Quantum-Safe Payments Readiness

Implementation Road Map

A strategic multi-year plan for transitioning to quantum-safe cryptographic solutions.

Payments Innovation Alliance®

Quantum-Safe Payments Readiness

Implementation Road Map

A strategic multi-year plan for transitioning to quantum-safe cryptographic solutions.

Now

Mobilization and Discovery

Years 1-2

- Establish governance and awareness.
- Conduct cryptographic inventory and risk assessment.
- Lay the technical foundation.
- Make quantum-safe a requirement with vendors.

Next

Planning and Piloting

Years 2-4

- Align with industry standards/expand networking.
- Plan phased migration strategy.
- Establish engineering readiness.

Later

Migration and Scaling

Years 4+

- Deploy full-scale post-quantum cryptography.
- Establish continuous monitoring and agility.

Now - Years 1-2 Next - Years 2-4 Later - Years 4+

Quantum-Safe Payments Readiness

Implementation Road Map

A strategic multi-year plan for transitioning to quantum-safe cryptographic solutions.

Now

Mobilization and Discovery

Years 1-2

Governance & Awareness

Form a Quantum Task Force

Appoint a dedicated, cross-functional team with executive sponsorship, including leaders from IT, cybersecurity, compliance, risk, and business units. Create a budget to support quantum readiness.

Executive Education

Provide focused training for the board of directors and senior leadership to underscore the "Harvest Now, Decrypt Later" (HNDL) risk, securing necessary budget and commitment.

Stakeholder Communications

Create educational resources to raise awareness across the entire organization and with critical third-party vendors or leverage existing resources such as Protecting Payments in the Quantum Era.

Cryptographic Inventory & Risk Assessment

Cryptographic Asset Inventory

Conduct a comprehensive inventory of all systems and applications that use public key cryptography (PQC) (e.g., TLS/SSL, PKI). Identify the specific algorithms (e.g., RSA, ECC) and key lengths in use.

Data Classification & Risk Model

Classify encrypted data based on its confidentiality lifetime. Prioritize the highest-risk, highest-value systems, and long-life data that are most exposed to the HNDL threat.

Vendor Engagement

Demand a quantum-safe road map from all existing vendors. Audit all critical vendors on their PQC road maps. All requests for information and proposals should require vendors be quantum-safe by 2030.

Technical Foundation

Develop Crypto-Agility

Start architecting systems to support cryptographic agility. This involves separating cryptographic functions from the applications so that algorithms can be updated or swapped quickly without a complete system overhaul.

Testbed & Sandbox

Establish a non-production test environment to begin experimenting with the newly finalized National Institute of Standards and Technology PQC algorithms (e.g., ML-KEM, ML-DSA).

Quantum-Safe Payments Readiness

Implementation Road Map

A strategic multi-year plan for transitioning to quantum-safe cryptographic solutions.

Next

Planning and Piloting

Years 2-4

Industry Alignment & Networking

Internal PKI Review

Evaluate and redesign the organization's Public Key Infrastructure (PKI) to handle PQC certificates, which will have larger size requirements.

Performance Testing

Conduct thorough testing to measure the performance impact of PQC on network latency, CPU utilization, and storage, and address any performance bottlenecks.

Coordinate with Payment Systems

Actively participate in industry working groups, such as Nacha's Payments Innovation Alliance Quantum Payments Project Team, to align PQC migration plans.

Migration Strategy

Develop a Phased Migration Plan

Based on the risk assessment, create a detailed, risk-based road map for systems migration. Prioritize the most exposed, business-critical systems first.

Regulatory Alignment

Map the migration road map against evolving regulatory requirements. Ensure migration milestones align with expected compliance deadlines and that documentation supports audit readiness at each phase.

Third-Party & Supply Chain Migration

Extend the migration plan to encompass critical third-party processors, payment networks, and technology vendors. Establish contractual public key cryptography (PQC) readiness requirements and shared migration timelines to prevent interoperability gaps at the network layer.

Engineering Readiness

Hybrid Cryptography Pilots

Begin implementing hybrid cryptography solutions in a few, non-customer-facing or low-risk production environments. Hybrid cryptography uses both a classical (RSA/ECC) and a PQC algorithm in tandem, ensuring that the connection remains secure if either algorithm holds up. This minimizes risk during the transition.

Infrastructure Upgrades

Begin technical planning and procurement for necessary infrastructure upgrades, such as new Hardware Security Modules (HSMs), to support the larger key and signature sizes of PQC algorithms.

Quantum-Safe Payments Readiness

Implementation Road Map

A strategic multi-year plan for transitioning to quantum-safe cryptographic solutions.

Later

Migration and Scaling

Years 4+

Full Scale Public Key Cryptography Deployment

Production Migration

Systematically migrate production systems based on the prioritized plan. Begin with the highest-risk areas and progressively move to general purpose channels.

Deprecation of Classical Cryptography

Establish formal processes to deprecate and decommission all quantum-vulnerable, purely classical cryptographic algorithms.

Third-Party Oversight

Implement robust oversight to ensure all third-party vendors and partners meet the agreed-upon PQC standards before integrating their services.

Continuous Monitoring & Agility

Operational Readiness

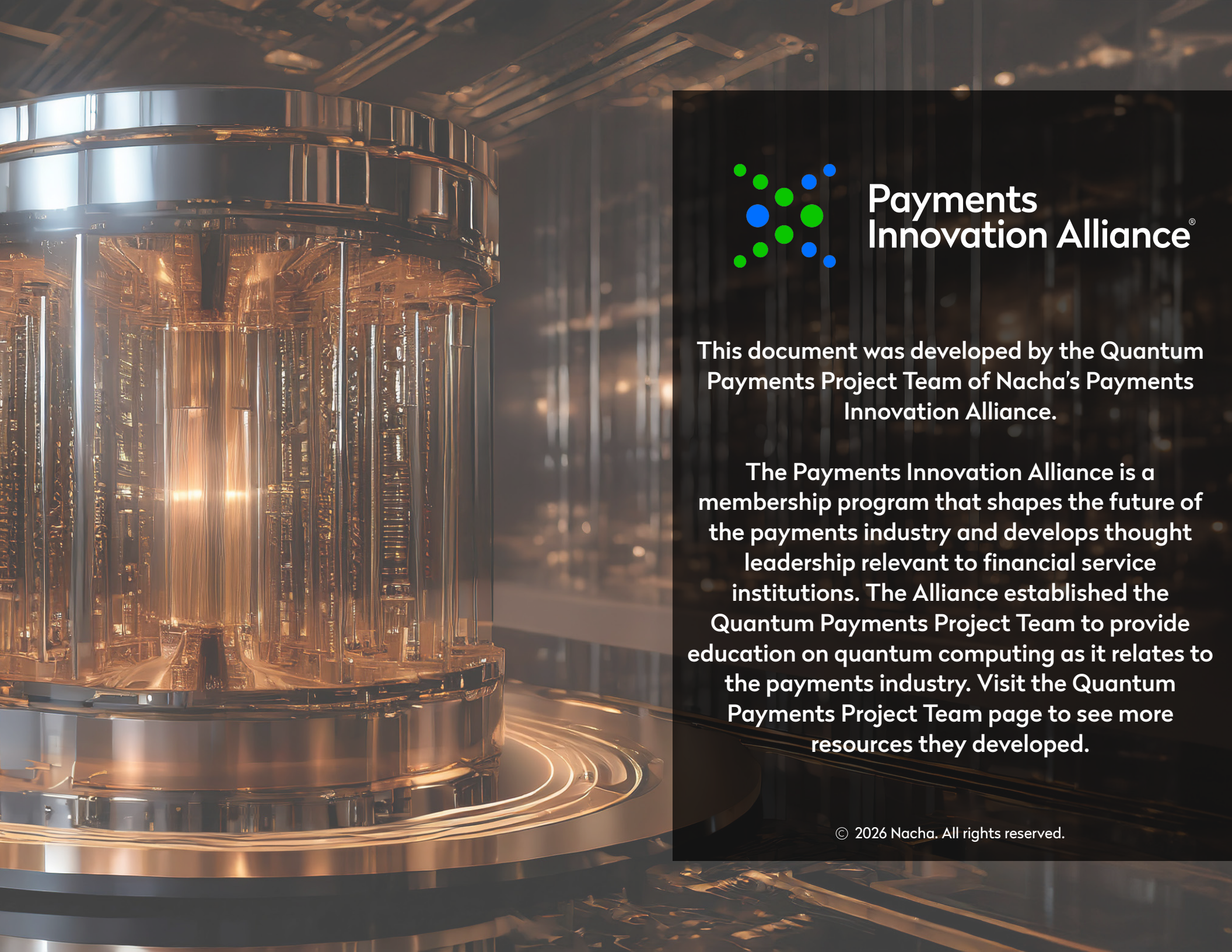
Update all security incident response plans and disaster recovery procedures to account for PQC-related failures or changes.

Crypto-Agility Maintenance

Ensure that the crypto-agile architecture is maintained and tested regularly. This ongoing agility is vital, as the PQC landscape may continue to evolve (e.g., with new National Institute of Standards and Technology updates).

Continuous Inventory

Institutionalize the cryptographic inventory and risk assessment process as a continuous, evergreen function, ensuring new systems are built with PQC from day one.



Payments Innovation Alliance®

This document was developed by the Quantum Payments Project Team of Nacha's Payments Innovation Alliance.

The Payments Innovation Alliance is a membership program that shapes the future of the payments industry and develops thought leadership relevant to financial service institutions. The Alliance established the Quantum Payments Project Team to provide education on quantum computing as it relates to the payments industry. Visit the Quantum Payments Project Team page to see more resources they developed.