

The PKI Post-Quantum Readiness Checklist

GOVERNMENT EDITION

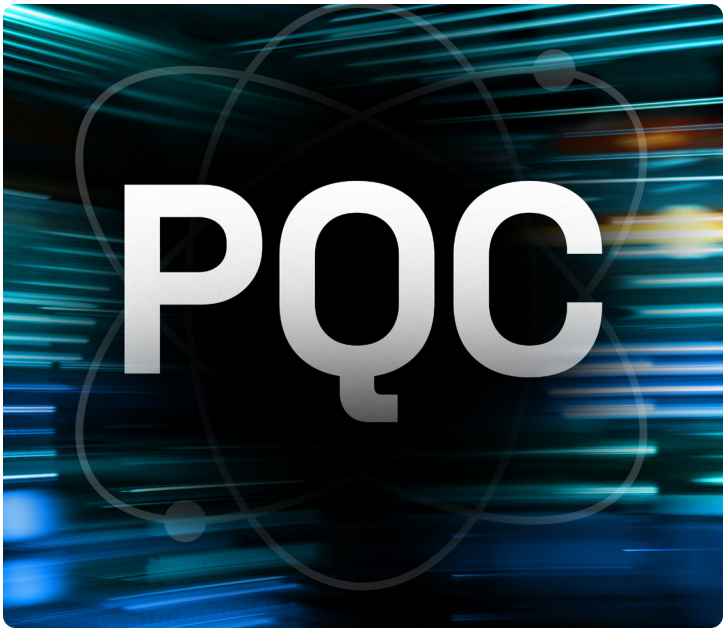
A Practical Guide for Assessing Post-Quantum Readiness Across Government PKI, Identity, and Critical Systems

PKI® SOLUTIONS

Executive Summary

Government agencies face a complex transition as they prepare their cryptographic infrastructure for a post-quantum future. With NIST having finalized its first set of PQC standards, agencies must now evaluate how quantum-resistant algorithms will impact their Public Key Infrastructure (PKI), identity systems, and security infrastructure.

While widespread PQC deployment will occur over time, agencies should begin evaluating their cryptographic dependencies, infrastructure readiness, and transition priorities now. This checklist provides a practical framework for identifying gaps, assessing existing PKI capabilities, and establishing a foundation for a phased, risk-informed post-quantum transition.



Federal PQC Readiness: Planning Is Already Underway

Federal agencies are moving from PQC awareness toward structured transition planning. NIST has finalized its initial PQC standards, while federal policy and guidance establish expectations for cryptographic inventory, transition ownership, risk prioritization, and migration planning.

Agencies should evaluate how these requirements intersect with their existing PKI infrastructure, authentication systems, HSMs, applications, and mission-critical services.

The immediate priority is to understand cryptographic dependencies, identify potential migration obstacles, and establish a practical path toward quantum-resistant infrastructure.

Why PQC Matters to PKI

Government PKI supports essential security functions, including identity verification, PIV authentication, secure communications, digital signatures, device authentication, and access to mission-critical systems.

Many of these capabilities rely on RSA and Elliptic Curve Cryptography (ECC), which are vulnerable to attacks by a sufficiently capable quantum computer.

For government organizations, PQC readiness is both a cryptographic modernization challenge and a long-term infrastructure planning responsibility.



Understanding PQC Readiness

Transitioning to quantum-resistant cryptography requires more than updating algorithms. Agencies must understand how changes to certificates, certificate authorities, HSMs, authentication systems, and applications could affect security, interoperability, and operational continuity.

This checklist evaluates readiness across key areas including governance, cryptographic inventory, PKI infrastructure, HSMs, applications, authentication, revocation, monitoring, and pilot planning.

© 2026 PKI Solutions LLC All Rights Reserved

The PKI Post-Quantum Readiness Checklist

Use the following checklist to evaluate your organization's post-quantum readiness across nine key areas, including governance, cryptographic inventory, PKI infrastructure, HSMs, applications, authentication, revocation, monitoring, and pilot planning.

For each completed item, assign **one point** and total your score at the end of the assessment. Add your total score at the end of the assessment to determine your organization's overall PQC readiness level.

1. Executive Sponsorship and Strategy

- [ ] Agency PQC transition ownership has been assigned
- [ ] A transition strategy exists
- [ ] Security leadership understands PQC implications
- [ ] Budget planning has begun
- [ ] Applicable federal requirements and agency guidance have been reviewed

TOTAL POINTS: 0

KEY TAKEAWAY

Most agencies will not migrate to PQC overnight. A transition will likely occur over several years and require coordination across multiple teams.

2. Cryptographic Asset Inventory

- [ ] All internal Certificate Authorities identified including appliances (VMWare, Citrix, etc..)
- [ ] All hardware security modules identified
- [ ] Systems exposed to the internet and using sensitive data identified
- [ ] Use of Public CAs documented
- [ ] Applications and Use cases using certificates have been identified
- [ ] Devices and appliances using certificates have been identified
- [ ] Cryptographic algorithms documented

TOTAL POINTS: 0

KEY TAKEAWAY

You cannot migrate what you cannot identify. Many organizations have limited visibility into how certificates are being used across their environment. PKI assessments routinely uncover unknown certificate authorities, undocumented templates, and unmanaged certificate usage.

3. PKI Infrastructure Readiness

- [ ] CA platform versions documented
- [ ] Operating systems supported
- [ ] CA database health reviewed
- [ ] PKI monitoring system deployed
- [ ] Disaster recovery plans updated
- [ ] Certificate issuance capacity evaluated

TOTAL POINTS: 0

KEY TAKEAWAY

PQC certificates are expected to be larger than traditional RSA and ECC certificates. Infrastructure that functions today may experience performance, storage, or operational challenges when handling larger certificates and cryptographic operations. Foundational capabilities such as monitoring, disaster recovery, and capacity planning should be established before evaluating PQC adoption.

© 2026 PKI Solutions LLC All Rights Reserved

4. HSM Readiness

- [ ] HSM vendor identified
- [ ] Current firmware versions documented
- [ ] HSM vendor PQC support and certification roadmap obtained
- [ ] FIPS 140 validation requirements reviewed
- [ ] Performance testing planned
- [ ] Licensing impacts understood

TOTAL POINTS: 0

KEY TAKEAWAY

The HSM is frequently the pacing item for PQC adoption. Many agencies assume PQC readiness is purely a software issue, when in reality the private keys protecting the CA must also be supported by the HSM infrastructure.

5. Application Compatibility

- [ ] Legacy applications & cross-agency interoperability requirements identified
- [ ] TLS termination points identified
- [ ] Mutual TLS deployments identified
- [ ] PIV and smart-card authentication dependencies assessed
- [ ] VPN platforms documented
- [ ] Network appliances inventoried
- [ ] Application certificate requirements documented

TOTAL POINTS: 0

KEY TAKEAWAY

The largest challenge may not be the PKI itself. The biggest risk is often application compatibility. Applications, appliances, and identity platforms may have assumptions about certificate size, key size, signature algorithms, or TLS behavior.

6. Identity and Authentication Readiness

- [ ] Smart card deployments documented
- [ ] Government identity & certificate-based authentication use cases documented
- [ ] Strong certificate mapping implemented
- [ ] ACME usage identified
- [ ] Domain controller readiness reviewed
- [ ] Authentication certificates inventoried

TOTAL POINTS: 0

KEY TAKEAWAY

Certificate-based authentication systems are among the most sensitive areas of a PQC migration. Agencies have successfully navigated cryptographic and PKI-related transitions before. The lessons learned from those efforts demonstrate the value of early planning, visibility, and testing before changes affect production systems.

© 2026 PKI Solutions LLC All Rights Reserved

7. Revocation and Validation Readiness

- [ ] CRL infrastructure documented
- [ ] OCSP infrastructure documented
- [ ] Revocation monitoring implemented
- [ ] CRL size growth evaluated
- [ ] Distribution point capacity reviewed

TOTAL POINTS: 0

KEY TAKEAWAY

Larger certificates and increased cryptographic complexity may place additional stress on validation infrastructure. Revocation failures remain one of the most common causes of PKI outages. Agencies should ensure revocation infrastructure is healthy before introducing additional complexity.

8. Operational Monitoring

- [ ] PKI health is actively monitored and reviewed
- [ ] Certificate expirations are monitored
- [ ] CA and CRL health are monitored
- [ ] HSM health is monitored
- [ ] Configuration drift is monitored

TOTAL POINTS: 0

KEY TAKEAWAY

A PQC migration introduces additional complexity. Organizations should have established operational processes for monitoring PKI health, certificate expirations, revocation services, configuration drift, and HSM dependencies. Effective monitoring helps identify issues early and reduces operational risk during future cryptographic transitions.

9. Pilot Planning

- [ ] PQC lab environment established
- [ ] Pilot use cases identified
- [ ] Test certificates issued
- [ ] Performance baselines collected
- [ ] Rollback plans documented
- [ ] Success criteria defined

TOTAL POINTS: 0

KEY TAKEAWAY

Most organizations are not ready for enterprise-wide PQC deployment today. The immediate goal should be readiness, testing, and controlled pilot programs rather than wholesale migration.

Readiness Score: 0

Score:	Readiness Level:
0-10	Not Prepared
11-20	Early Planning
21-32	Foundational Readiness
33-43	Operationally Prepared
44-53	PQC Transition Ready

© 2026 PKI Solutions LLC All Rights Reserved

Preparing Government PKI for the Post-Quantum Transition

Post-quantum readiness begins with understanding the cryptographic infrastructure that supports your organization's operations.

For government agencies, this includes evaluating certificate authorities, HSMs, identity systems, applications, and the operational processes that support secure communications and authentication.

A structured PKI readiness assessment can help identify existing gaps, evaluate infrastructure dependencies, and establish priorities for future modernization.

Understand Your PKI. Identify the Gaps. Prepare for What's Next.

Recommended Next Steps:

- **Establish visibility** by inventorying certificates, cryptographic algorithms, and PKI-dependent systems.
- **Assess infrastructure readiness** including Certificate Authorities, HSMs, authentication systems, and revocation services.
- **Engage vendors** to understand product-specific PQC support timelines and migration paths.
- **Develop a transition strategy** that aligns with business requirements, regulatory obligations, and technology refresh cycles.
- **Create a test environment** to evaluate PQC-capable solutions and understand potential operational impacts.
- **Continuously reassess readiness** as standards, products, and industry guidance continue to evolve.



Agencies *that begin planning now will be better positioned to adopt post-quantum cryptography with confidence, reduce future migration risk, and maintain trust in their PKI as the cryptographic landscape evolves.*



Need help assessing your organization's PQC readiness?
PKI Solutions can help identify cryptographic dependencies, evaluate PKI infrastructure, and develop a practical roadmap for post-quantum preparedness.

PKI SOLUTIONS

About:

PKI Solutions provides end-to-end Public Key Infrastructure expertise — from specialized consulting and co-managed services to PKI Spotlight®, the industry's first real-time monitoring solution for PKI and HSM environments.

Build a PKI you can trust. Visit **www.pkisolutions.com** to request a demo or consult with a PKI expert.

© 2026 PKI Solutions LLC All Rights Reserved