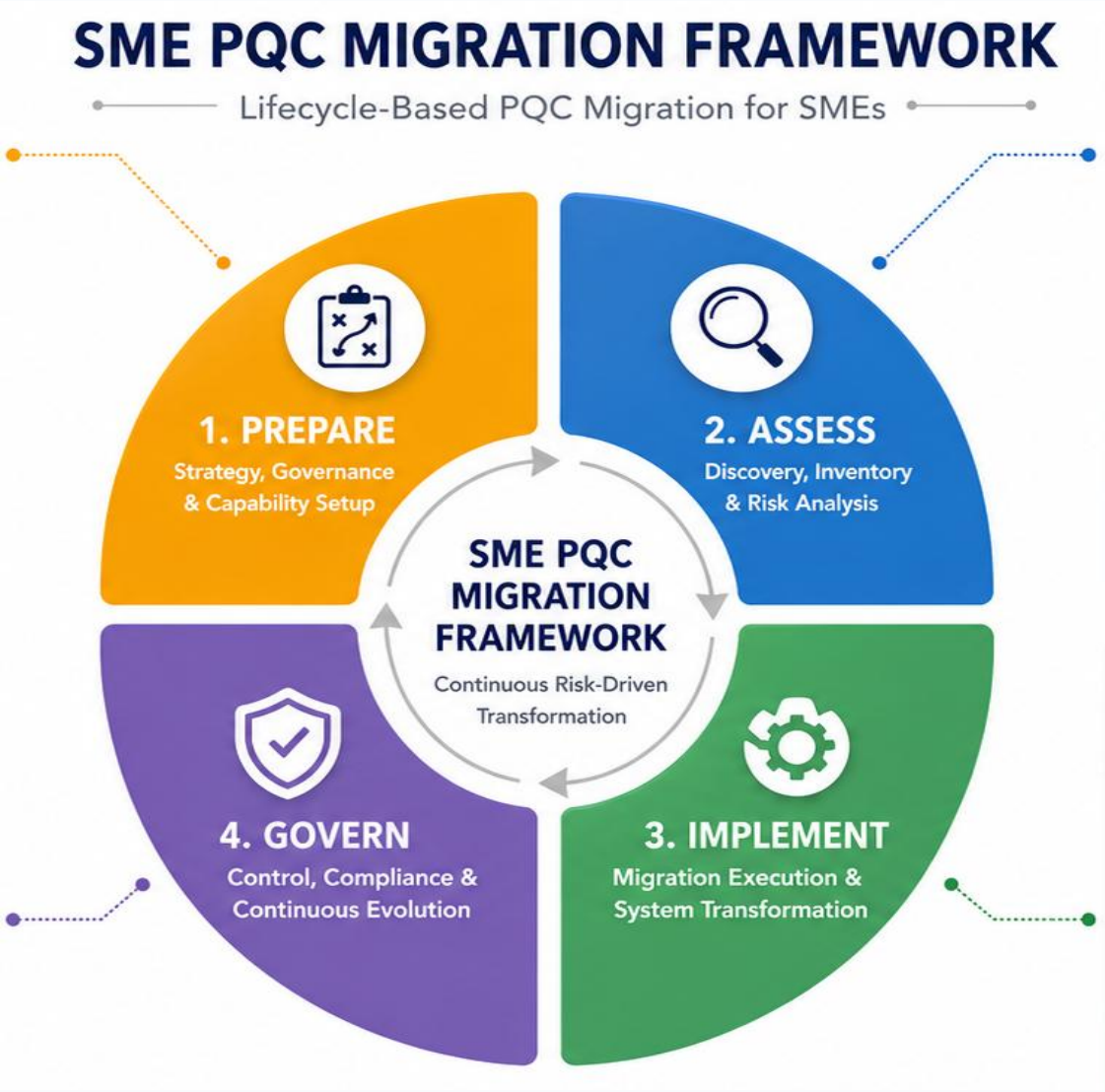
Translating PQC Roadmaps into an Actionable SME Migration Framework



Babatunde Oladoja & Stoyan Tanev

Technology Innovation Management (TIM)
Sprott School of Business
Carleton University | April 2026

Why this research study matters

The problem

- PQC guidance exists, but it is fragmented, high-level, and primarily designed for gov departments and large enterprises.
- SMEs face the same cryptographic risk with fewer security specialists, less formal governance, and tighter budgets.
- Vendor, cloud, and supply-chain dependencies make migration harder to interpret and sequence.

Core research gap

- The missing piece is not awareness of PQC importance and its urgency.
- It is the lack of an SME-executable migration path.

Project objective

Develop an actionable, evidence-based, SME-specific PQC migration framework that translates existing guidance documents into a structured, prioritised, and implementable roadmap aligned with SME constraints.

Design principle

Human-in-the-Loop Generative AI-assisted text analytics approach to shape a rigorous, traceable & reproducible process translating existing guidance into an actionable PQC migration framework.

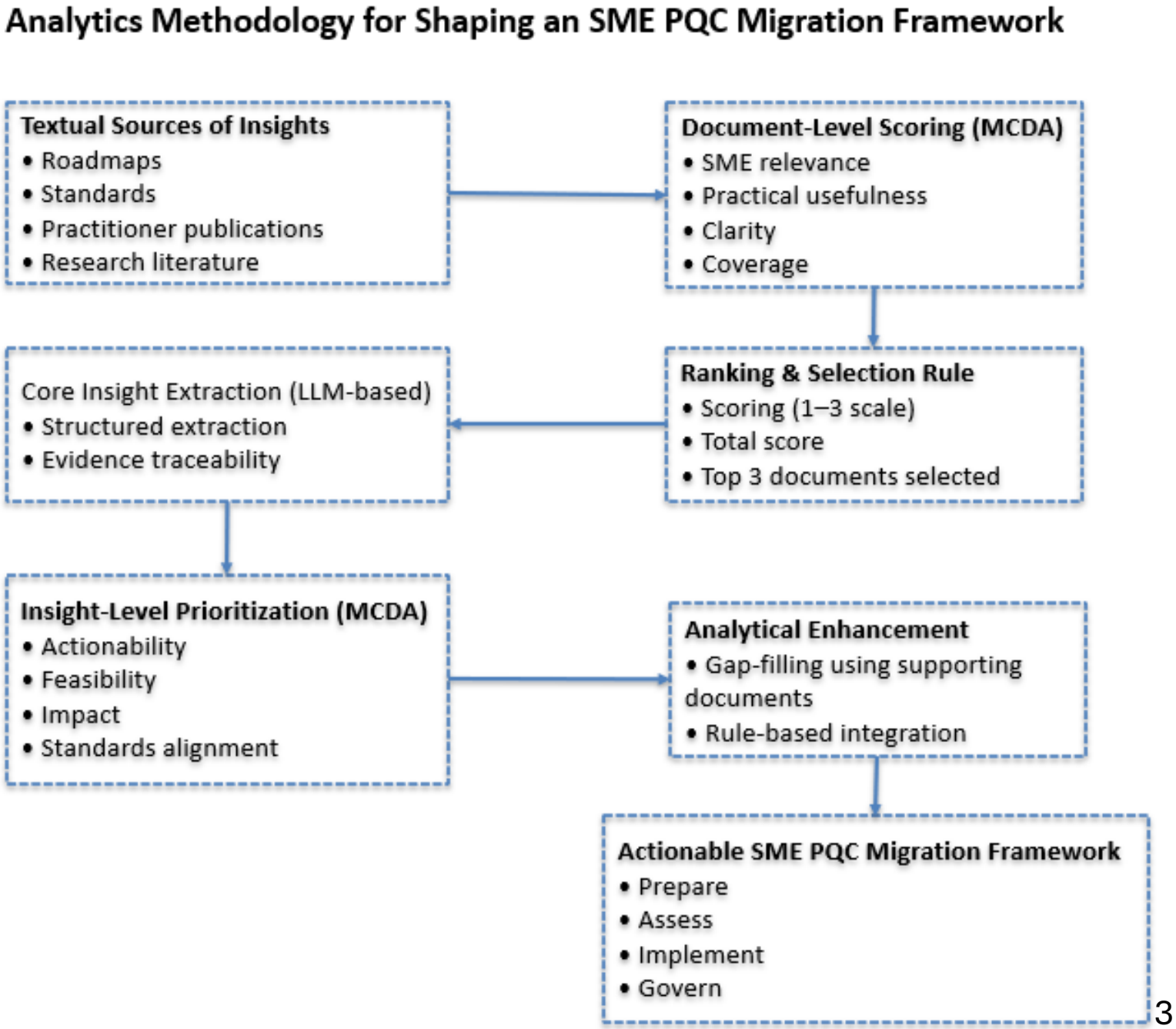
Analytical approach

How the framework was built

- Structured documentary analysis of
  - *PQC roadmaps*
  - *Standards*
  - *Practitioner frameworks*
  - *Academic studies*
- Controlled LLM-assisted extraction of migration actions.
- Multi-Criteria Decision Analysis (MCDA) and human validation to retain only the most relevant SME-feasible, high-impact actions.

Methodological contribution

A replicable pipeline for converting diverse PQC guidance documents into decision-ready organisational actions.



Source selection

Initial corpus

4 Roadmaps

3 Standards

25 Practitioner docs

20 Academic studies

Selection rule

MCDA screening of the 52 documents based on relevance to SMEs, practical usefulness, clarity, and scope.

17 high-value documents selected for deeper insights

Selected set

- 4 roadmaps (baseline)
- 3 standards (normative guidance)
- 6 practitioner docs (actionable advice)
- 4 academic articles (research insights)

Highest ranked documents

- Ultimate Guide to PQC
- IBM–NCSC roadmap
- TNO guidance
- A Banker's Guide to Quantum-Safe Cryptography, Part 3: Roadmap
- Practical Quantum Technologies – Canada Landscape, etc.

Key pattern from MCDA results

Practitioner documents produced the strongest implementation-level guidance, while roadmaps and standards provided structural and compliance anchors.

From evidence to action

The synthesis pipeline

17
high-value docs selected
based on MCDA

→

556
original insights extracted
LLM prompt-based traceable extraction

→

73
prioritised actions
optimized total set of actions

Criteria for selecting the 73 actions

- **Actionability**
- **Feasibility in SME context**
- **Impact on PQC readiness**
- **Alignment with PQC standards**

Distribution of the 73 prioritised actionable insights into 4 natural phases

Counts: Assess 20, Govern 19, Implement 18, Prepare 16 | Total n=73

The SME PQC migration framework

A four-phase lifecycle, not single-phase transition

- **Prepare** lays down the organisational foundation.
- **Assess** builds cryptographic visibility and risk understanding.
- **Implement** executes phased migration with testing and vendor coordination.
- **Govern** turns PQC readiness into a continuous organisational capability.

PREPARE PHASE

PREPARE PHASE RESULTS

Establish governance, strategy, and foundational capabilities for PQC migration

THEME	REPRESENTATIVE ACTIONS (Derived from Results)
1. Governance & Leadership	• Establish executive-sponsored PQC governance structure and cross-functional committee. • Define leadership roles, ownership and responsibilities for PKI and PQC strategy. • Secure organisational commitment and mandate resource allocation for the migration programme.
2. Strategy, Roadmap & Risk Management	• Develop comprehensive PQC strategy, phased migration roadmap and execution plan. • Align roadmap with organisational risk profile, regulatory timelines and business priorities. • Apply risk-based prioritisation (e.g., long-lived data, critical systems, high-risk algorithms).
3. Policy, Compliance & External Engagement	• Review and update cryptographic policies, governance frameworks and compliance obligations. • Engage regulators, vendors, partners and external experts for guidance and collaboration. • Integrate compliance and regulatory requirements into PQC migration planning.
4. Cryptographic Agility & Asset Foundations	• Establish cryptographic asset management and discovery capabilities across the organisation. • Assess algorithm and protocol dependencies across systems, applications and infrastructure. • Build crypto-agility through updatable libraries, tools, architectures and PQC-ready components.
5. Quantum Readiness & Stakeholder Alignment	• Define and communicate a quantum security vision aligned to business value. • Build awareness and training for executives, IT and technical teams. • Align stakeholders from awareness to action to support PQC adoption.
6. Resourcing & IT Integration	• Plan and secure financial, staffing and operational resources for PQC migration. • Address internal skill gaps through training, upskilling or external expertise. • Integrate PQC planning into IT lifecycle, architecture and system design processes.
7. Early Experimentation & Program Development	• Initiate pilots, PoCs and solution discovery activities (e.g., proxy-based testing). • Benchmark and evaluate solutions to inform migration decisions. • Develop playbooks and structured programmes for PQC readiness and execution.

Each action represents a synthesis of multiple detailed insights derived from the analysis of **556** evidence points.

ASSESS PHASE RESULTS

ASSESS PHASE

Build comprehensive understanding, evaluate risks and readiness, and define migration scope

THEME	REPRESENTATIVE ACTIONS (Derived from Results)
1. Cryptographic Bill of Materials Management	• Create and maintain a Cryptographic Bill of Materials (CBOM) with detailed attributes and dependencies. • Identify all systems, assets, and services using cryptography across code, infrastructure and applications. • Prioritise and track improvements to discovery and inventory visibility as part of migration planning.
2. Cryptographic Discovery and Inventory	• Conduct iterative discovery to identify cryptographic usage, algorithms, keys and certificates. • Map cryptography across code, infrastructure, applications and databases (including algorithm and key usage). • Inventory PQC-relevant components including libraries, archives, keystores, software and external products.
3. Dependency and Ecosystem Mapping	• Map dependencies across applications, vendors, external systems and third parties. • Verify algorithm support and availability of quantum-safe libraries across operating environments. • Assess vendors and suppliers and the broader ecosystem for PQC readiness.
4. Quantum Risk and Data Criticality Assessment	• Evaluate data sensitivity and confidentiality (lifespan) and identify long-lived sensitive data. • Classify and prioritise systems and assets based on quantum risk and mission/business criticality. • Assess quantum-related risk using structured frameworks, exposure modelling and cost–benefit analysis.
5. Assessment Documentation and Baselines	• Document assessment artefacts, diagnostic outputs and baseline documentation for PQC migration. • Establish baselines for current cryptographic posture, risks and dependencies. • Create traceable records to support decision-making and future re–assessments.
6. System and Infrastructure Feasibility Analysis	• Analyse system architecture, dependencies and infrastructure constraints (compute, memory, energy, continuity). • Assess legacy systems and constrained technologies to determine feasible migration approaches. • Evaluate PQC algorithm suitability, performance impact and interoperability considerations.
7. Migration Effort and Timeline Estimation	• Define transition risk appetite and identify key visibility gaps and technology readiness. • Estimate migration effort, timelines and sequencing while accounting for execution constraints. • Integrate quantum risk considerations into enterprise risk management and security governance.
8. Organisational Readiness and Governance Assessment	• Evaluate governance clarity, skill sufficiency, resource constraints and requirement fragmentation. • Assess organisational readiness for PQC adoption and ability to absorb change. • Identify capability gaps, training needs and enablers for successful migration.
9. Standards, Regulation and Guidance Review	• Review applicable PQC standards, regulations and compliance requirements. • Monitor regulatory milestones, procurement signals and industry guidance. • Align assessment outputs with regulatory expectations and reporting needs.

Each action represents a synthesis of multiple detailed insights derived from the analysis of **556** evidence points.

IMPLEMENT PHASE RESULTS

Execute phased and risk-aligned migration with testing and infrastructure readiness

IMPLEMENT PHASE	REPRESENTATIVE ACTIONS (Derived from Results)
1. PQC Migration Planning and Sequencing	• Use cryptographic inventory to plan, prioritise and sequence system-level PQC migrations. • Align transitions with asset lifecycles and avoid disruptive rip-and-replace approaches. • Design system-specific migration plans with cutover strategies, contingency measures and hybrid deployment options.
2. PQC Solution Selection and Deployment	• Select, acquire and deploy PQC-capable or hybrid cryptographic solutions aligned with standards and interoperability needs. • Implement interim quantum-risk mitigation controls while full PQC migration is underway. • Implement phased deployments and retire vulnerable cryptographic algorithms.
3. Infrastructure and Application Modernisation	• Plan and implement hardware, software and infrastructure upgrades for PQC readiness. • Upgrade cryptographic infrastructure, libraries and development architectures to support PQC and crypto-agility. • Upgrade security infrastructure and components (e.g., PKI, TLS, SSH, identity systems) to support PQC.
4. Pilot Testing and Laboratory Validation	• Run pilots, proofs of concept and controlled tests to validate PQC solutions in lab and pre-production. • Test implementations in laboratory environments, validating interoperability, usability, performance and security. • Benchmark solutions to inform full deployment decisions.
5. Vendor, Supplier and Ecosystem Execution	• Align supply chain and ecosystem partners with the organisation's PQC transition strategy. • Execute PQC migration in coordination with vendors, suppliers and system owners. • Ensure vendor engagement captures support status, timelines, hybrid capabilities and roadmap commitments.
6. Change Management and SDLC Integration	• Integrate PQC transition activities into organisational change management and development processes. • Ensure PQC is integrated across SDLC, APIs and application/product lifecycles. • Continuously execute, monitor and adjust the migration program during implementation.
7. Legacy and Non-Migratable Systems	• Implement mitigation strategies for legacy or non-migratable systems using asset-level decisions. • Retire, accept temporarily or remediate systems based on risk, usage and compliance impact. • Maintain business continuity while reducing quantum-related risk exposure.
8. Quality Assurance, Compliance and Inventory	• Validate PQC implementations and ensure compliance with standards and policies. • Update cryptographic inventories to reflect new implementations and retirements. • Maintain configuration records and evidence for compliance and audit.
9. Centralised Crypto and Key Management Services	• Establish centralised cryptographic services and key management infrastructure. • Implement automated key management, rotation and lifecycle controls. • Ensure infrastructure supports PQC algorithms and TLS termination where appropriate.

Each action represents a synthesis of multiple detailed insights derived from the analysis of **556** evidence points.

GOVERN PHASE RESULTS

GOVERN PHASE

Sustain, measure, and continuously improve PQC governance, compliance, and resilience

THEME	REPRESENTATIVE ACTIONS (Derived from Results)
1. PQC Governance Bodies and Leadership Roles	• Establish PQC governance bodies, roles, and ownership across the organisation. • Appoint and empower cryptographic champions to coordinate PQC adoption.
2. PQC Roadmap Evolution and Milestone Tracking	• Establish and evolve a PQC migration roadmap with defined milestones and timelines. • Align roadmap with external regulatory and vendor transition milestones.
3. Programme Monitoring, Measurement, and Reporting	• Monitor, measure, and report PQC migration progress as a managed risk program using defined KPIs (e.g., reduction in quantum-vulnerable systems). • Report outcomes to leadership through regular dashboards and governance reporting.
4. Continuous Monitoring and Control Adaptation	• Continuously monitor PQC implementations and adapt controls over time. • Incorporate posture and policy management as part of ongoing governance.
5. Exception Management and Incident Response	• Manage exceptions, sunsets, and disallowed cryptography through formal registries and monitoring. • Define and execute incident response procedures within plano, ensuring defined escalations and remediation.
6. PQC Standards and Technology Horizon Scanning	• Track and respond to PQC standardisation, protocol, and technology developments. • Monitor certificate ecosystem readiness and technology maturity before production deployment.
7. Cryptographic Policy and Standards Lifecycle	• Maintain and update cryptographic and PQC policies, standards, and procedures. • Embed cryptographic agility requirements into governance, processes, and technical practices.
8. Enterprise Risk and Compliance Integration	• Integrate PQC and quantum risk into enterprise cyber, risk, and governance models. • Continuously assess and report on risks such as inventory gaps, crypto-agility limitations, technology readiness, resource constraints, and leadership alignment.
9. Regulatory Compliance and Standards Alignment	• Ensure compliance with PQC-related regulations and standards. • Align migration timelines with government adoption schedules and leverage hybrid approaches where needed to meet certification constraints.
10. Vendor and Product Cryptography Governance	• Govern vendor and product cryptography by enforcing PQC-capable upgrade paths. • Incorporate procurement preferences and vendor transition expectations into governance processes.
11. Governance Refinement through Feedback and Workshops	• Use workshops, pilots, and structured feedback mechanisms to refine PQC governance and migration plans. • Continuously improve processes based on stakeholder input and operational learnings.
12. Workforce Capability Assessment and Training	• Assess workforce capability and address skill gaps. • Provide PQC training through role-based assessments and structured learning plans.
13. Knowledge Sharing and Industry Collaboration	• Create and participate in PQC knowledge-sharing and collaboration initiatives. • Engage with governments, industry bodies, and peers to share best practices and intelligence.
14. Incident Response and Security Culture	• Establish a quantum-aware incident response capability and culture. • Continuously update security posture to respond to emerging quantum threats.
15. Stakeholder Communication and Regulatory Reporting	• Communicate PQC strategy and progress to stakeholders and regulators. • Provide evidence of migration plans, outcomes and risk posture in line with supervisory expectations.
16. Strategic Positioning and Trust	• Use adoption of quantum-safe cryptographic standards as a trust and market differentiation strategy. • Demonstrate leadership in PQC readiness to build stakeholder and customer confidence.

Each action represents a synthesis of multiple detailed insights derived from the analysis of 556 evidence points.

Key findings

Four messages that run across the full framework

01 **PQC migration is a structured organisational transformation**

It requires governance, coordination, and continuous adaptation — not just algorithm replacement.

02 **Discovery and risk assessment drive the transition**

Inventory, dependency mapping, CBOMs, and data criticality are key prerequisites for shaping migration decisions.

03 **Vendor and ecosystem dependence is central**

Cloud platforms, suppliers, and third-party technologies strongly shape migration timing and feasibility.

04 **Implementation must be phased and adaptive**

Pilots, hybrid cryptography, and lifecycle-aligned sequencing outperform blanket replacement strategies.

Practical implications

What SMEs should do first

Implications for SMEs

- Start with governance, not technology
- Prioritise cryptographic visibility through inventory and CBOM development
- Adopt risk-based migration waves instead of blanket replacement
- Treat vendors and suppliers as central migration actors
- Build continuous monitoring, policy adaptation, and workforce capability

Management implication

The framework helps SMEs move from uncertainty to structured, evidence-based decision-making.

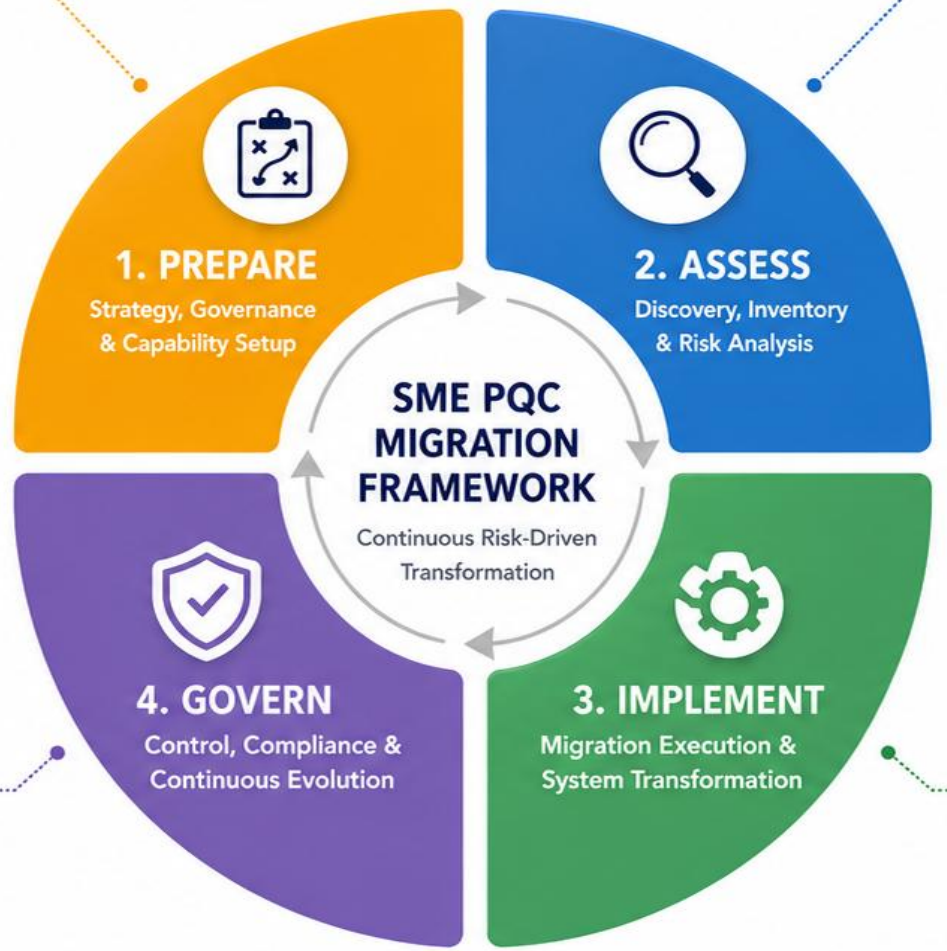
Suggested migration work packages

1. **Governance and ownership**
2. **Discovery and CBOM development**
3. **Risk and feasibility assessment**
4. **Pilot execution and continuous governance**

Each work package should define specific ownership, timelines, and success metrics.

SME PQC MIGRATION FRAMEWORK

Lifecycle-Based PQC Migration for SMEs



1 PREPARE

KEY INSIGHTS

Governance & Leadership
Establish PQC governance structure, roles and executive sponsorship.

Strategy & Roadmap
Define PQC strategy, roadmap and milestones aligned to business goals.

Policy & Compliance Alignment
Review policies, standards and ensure compliance obligations.

Stakeholder Awareness & Training
Build awareness, skills and communication across teams.

Early Experimentation
Run pilots and PoCs to validate feasibility and reduce risk early.

2 ASSESS

KEY INSIGHTS

Cryptographic Discovery & Inventory
Create CBOM and discover all crypto assets, systems, keys and certificates.

Dependency & Ecosystem Mapping
Map dependencies across applications, infrastructure, vendors and third parties.

Risk & Data Sensitivity Assessment
Assess quantum risk, data criticality and prioritise high-risk exposures.

Feasibility & Constraint Analysis
Analyse technical, operational and business constraints and options.

Migration Scope & Timeline
Define migration scope, sequencing, timelines and quick wins.

4 GOVERN

KEY INSIGHTS

Monitoring & KPI Tracking
Monitor PQC progress, security posture and KPI performance.

Roadmap & Milestone Tracking
Track milestones and adapt roadmap based on risk and technology changes.

Risk, Compliance & Standards
Integrate PQC into enterprise risk, audits and compliance programs.

Vendor Governance
Govern vendors and products; enforce SLAs and crypto-agility.

Incident Response & Trust
Embed PQC in incident response plans and build trust with stakeholders.

3 IMPLEMENT

KEY INSIGHTS

Migration Planning & Sequencing
Plan migration waves, dependencies and cutover strategy.

Solution Selection & Deployment
Select PQC solutions and deploy PQC-enabled services, libraries and tools.

Infrastructure Modernisation
Modernise infrastructure and applications for PQC readiness and interoperability.

Testing & Validation
Test interoperability, performence, security and failure scenarios.

Vendor & Ecosystem Execution
Engage vendors, manage contracts and ensure delivery.

Crypto & Key Management Services
Establish/modernise key management and cryptographic operations.

CROSS-CUTTING ENABLERS (Across All Phases)

- Crypto Agility by Design
- Stakeholder & Ecosystem Collaboration
- Data Protection & Confidentiality
- Regulatory & Standards Alignment
- Continuous Improvement & Feedback Loops

References

• Ahmed, S. K., Mohammed, R. A., Nashwan, A. J., Ibrahim, R. H., Abdalla, A. Q., Ameen, B. M. M., & Khdhir, R. M. (2025). Using thematic analysis in qualitative research. Journal of Medicine, Surgery, and Public Health, 6, 100198. https://doi.org/10.1016/j.glmedi.2025.100198

• Communications Security Establishment Canada. (2025). Roadmap: Migration to post-quantum cryptography for the Government of Canada (ITSM.40.001). https://www.cyber.gc.ca/sites/default/files/itsm.40.001-migration-post-quantum-cryptography-government-canada-e.pdf

• Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organisations to post-quantum cryptography. Nature, 605(7909), 237–243. https://doi.org/10.1038/s41586-022-04623-2

• National Institute of Standards and Technology. (2023). PQC migration: NIST SP 1800-38B preliminary draft. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf

• PQC Coalition. (2025). PQC migration roadmap. https://pqcc.org/wp-content/uploads/2025/05/PQC-Migration-Roadmap-PQCC-2.pdf

• World Economic Forum. (2023). Quantum readiness toolkit. https://www3.weforum.org/docs/WEF_Quantum_Readiness_Toolkit_2023.pdf