

Quantum Readiness Framework (QRF[™])

Operationalizing Post-Quantum Migration at the System Level

Turn existing GRC, scanning, asset, and cryptographic data into a decision-ready view of PQC readiness.

Executive Summary

Federal post-quantum cryptography (PQC) transition has moved from long-range preparation to execution. Executive Order 14412 directs an accelerated Federal transition to NIST-approved PQC standards. For Federal civilian agencies, OMB Memorandum M-26-15 requires a risk-based, multi-year PQC Migration Plan and emphasizes governance, prioritization, automation, cryptographic agility, vendor coordination, and measurable progress.

QRF[™] helps organizations turn existing security and technology data into a system-level view of PQC readiness. It brings together evidence already produced across enterprise tools and inventories so leaders can identify which systems need attention, understand the business and mission context behind that need, prioritize migration activity, and track readiness over time.

QRF is designed to complement - not replace - cryptographic discovery and cybersecurity platforms. Its role is to provide the enterprise context needed to move from isolated findings to coordinated migration decisions.

QRF Benefit

QRF gives organizations a practical way to connect cryptographic exposure, system importance, cybersecurity requirements, and migration progress - creating a defensible view of where to act first and how readiness is changing over time.

QRF at a Glance

CONNECT	PRIORITIZE	TRACK	REPORT
Bring together existing enterprise data.	Identify systems that need attention first.	Measure remediation and migration progress.	Give leadership an evidence-backed readiness view.

Executive Decision Support

Decision Question	Typical Friction	QRF Contribution
Where is quantum-vulnerable cryptography?	Relevant evidence is fragmented across enterprise tools and inventories.	Brings findings into system context so leaders can see where exposure exists and who owns it.
Which systems should migrate first?	Technical findings alone do not express mission impact, sensitivity, or modernization dependencies.	Adds enterprise context to support risk-based prioritization and sequencing.
Are we making measurable progress?	Point-in-time inventories make transition velocity difficult to demonstrate.	Maintains a current readiness view and shows how posture changes as migration advances.

Federal Direction: From Inventory to Prioritized Migration

The Federal policy environment reinforces an operating model centered on continuous discovery, risk-based system prioritization, phased migration, automation, and crypto agility. QRF is designed to support those management needs while allowing agencies to retain their existing cybersecurity and GRC ecosystems.

Source	Public Direction	Why It Matters
Executive Order 14412 (June 2026)	Accelerates Federal PQC migration and directs agency leadership, prioritized system transition, and a NIST-led pilot.	PQC readiness is an enterprise transformation issue, not only a cryptography inventory exercise.
OMB M-26-15 (June 2026)	Requires Federal civilian agencies to develop a risk-based PQC Migration Plan, use automation where feasible, and execute migration in phases.	Agencies need a dynamic, system-level view of priorities, ownership, progress, and evidence.
NIST FIPS 203 / 204 / 205	Establishes NIST-approved PQC standards for key establishment and digital signatures.	Organizations need visibility into current cryptography, target states, and migration status.
NIST CSWP 39upd1	Defines and discusses crypto agility across systems, applications, protocols, and enterprise environments.	Migration decisions should support future cryptographic change without unnecessary operational disruption.
NIST CSWP 48 (IPD)	Maps NCCoE PQC migration capabilities to CSF 2.0 outcomes and SP 800-53 controls.	PQC migration can be managed within established cybersecurity risk and control frameworks.

OMB M-26-15 Migration Phases

2026-2027	2027-2028	2028-2030	2031	By 2035
Strategy, planning & discovery	Pilots & early migration	Prioritized migration	Signature migration	Full migration

Why this matters to a CISO

Leadership needs more than a list of vulnerable algorithms. A defensible migration program must show which systems are affected, why they are prioritized, who owns the action, what evidence supports the decision, and whether the organization is making measurable progress.

What QRF Helps Organizations Answer

- Which systems have meaningful PQC exposure or migration dependencies?
- Which systems should receive attention first based on enterprise risk and mission context?
- Where are evidence gaps preventing a confident readiness assessment?
- How is readiness changing as remediation and modernization actions are completed?
- Can leadership see a coherent, repeatable picture of migration status across the enterprise?

From Existing Data to Decision-Ready Insight

QRF is designed to use information organizations already maintain. It can incorporate data from governance, asset, security, cryptographic, and modernization sources and present that information in a consistent system-level context. The objective is to reduce manual reconciliation and help teams focus on decisions and execution.

1 CONNECT DATA	2 ESTABLISH READINESS	3 PRIORITIZE ACTION	4 TRACK PROGRESS
Use existing GRC, asset, security, and cryptographic sources.	Create a consistent enterprise view at the system level.	Focus migration activity where risk and mission impact are highest.	Show how readiness changes as migration advances.

Designed to Work with the Enterprise You Already Have

QRF is intentionally source-agnostic. It can work with a mix of enterprise platforms and managed data sources rather than requiring an organization to replace its current investments.

Governance & Inventory	GRC platforms, CMDBs, system inventories, ownership records, lifecycle information
Technical & Cryptographic Evidence	Cryptographic discovery, vulnerability and security scanning, certificate/PKI information, cloud and network evidence
Planning & Modernization Context	Mission and business criticality, modernization plans, vendor readiness, remediation milestones

QRF Focuses on the Decision Layer

Discovery tools are essential for finding cryptography and technical exposure. QRF is intended to help organizations use those findings in enterprise decision-making - connecting them to systems, organizational priorities, migration activity, and leadership reporting without requiring every source to be standardized first.

The Outcome

A repeatable enterprise picture that helps answer three practical questions: Where are we now? What should we do next? Are we improving?

Public-Release Scope

This public white paper describes QRF at a functional level. Technical implementation details and analytical methods remain proprietary.

A Practical QRF Pilot

A limited pilot can demonstrate the value of a system-level PQC readiness view without waiting for enterprise-wide tool standardization. A representative pilot can begin with a focused group of systems and the data sources already available to the organization.

- Connect selected authoritative system, asset, and security data sources.
- Establish a baseline view of PQC readiness and identify evidence gaps.
- Validate priorities with system owners, security architecture, identity/PKI, and modernization stakeholders.
- Produce a prioritized migration view, progress baseline, and executive-ready reporting.
- Demonstrate a repeatable refresh approach that can scale to additional systems and data sources.

Pilot Success Criteria

A successful pilot should demonstrate traceability from authoritative requirements and enterprise data to actionable system-level decisions; transparent priorities; visible evidence gaps; repeatable refresh; and reporting that both system owners and leadership can use.

Why QRF

Use what you already have	QRF is designed to integrate existing enterprise data rather than force another standalone inventory.
Prioritize at the system level	Technical findings are placed in the context leaders use to fund, sequence, and govern migration.
Measure progress over time	Readiness can be revisited as evidence changes and migration work is completed.
Support leadership decisions	QRF provides a consistent enterprise view for planning, governance, and executive reporting.

About 9th Way Insignia

9th Way Insignia is a Service-Disabled Veteran-Owned Small Business supporting Federal cybersecurity, analytics, automation, ServiceNow, and mission technology programs. QRF helps agencies move from cryptographic findings to enterprise migration decisions while preserving visibility into the evidence and progress behind those decisions.

STOP COLLECTING. START DECIDING.

To discuss a QRF demonstration or pilot engagement:
quantum@insigniatechnology.com

Selected Federal References

- [Executive Order 14412 - Securing the Nation Against Advanced Cryptographic Attacks](#)
- [OMB M-26-15 - Execution of the Migration to Post-Quantum Cryptography](#)
- [NIST Post-Quantum Cryptography Project and FIPS 203, 204, 205](#)
- [NIST CSWP 39upd1 - Considerations for Achieving Crypto Agility](#)
- [NIST CSWP 48 \(Initial Public Draft\) - PQC Migration Mappings to CSF 2.0 and SP 800-53](#)