MUNICIPAL QUANTUM COMPUTING READINESS CHECKLIST

PQC Implementation Pathway and Cost Analysis

For a Municipality of 100,000 Residents

Prepared for:
City of [Municipality Name]
Office of Information Technology

Date: June 2026
Classification: For Official Use Only

Table of Contents

Table of Contents 2
Executive Summary 4
1. Background: The Quantum Threat to Municipal Government 5
1.1 Why Municipalities Must Act Now 5
1.2 Regulatory and Compliance Drivers 5
1.3 Municipal Data at Risk 6
2. The Municipal Quantum Computing Readiness Checklist 7
3. Implementation Pathway 8
Phase 1: Cryptographic Discovery and Inventory (Q3–Q4 2026) 8
Key Activities 8
Staffing Model 9
Estimated Cost — Phase 1 9
Phase 2: Risk Assessment and Prioritization (Q4 2026 – Q1 2027) 9
Key Activities 9
Staffing Model 10
Estimated Cost — Phase 2 10
Phase 3: Architecture Planning and Crypto-Agility (2027) 11
Key Activities 11
Staffing Model 11
Estimated Cost — Phase 3 12
Phase 4: Pilot Migration and Testing (2028) 12
Key Activities 12
Staffing Model 13
Estimated Cost — Phase 4 13
Phase 5: Production Migration (2029–2030) 13
Migration Sequence 14
Key Activities 14
Estimated Cost — Phase 5 14
4. Staffing Strategy 15
4.1 Internal Roles 15
4.2 Consultant Engagements 16
4.3 Training Program 17
5. Consolidated Cost Summary 17
5.1 Budget and Financing Considerations 18

6. Master Implementation Timeline 19
7. Key Risks and Mitigations 20
8. References 20

Executive Summary

Quantum computing represents one of the most significant cryptographic threats to municipal information systems in the coming decade. Nation-state actors are already executing **"harvest now, decrypt later" (HNDL)** strategies - intercepting and storing encrypted government communications today with the intent to decrypt them once sufficiently powerful quantum computers become available. For a municipality of 100,000 residents, this threat extends to citizen records, financial transactions, law enforcement data, utility control systems, and inter-agency communications.[1]

This report synthesizes the Municipal Quantum Computing Readiness Checklist — drawing on guidance from the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and leading practitioners — into a concrete, costed implementation pathway scaled to a mid-size city. The approach prioritizes minimum new headcount, maximum upskilling of existing staff, and targeted consultant engagement.

Phase	Timeline	Estimated Cost
Phase 1: Cryptographic Discovery & Inventory	2026 (Q3-Q4)	$65,000 - $110,000
Phase 2: Risk Assessment & Prioritization	2026 (Q4) - 2027 (Q1)	$40,000 - $75,000
Phase 3: Architecture Planning & Crypto-Agility	2027	$90,000 - $160,000
Phase 4: Pilot Migration & Testing	2028	$120,000 - $200,000
Phase 5: Production Migration	2029-030	$350,000 - $550,000
Ongoing Training & Coordination (annual)	2026-2030	$25,000 - $40,000/yr
TOTAL (5-Year Estimate)	**2026–2030**	**$790,000 – $1,245,000**

Figures above reflect costs for a municipality with approximately 15-25 IT staff, minimal new hires (one part-time Quantum Security Coordinator role absorbed by an existing senior IT staff member), and selective consultant engagement. All costs are in 2026 USD.

[1]CISA. (2023). Quantum-Readiness: Migration to Post-Quantum Cryptography. https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

1. Background: The Quantum Threat to Municipal Government

1.1 Why Municipalities Must Act Now

Modern public-key cryptography — including RSA and Elliptic Curve Cryptography (ECC) — relies on mathematical problems that are computationally infeasible for classical computers. A cryptographically relevant quantum computer (CRQC), using Shor's algorithm, could break these protections. While a CRQC capable of attacking 2048-bit RSA is not yet operational, the convergence of hardware advances, error correction breakthroughs, and geopolitical investment means the threat horizon is measured in years, not decades.

For government organizations, the HNDL threat is already active. The U.S. White House estimated in 2024 that government-wide post-quantum cryptography (PQC) migration would cost approximately **$7.1 billion** across federal systems from 2025–2035.[2] A proportional estimate for a city of 100,000 — scaling by system complexity, not population — places the municipal equivalent in the range of **$790,000 to $1.25 million** over the same period, depending on IT infrastructure scope.

1.2 Regulatory and Compliance Drivers

Several federal mandates and standards now drive state and local government action:

- NIST FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) - the first three finalized post-quantum cryptography standards - were published in August 2024 and are ready for deployment.[3]
- NIST IR 8547 establishes a deadline of 2035 for deprecating quantum-vulnerable algorithms from federal standards. High-risk systems are expected to migrate significantly earlier.
- National Security Memorandum 10 (NSM-10) directs federal agencies to prioritize quantum-resistant cryptography adoption by 2035 and to establish partnerships with state, local, tribal, and territorial (SLTT) entities.
- CISA's Post-Quantum Cryptography Initiative specifically identifies SLTT governments as a priority population for quantum readiness support.[4]
- Executive Order 14306 (2025) directed CISA to publish product categories for technologies using PQC standards, accelerating vendor compliance.

[2]White House Office of Science and Technology Policy. (2024). Report on Post-Quantum Cryptography. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf
[3]NIST. (2024). NIST Releases First 3 Finalized Post-Quantum Encryption Standards. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
[4]CISA. (2025). Post-Quantum Cryptography Initiative. https://www.cisa.gov/quantum

1.3 Municipal Data at Risk

A city of 100,000 typically manages a broad portfolio of sensitive encrypted data, including:

- Citizen personally identifiable information (PII) - utility accounts, permit records, court files
- Law enforcement and public safety communications and records
- Financial systems - payroll, tax, procurement, treasury
- Critical infrastructure control systems - water treatment, traffic management, emergency dispatch
- Inter-agency communications with county, state, and federal partners
- Long-retention archival records (often 10–75-year retention mandates)

The long retention requirements are particularly significant: data encrypted today with RSA-2048 and intercepted by a nation-state adversary could be decrypted once CRQCs become available - well within the retention window of many municipal records.

2. The Municipal Quantum Computing Readiness Checklist

The following eight-item checklist synthesizes guidance from CISA, NIST NCCoE, and PQC industry frameworks into a practical readiness standard for municipalities.[5]

#	Checklist Item	Municipal Application
1	**Assess Cryptographic Inventory**	Catalog all city systems using public-key cryptography: email gateways, VPNs, utility SCADA systems, police CAD systems, financial platforms, and citizen-facing portals. Identify algorithms in use (RSA, ECC, Diffie-Hellman).
2	**Understand the Quantum Threat Timeline**	Brief elected officials, the city manager, and department heads on HNDL risk. Align quantum readiness with the city's long-range technology and capital improvement planning cycles.
3	**Evaluate Post-Quantum Algorithms**	Test NIST-finalized PQC algorithms (ML-KEM/FIPS 203, ML-DSA/FIPS 204, SLH-DSA/FIPS 205) in a non-production lab. Evaluate performance impact on city systems, particularly latency-sensitive public safety applications.
4	**Adopt a Transitional Security Model**	Implement hybrid cryptography — running classical and PQC algorithms in parallel during the transition. This avoids single-point migration risk and maintains compatibility with legacy vendor systems.
5	**Collaborate with Vendors and Partners**	Survey all technology vendors on PQC migration roadmaps. Incorporate PQC readiness requirements into new RFPs and contract renewals. Coordinate with county and state IT offices and regional COGs.
6	**Plan for Compliance and Regulations**	Build a governance framework to track NIST, CISA, and state-level PQC requirements. Document cryptographic assets and maintain a living transition plan updated annually.
7	**Invest in Training and Workforce Culture**	Upskill existing IT and cybersecurity staff via structured PQC training. Brief department directors annually. Designate a Quantum Security Coordinator from existing senior IT staff.
8	**Run Pilot Projects**	Deploy PQC in a controlled non-critical environment first (e.g., internal email encryption, file storage). Document lessons learned before migrating production systems.

[5]Gsinfotechvis. (2025). Post-Quantum Cryptography: Readiness Checklist for 2026. https://medium.com/@gsinfotechvis/post-quantum-cryptography-readiness-checklist-for-2026-8a3cb46e9e45

3. Implementation Pathway

The following five-phase roadmap adapts the NIST NCCoE migration framework and CISA guidance to the operational realities of a 100,000-resident municipality. The approach minimizes new hires, maximizes upskilling, and deploys consultants only for specialized tasks.[6]-[7]

Phase 1: Cryptographic Discovery and Inventory (Q3–Q4 2026)

Attribute	Detail
Objective	Produce a complete map of all cryptographic assets across city systems.
Checklist Items	Items 1, 2
Duration	3-4 months
Lead	Existing IT Director + PQC Consultant (part-time engagement)

Key Activities

- Engage a specialized PQC consultant to deploy cryptographic discovery tooling (e.g., NIST NCCoE-validated scanning tools) across city network segments.
- Catalog all systems using RSA, ECC, or Diffie-Hellman key exchange, including: email/calendaring (Microsoft 365 or Google Workspace), police CAD and records management, utility SCADA/OT systems, financial ERP (e.g., Tyler Technologies Munis), citizen portals and permitting platforms, VPN gateways, and inter-agency shared infrastructure.
- Classify data by sensitivity and retention period. Prioritize assets where data must remain confidential for 10+ years.
- Document all third-party vendor software and cloud service dependencies and their published PQC migration timelines.
- Produce a Cryptographic Asset Register — a structured inventory used in all subsequent phases.

[6]NIST NCCoE. (2024). Migration to Post-Quantum Cryptography. https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc

[7]Hacker, M. (2026). Quantum Readiness by 2030: A Practical Roadmap for Government IT Leaders. https://blog.mikehacker.net/p/quantum-readiness-by-2030-a-practical-roadmap-for-government-it-leaders/

Staffing Model

Role	Type	Time Commitment	Notes
IT Director / CISO	Existing staff	20% FTE	Project sponsor and internal lead
Network/Systems Administrator	Existing staff	30% FTE	Supports scanning and asset documentation
PQC Discovery Consultant	External consultant	~320 hrs @ $175-$225/hr	Specializes in cryptographic scanning tools

Estimated Cost - Phase 1

Cost Item	Low Estimate	High Estimate
PQC Discovery Consultant (320 hrs)	$56,000	$72,000
Cryptographic scanning software/licenses	$5,000	$15,000
Internal staff time (blended IT rate ~$45/hr, est. 90 hrs)	$4,050	$4,050
Phase 1 Total	**$65,050**	**$91,050**

Phase 2: Risk Assessment and Prioritization (Q4 2026 – Q1 2027)

Attribute	Detail
Objective	Score and rank cryptographic assets by quantum risk. Produce a prioritized migration queue.
Checklist Items	Items 2, 6
Duration	2-3 months
Lead	Quantum Security Coordinator (upskilled senior IT staff) + short-term consultant review

Key Activities

- Apply a risk scoring matrix to each asset in the Cryptographic Asset Register, weighting for: data sensitivity, data retention duration, HNDL exposure (internet-facing vs. internal), and migration complexity.

- Use the Microsoft Azure Quantum Resource Estimator (available free at quantum.microsoft.com) to model the quantum threat against current encryption key sizes and algorithm choices.
- Segment assets into three tiers: Tier 1 (migrate first - long-lived sensitive data, internet-exposed), Tier 2 (migrate in Phase 5 production wave), and Tier 3 (low risk - migrate last or as part of system refresh cycles).
- Assess Public Key Infrastructure (PKI) and certificate authority dependencies - these are among the most complex components to migrate and require early planning.
- Survey all major technology vendors on their PQC roadmaps; require written commitment on migration timelines for Tier 1 systems.

Staffing Model

Role	Type	Time Commitment	Notes
Quantum Security Coordinator	Existing staff (upskilled)	50% FTE	Senior IT staff member; receives PQC training in Phase 1
IT Director / CISO	Existing staff	10% FTE	Oversight and executive reporting
Risk Assessment Consultant	External consultant	~80 hrs @ $175-$225/hr	Validates risk scoring methodology

Estimated Cost - Phase 2

Cost Item	Low Estimate	High Estimate
Risk Assessment Consultant (80 hrs)	$14,000	$18,000
Internal Quantum Security Coordinator time (~300 hrs)	$13,500	$18,000
Risk assessment tooling / threat modeling platform	$8,000	$25,000
Vendor PQC survey and legal review	$4,000	$8,000
Phase 2 Total	**$39,500**	**$69,000**

Phase 3: Architecture Planning and Crypto-Agility (2027)

Attribute	Detail
Objective	Redesign system architecture for crypto-agility. Update procurement standards. Establish a PQC lab environment.
Checklist Items	Items 3, 4, 5, 6
Duration	8 -10 months
Lead	Quantum Security Coordinator + Enterprise Architect + PQC Architecture Consultant

Key Activities

- Adopt crypto-agile design patterns across all new and refreshed city systems - ensuring cryptographic algorithms can be swapped via configuration, not code changes.
- Centralize key management using a hardware security module (HSM) or cloud HSM service (e.g., Azure Key Vault Managed HSM with FIPS 140-3 Level 3 validation). AES-256 symmetric keys in such systems are already quantum-resistant.
- Establish a PQC test lab - an isolated network segment used to pilot ML-KEM, ML-DSA, and SLH-DSA algorithms against city system profiles.
- Update the city's IT procurement policy and standard RFP language to require PQC readiness and crypto-agility certifications from all new technology vendors.
- Update the city's IT security policy, system security plans, and risk management framework to incorporate PQC requirements.
- Begin AES-256 deployment for data-at-rest encryption where not already implemented - this is quantum-resistant using current hardware.

Staffing Model

Role	Type	Time Commitment	Notes
Quantum Security Coordinator	Existing staff (upskilled)	60% FTE	Leads lab setup and policy updates
Enterprise Architect / Senior Systems Analyst	Existing staff	25% FTE	Crypto-agility architecture design
PQC Architecture Consultant	External consultant	~240 hrs @ $200-$275/hr	Validates architecture and lab design

Estimated Cost - Phase 3

Cost Item	Low Estimate	High Estimate
PQC Architecture Consultant (240 hrs)	$48,000	$66,000
PQC test lab hardware/infrastructure	$20,000	$40,000
HSM / Key Management system setup	$12,000	$30,000
Policy and procurement document revision (legal/IT)	$5,000	$12,000
Internal staff time (blended, ~400 hrs)	$18,000	$18,000
Phase 3 Total	**$103,000**	**$166,000**

Phase 4: Pilot Migration and Testing (2028)

Attribute	Detail
Objective	Execute controlled PQC migration on non-critical systems. Validate performance. Train IT teams on production implementation.
Checklist Items	Items 3, 7, 8
Duration	10-12 months
Lead	Quantum Security Coordinator + IT Systems team

Key Activities

- Deploy hybrid PQC (classical + post-quantum) on a subset of non-critical systems: internal employee email/file storage, internal intranet services, and test VPN segments.
- Validate TLS, VPN, and SSH implementations using NIST PQC algorithms. Use the Open Quantum Safe (OQS) project's open-source liboqs library for protocol testing.
- Benchmark performance: PQC algorithms generally produce larger key sizes and signatures. Test against real municipal workloads — particularly latency-sensitive 911 dispatch and citizen-facing web applications.
- Deliver structured PQC training to the full IT and cybersecurity team (see Section 4 for training details).
- Document all pilot findings, integration challenges, and vendor coordination issues. Update the Cryptographic Asset Register with migration status.

Staffing Model

Role	Type	Time Commitment	Notes
Quantum Security Coordinator	Existing staff (upskilled)	70% FTE	Leads pilot execution
Systems Administrators (2)	Existing staff	20% FTE each	Implement PQC configurations
PQC Implementation Consultant	External consultant	~160 hrs @ $200–$275/hr	Advises on integration issues; on-call support

Estimated Cost - Phase 4

Cost Item	Low Estimate	High Estimate
PQC Implementation Consultant (160 hrs)	$32,000	$44,000
Staff training (5 IT staff × $10,000-$15,000 per course)	$50,000	$75,000
Software/tooling for PQC pilot deployment	$20,000	$40,000
Internal staff time (blended, ~450 hrs)	$20,000	$20,000
Phase 4 Total	**$122,000**	**$179,000**

Phase 5: Production Migration (2029-2030)

Attribute	Detail
Objective	Complete migration of all production systems to post-quantum cryptography, prioritized by tier.
Checklist Items	Items 1-8 (closure and certification)
Duration	18-24 months
Lead	Quantum Security Coordinator + IT Department + Vendor project teams

Migration Sequence

- Tier 1 (Highest Priority, 2029 H1): Internet-facing citizen portals, VPN gateways, PKI/certificate authority infrastructure, law enforcement records systems, financial ERP platforms.
- Tier 2 (2029 H2): Internal email and collaboration tools, utility billing systems, GIS/permitting platforms, court management systems.
- Tier 3 (2030): Low-sensitivity internal applications, legacy systems scheduled for replacement, SCADA/OT systems (coordinated with utility providers).

Key Activities

- Deploy hybrid cryptography first on all production systems, maintaining backward compatibility throughout.
- Migrate PKI infrastructure and update all certificates to PQC-compliant algorithms — this is the most complex and high-impact single migration task.
- Coordinate SCADA/OT system migration with utility operators and public safety agencies; these may require vendor-managed updates on vendor timelines.
- Revise all system security plans, compliance documentation, and audit procedures to reflect PQC adoption.
- Establish ongoing cryptographic monitoring: quantum computing advances rapidly, and algorithms or key sizes may need revisiting as new NIST guidance (e.g., FN-DSA/Falcon, HQC) is published.

Estimated Cost - Phase 5

Cost Item	Low Estimate	High Estimate
Vendor-managed system migration costs (Tier 1 platforms)	$120,000	$220,000
PKI/Certificate Authority migration (consultant-assisted)	$45,000	$80,000
Tier 2 system migration (mix of in-house and vendor)	$60,000	$100,000
Tier 3 / legacy system migration or decommission	$40,000	$70,000
Compliance documentation update and audit	$20,000	$35,000
Internal staff time (blended, ~800 hrs)	$36,000	$36,000
Phase 5 Total	**$321,000**	**$541,000**

4. Staffing Strategy

The staffing model is built on three principles: (1) no net new headcount during Phases 1-2; (2) one designated Quantum Security Coordinator role absorbed from existing senior IT staff by Phase 2; and (3) targeted consultant use for specialized tasks beyond existing staff capability. This approach reflects the OECD finding that the primary barrier to quantum readiness is not budget, but the shortage of combined quantum-IT-domain expertise.[8]

4.1 Internal Roles

Role	Status	Phase Active	Responsibilities
IT Director / CISO	Existing	All phases	Executive sponsor; city council reporting; budget oversight
Quantum Security Coordinator	Upskilled (from existing senior IT)	Phase 2 onward	Leads day-to-day implementation; manages Cryptographic Asset Register; vendor coordination; policy updates
Network / Systems Administrators (2)	Existing (upskilled)	Phases 1, 4, 5	Cryptographic scanning support; PQC configuration deployment; protocol testing
Enterprise Architect / Senior Systems Analyst	Existing (upskilled)	Phase 3	Crypto-agility architecture design; procurement policy

The Quantum Security Coordinator role does not require a new hire. It should be filled by a senior IT staff member (Network Manager, Systems Architect, or equivalent) who receives structured PQC training in Phase 1 and formally takes on the coordinator responsibilities in Phase 2. This individual becomes the city's institutional quantum knowledge holder.[9]

[8]OECD. (2024). Building Business Readiness for Quantum Computing. https://www.oecd.org/en/publications/building-business-readiness-for-quantum-computing
[9]TechTarget. (2025). Top 5 Quantum Computing Certifications in 2025. https://www.techtarget.com/whatis/feature/Top-quantum-computing-certifications

4.2 Consultant Engagements

Consultant Role	Phase	Estimated Hours	Hourly Rate Range	Notes
PQC Discovery Specialist	1	320 hrs	$175-$225/hr	Cryptographic scanning tools; asset register
Risk Assessment Specialist	2	80 hrs	$175-$225/hr	Validates risk scoring; threat modeling
PQC Architecture Consultant	3	240 hrs	$200-$275/hr	Crypto-agility design; HSM setup; lab design
PQC Implementation Advisor	4	160 hrs	$200-$275/hr	Pilot support; protocol testing; on-call
PKI Migration Specialist	5	120 hrs	$225-$300/hr	Certificate authority migration; PKI redesign
Total Consultant Hours	**All**	**920 hrs**	**Blended ~$200-$250/hr**	**Total: ~$184,000-$230,000**

Consultant rate ranges reflect 2025-2026 market rates for quantum cybersecurity specialists. Rates have risen 25–30% annually in recent years due to strong federal agency demand. Municipalities are advised to issue RFQs and consider multi-phase framework agreements to lock in rates and ensure continuity.[10]

[10]QuantumJobs.us. (2025). Quantum Computing Salaries. https://www.quantumjobs.us/salaries

4.3 Training Program

The following training investments support internal upskilling and are included in phase cost estimates:

Training	Target Staff	Estimated Cost	Timing
ISC2 Certified in Post-Quantum Cryptography or equivalent	Quantum Security Coordinator	$3,000–$5,000	Phase 1
IBM Quantum Learning / AWS Quantum Training (online)	2 Systems Admins	$1,000–$3,000 each	Phase 1–2
PQC Implementation Bootcamp (vendor-led, 3-day)	IT team (5 staff)	$8,000–$15,000/group	Phase 4
Executive Quantum Awareness Briefing	City Manager, Dept. Heads	$2,500–$5,000 (consultant-delivered)	Phase 2
Annual PQC refresher (standards updates)	IT team	$3,000–$6,000/yr	Phase 3 onward

5. Consolidated Cost Summary

The following table consolidates all phase and training costs into a five-year budget projection for a municipality of 100,000 residents with 15-25 IT staff.

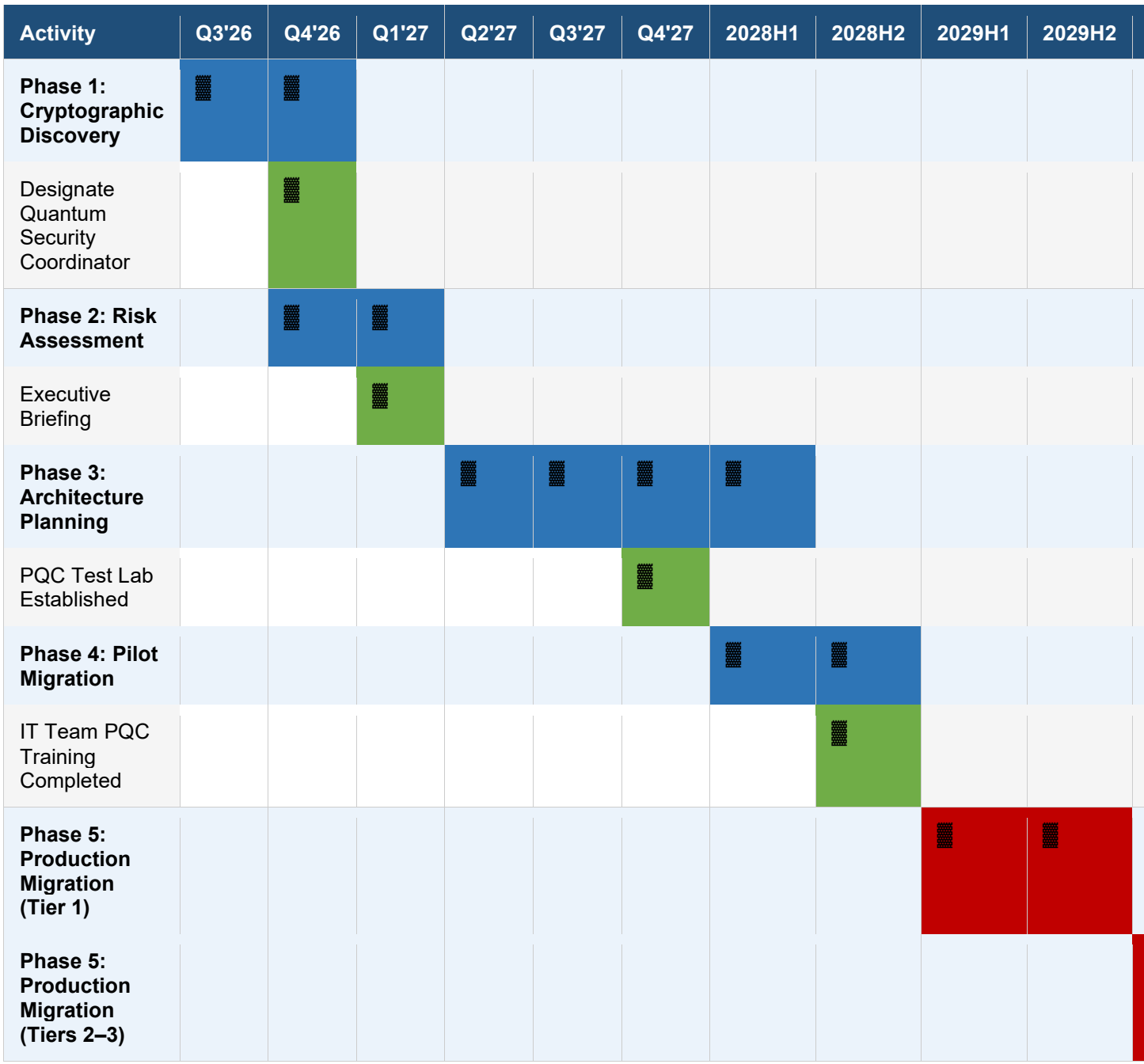
Phase	Description	Timeline	Low Cost	High Cost
1	Cryptographic Discovery & Inventory	Q3-Q4 2026	$65,050	$91,050
2	Risk Assessment & Prioritization	Q4 2026-Q1 2027	$39,500	$69,000
3	Architecture Planning & Crypto-Agility	2027	$103,000	$166,000
4	Pilot Migration & Testing	2028	$122,000	$179,000
5	Production Migration	2029-2030	$321,000	$541,000
—	Ongoing Training & Coordination (annual, ×5 yrs)	2026-2030	$125,000	$200,000
TOTAL	**5-Year Total Investment**	**2026-2030**	**$775,550**	**$1,246,050**

5.1 Budget and Financing Considerations

- Federal and state grants: CISA's State and Local Cybersecurity Grant Program (SLCGP) and FEMA's BRIC program are potential funding sources for cybersecurity upgrades including PQC migration.
- Capital improvement programming: The 5-year timeline aligns well with a typical municipal CIP cycle. Phases 1–2 can be funded from existing IT operating budgets; Phases 3–5 should appear as distinct CIP line items.
- Technology refresh alignment: Where possible, PQC migration should be bundled with existing planned system replacements to avoid double-spending (e.g., migrating a financial ERP that is already scheduled for replacement avoids separate migration costs).
- Multi-jurisdictional cost sharing: Coordinating with the county or a regional Council of Governments (COG) on shared consultant procurement and joint training can reduce per-municipality costs by 20-35%.[11]

[11]U.S. GAO. (2026). Quantum Computing: Updating the National Strategy Could Promote U.S. Leadership. https://www.gao.gov/products/gao-26-107759

6. Master Implementation Timeline



Legend: Blue = Phase Active Green = Milestone Red = Production Migration

7. Key Risks and Mitigations

#	Risk	Likelihood	Mitigation
1	Quantum computing timeline accelerates - CRQC arrives before 2030	Medium	Prioritize Tier 1 HNDL-exposed systems first; HNDL threat exists regardless of CRQC timeline.
2	Vendor systems not PQC-ready on city's timeline	High	Build PQC requirements into all new contracts now; maintain pressure via procurement; align migration to vendor upgrade cycles.
3	Staff turnover - loss of Quantum Security Coordinator	Medium	Cross-train a backup; maintain thorough documentation of the Cryptographic Asset Register and decisions.
4	Budget constraints delay Phase 5 production migration	Medium	Begin grant applications (SLCGP, BRIC) in 2026; align with CIP cycles; pursue regional cost-sharing.
5	NIST updates or adds algorithms, requiring rework	Low–Medium	Crypto-agility architecture (Phase 3) specifically designed to absorb algorithm changes via configuration, not redesign.

8. References

The following sources informed this report and implementation pathway:

CISA. (2023). Quantum-Readiness: Migration to Post-Quantum Cryptography.
CISA. (2025). Post-Quantum Cryptography Initiative.
Gsinfotechvis. (2025). Post-Quantum Cryptography: Readiness Checklist for 2026.
Hacker, M. (2026). Quantum Readiness by 2030: A Practical Roadmap for Government IT Leaders.
NIST. (2024). NIST Releases First 3 Finalized Post-Quantum Encryption Standards.
NIST NCCoE. (2024). Migration to Post-Quantum Cryptography Project.
OECD. (2024). Building Business Readiness for Quantum Computing.
PQShield. (2025). Government Readiness for Quantum Computing and PQC.
QuantumJobs.us. (2025). Quantum Computing Salaries.
TechTarget. (2025). Top 5 Quantum Computing Certifications in 2025.
U.S. GAO. (2026). Quantum Computing: Updating the National Strategy Could Promote U.S. Leadership.
White House OSTP. (2024). Report on Post-Quantum Cryptography.