-3, RA-5	A.5.7	Primary driver	
DS-4	Data-at-rest encryption mapping	PR.DS-01	SC-28, SC-12	A.8.24	QR algorithms by 2030	
DS-5	Transit quantum vulnerability	PR.DS-02	SC-8, SC-13	A.8.24	Key establishment by 2030	
DS-6	Key hierarchy depth	PR.DS-01	SC-12, SC-28	A.8.24	Key wrapping transition	
DS-7	Transit protection by segment	PR.DS-02, PR.IR-01	SC-8, SC-8(1)	A.8.24, A.8.20	All network encryption by 2030	

Domain 3: Standards compliance

ID	Question (abbreviated)	NIST CSF 2.0	SP 800-53	ISO 27001	CNSA 2.0	DORA
SC-1	NIST PQC standards awareness	GV.RM-01	SC-13	A.8.24	FIPS 203/204/205 approved	
SC-2	Migration timeline alignment	GV.RM-01, GV.RM-02	SC-13, PM-9	A.8.24, A. 5.36	Timelines: 2025, 2030, 2035	
SC-3	Sector-specific requirements	GV.OC-03	SC-13, SA-9	A.5.31, A. 5.36	Sector timelines may be earlier	Art. 5
SC-4	IETF protocol tracking	GV.RM-01	SC-8, SC-13	A.8.24	Protocol migration required	
SC-5	Standards adoption process	GV.RM-01, GV.PO-01	SC-13, SA-8	A.5.1, A. 8.24		
SC-6	Compliance evidence collection	GV.OC-03, ID.GV-01	CA-2, CA-7, SC-13	A.5.31, A. 5.35, A. 5.36	Audit readiness	Art. 5, Art. 6

Domain 4: Migration readiness

ID	Question (abbreviated)	NIST CSF 2.0	SP 800-53	ISO 27001	CNSA 2.0	DORA
MR-1	Crypto-agility	PR.DS-01, PR.DS-02	SC-12, SC-13, SA-8	A.8.24	Prerequisite for timelines	
MR-2	PKI PQC readiness	PR.DS-01	SC-12, SC-17	A.8.24	QR certificates by 2030	
MR-3	PQC algorithm testing	PR.DS-01, PR.IP-12	SC-13, SA-11	A.8.24	Testing required	Art. 11
MR-4	Performance impact evaluation	PR.DS-01	SC-13, SA-8	A.8.24		
MR-5	Key management PQC support	PR.DS-01	SC-12	A.8.24	PQC key sizes	
MR-6	Rollback planning	PR.IP-12, RC.RP-01	CP-2, CP-10	A.8.24, A.5.30		Art. 11
MR-7	Dev pipeline readiness	PR.DS-01, PR.IP-12	SA-8, SA-15	A.8.24, A.8.25		
MR-8	OT/ICS/SCADA readiness	PR.DS-01, ID.AM-01	SC-12, SC-13, SA-4	A.8.24	Same migration timelines	
MR-9	Crypto incident response	RS.RP-01, RS.AN-01	IR-4, IR-5, SC-12	A.5.24, A.5.26		Art. 17
MR-10	Hybrid deployment strategy	PR.DS-01, PR.DS-02	SC-8, SC-12, SC-13	A.8.24	Hybrid until 2031/2035	

Domain 5: Vendor and supply chain

ID	Question (abbreviated)	NIST CSF 2.0	SP 800-53	ISO 27001	CNSA 2.0	DORA
VS-1	Vendor crypto dependency ID	GV.SC-01, GV.SC-04	SA-9, SR-3	A.5.19, A.5.21	Constrains timeline	Art. 28
VS-2	Vendor PQC roadmap assessment	GV.SC-04, GV.SC-05	SA-9, SR-6	A.5.19, A.5.22	Align with CNSA 2.0	Art. 28, Art. 30
VS-3	PQC procurement criteria	GV.SC-02, GV.SC-05	SA-4, SA-9, SR-3	A.5.19, A.5.20		Art. 28, Art. 30
VS-4	Vendor contingency plans	GV.SC-04, GV.SC-07	SA-9, CP-2	A.5.19, A.5.30		Art. 28
VS-5	CBOM capability	GV.SC-04, ID.AM-02	SR-3, SR-4, CM-8	A.5.19	Visibility for planning	Art. 28
VS-6	Cloud provider crypto visibility	GV.SC-04, ID.AM-05	SA-9, SC-12, SC-13	A.5.23, A.8.24	Provider timelines	Art. 28, Art. 29
VS-7	Library crypto dependency analysis	GV.SC-04, ID.AM-02	SA-4, SR-3, SI-2	A.5.19, A.8.24	Library PQC support	Art. 28

Domain 6: Timeline and urgency

ID	Question (abbreviated)	NIST CSF 2.0	SP 800-53	ISO 27001	CNSA 2.0	DORA
TU-1	Quantum risk timeline position	GV.RM-01, ID.RA-01	RA-3, PM-9	A.5.7	Baseline for NSS	
TU-2	Migration duration estimate	GV.RM-02	PM-9, SA-8	A.5.8	Must fit CNSA deadlines	
TU-3	HNDL in urgency assessment	ID.RA-01, ID.RA-04	RA-3	A.5.7	Primary argument for action	
TU-4	Defined milestones	GV.RM-02	PM-9, PM-4	A.5.8	Reference 2025, 2030, 2031, 2035	
TU-5	Executive support	GV.RR-01, GV.OC-01	PM-1, PM-2	A.5.1, A.5.4		Art. 5
TU-6	Regulatory deadline tracking	GV.OC-03, GV.RM-02	PM-9, SA-4	A.5.31, A.5.36	CNSA 2.0 milestones	Art. 5

Domain 7: Governance and policy

ID	Question (abbreviated)	NIST CSF 2.0	SP 800-53	ISO 27001	CNSA 2.0	DORA
GP-1	Designated PQC owner	GV.RR-01, GV.RR-02	PM-2, PM-10	A.5.2, A. 5.4		Art. 5
GP-2	PQC cryptographic policy	GV.PO-01, GV.PO-02	SC-13, PL-1	A.5.1, A. 8.24	Reference approved algorithms	Art. 5
GP-3	PQC budget allocation	GV.RR-04	PM-3	A.5.4		Art. 5
GP-4	PQC in enterprise risk management	GV.RM-01, GV.RM-02	RA-3, PM-9	A.5.7, A. 5.8		Art. 6
GP-5	Cross-functional coordination	GV.RR-01, GV.OC-04	PM-1, PM-2	A.5.2, A. 5.4		Art. 5
GP-6	Crypto vulnerability response policy	RS.RP-01, RS.AN-01, GV.PO-01	IR-4, IR-8, SC-12	A.5.24, A. 5.26, A. 8.24		Art. 17
GP-7	PQC training and awareness	GV.RR-03, PR.AT-01	AT-2, AT-3	A.6.3		Art. 13(6)