
Translating Post-Quantum Cryptography Roadmaps into an Actionable SME Migration Framework

Babatunde Oladoja and Stoyan Tanev*

Technology Innovation Management Program, Sprott School of Business, Carleton University, Ottawa, ON, Canada

E-mail: stoyan.tanev@carleton.ca

**Corresponding Author*

Received 21 July 2026; Accepted 12 August 2026

Abstract

Small and medium-sized enterprises (SMEs) face the same quantum-era cryptographic exposure as large organisations, but they often lack the specialised security teams, governance maturity, asset visibility, and implementation budgets assumed by most post-quantum cryptography (PQC) roadmaps developed for governments, public institutions, and large enterprises. This paper addresses this challenge by adopting a structured research process to develop an evidence-based, SME-specific PQC migration framework that translates practical insights from existing roadmaps, standards, practitioner publications, and academic studies into structured actionable guidance. The framework also identifies activities that extend beyond typical SME capabilities into the operational domain of larger enterprises. The research study uses a human-supervised, large-language-model (LLM)-assisted text-analytics workflow based on a comprehensive multi-criteria decision analysis (MCDA). An initial corpus of 52 documents was evaluated for SME relevance, practical usefulness, clarity, and coverage. Seventeen high-value documents were selected for deeper analysis, producing 556 source-linked

Quantum Information Technologies Journal, Vol. 2_1, 75–104.

doi: 10.13052/qitj2795-0492.215

© 2026 River Publishers

migration insights. These insights were validated, consolidated, and prioritised into 73 decision-oriented actions organised across four phases: Prepare, Assess, Implement, and Govern. The results show that PQC migration is not simply an algorithm-replacement exercise; it is an organisational transformation process requiring governance, cryptographic visibility, vendor coordination, phased implementation, and continuous monitoring. The contribution is both practical and methodological: a lifecycle-based migration model for SMEs and larger enterprises, and a replicable evidence-to-action analytical process for converting dispersed technical guidance into context-specific organisational action.

Keywords: Post-quantum cryptography, SME cybersecurity, quantum-safe migration, cryptographic inventory, crypto-agility, standards adoption, text analytics, LLM-assisted research.

1 Introduction

Post-quantum cryptography (PQC) has moved from a specialised cryptographic research issue into an organisational readiness challenge. The National Institute of Standards and Technology (NIST) final standards define approved quantum-resistant mechanisms for key establishment and digital signatures [1–3], while national and industry roadmaps establish transition priorities, sequencing, inventory, risk assessment, and governance expectations [4–7]. These developments focus on the technical destination, but they do not by themselves solve the adoption problem for SMEs. For many SMEs, the question is no longer whether quantum-safe migration matters; the more difficult question is how to convert broad guidance into a feasible sequence of actions under constrained resources. The key issue is that existing PQC guidance is valuable, but it is frequently written for governments, critical-infrastructure operators, financial institutions, and large enterprises with mature cybersecurity functions [4–13]. Such organisations can assign specialised teams to inventory cryptography, model dependencies, run pilots, negotiate vendor roadmaps, and report progress to senior executives. SMEs deal with a different reality. They often depend on cloud platforms, managed service providers, vendor-controlled software, informal governance processes, limited security staffing, and incomplete visibility into where cryptography is used across applications, certificates, protocols, APIs, backups, devices, and third-party services. The current status of PQC adoption can therefore be characterised by a standards-to-implementation challenge.

Standards define the cryptographic destination, and roadmaps describe the broad migration logic, but SMEs still need decision support: what to do first, how to determine risk, how to identify vendor dependencies, how to sequence implementation, and how to govern readiness over time. Without such guidance, PQC migration can appear as a distant technical problem rather than a manageable programme of organisational work.

The objective of this paper is to develop an actionable, SME-focused PQC migration framework derived from a structured textual evidence pipeline. The research process focuses on translating practical insights from heterogeneous guidance documents into a prioritised set of SME-feasible migration actions while retaining enterprise-relevant extensions. The resulting framework treats PQC migration as a dynamic journey including four phases – Prepare, Assess, Implement, and Govern – rather than a homogeneous, one-time technical replacement project. The research study is an example of an applied research project which is driven by the practical needs of SMEs and larger enterprises.¹ The core practical challenge is the fragmentation of PQC migration guidance and its limited operational fit for SMEs. In addition, the PQC knowledge domain is distributed across different types of sources that serve different purposes: standards specify normative cryptographic baselines [1–3]; roadmaps provide policy direction and strategic sequencing [4–7]; practitioner publications translate strategy into implementation guidance [8–13]; and academic studies explain adoption barriers, organisational readiness, system dependencies, and transition design [14–25]. SME managers need all these streams of actionable insights integrated into one traceable and decision-oriented framework.

This study makes several contributions that correspond to the key research steps and deliverables (Table 1).

First, it builds a transparent document-based analytical pipeline beginning with a corpus of 52 PQC-related documents and using MCDA to select the most relevant sources. Second, it applies a controlled, human-supervised LLM-assisted practical insight extraction process to convert unstructured guidance into source-traceable organisational insights. Third, it consolidates and prioritises those insights into 73 actions using operational importance,

¹The study distinguishes between SMEs and larger enterprises. In Canada, an SME is officially defined as any business with 1 to 499 paid employees: <https://ised-isde.canada.ca/site/sme-research-statistics/en/key-small-business-statistics/key-small-business-statistics-2025>. In the context of this study, a larger enterprise is defined as a business with 500 to 1500 employees.

Table 1 Summary of the research process, key deliverables and contributions

Contribution Area	What the Study Provides	Practical Value for SMEs
Evidence synthesis	A structured corpus of 52 roadmaps, standards, practitioner documents, and academic studies.	Prevents SME guidance from relying on a single source or isolated expert opinion.
Methodological pipeline	Document-level MCDA, LLM-assisted extraction, human validation, insight-specific MCDA, and framework synthesis.	Creates traceable, reproducible translation from complex documents into actions.
Action library	556 extracted insights consolidated into 73 prioritised actions.	Gives SMEs a manageable action set instead of an overwhelming document landscape.
Migration framework	Four phases – Prepare, Assess, Implement, and Govern – of an integrated model.	Supports staged planning, risk-based prioritisation, and continuous governance.

SME practicality, evidence breadth, and standards alignment. Fourth, it synthesises the actions into a four-phase framework that distinguishes an SME-executable core set of activities from additional enterprise-focused extensions.

2 Empirical Foundation and Review of Data Sources

The empirical foundation of the study is based on four source categories: PQC adoption roadmaps, technology standards, practitioner publications, and academic studies. Practitioner publications were further divided into private-sector and government or consortium sources because these two groups provide different forms of implementation guidance. Each category contributed a distinct layer of knowledge.

Roadmaps provided strategic direction and transition sequencing; standards established the normative cryptographic destination; practitioner publications translated strategic and technical requirements into operational activities; and academic studies explained organisational adoption, implementation barriers, and migration-management considerations. Taken together, these sources provided the strategic, technical, operational, and organisationally documented evidence used to develop the SME and enterprise PQC migration frameworks.

2.1 Roadmaps: Strategic Direction and Transition Sequencing

Roadmaps are transition-oriented documents published by national cybersecurity authorities, public agencies, and industry coalitions. They define how organisations should prepare for, plan, sequence, implement, and govern the transition from quantum-vulnerable cryptography to post-quantum cryptography. Unlike formal technical standards, roadmaps do not primarily specify cryptographic algorithms. Instead, they address organisational readiness, programme ownership, asset discovery, risk prioritisation, stakeholder responsibilities, migration sequencing, implementation milestones, vendor coordination, testing, and continuing governance [4–7]. The study examined four roadmaps: the Canada PQC Migration Roadmap [4], published by the Canadian Centre for Cyber Security; the PQC Migration Roadmap, published by the Post-Quantum Cryptography Coalition [5]; the EU Post-Quantum Cryptography Migration Roadmap [6]; and Planning for Post-Quantum Cryptography, prepared by the Australian Cyber Security Centre [7]. All four roadmaps were retained for detailed analysis because they provided complementary national, policy, industry, and implementation perspectives. They were, however, not retained because they were specifically designed for SMEs. Rather, they served as strategic anchors whose public-sector and enterprise-oriented recommendations could be translated into proportionate actions for smaller organisations [4–7].

The Canada PQC Migration Roadmap [4] was retained as the primary national anchor. It provides a structured transition direction for the Government of Canada systems and the organisations, suppliers, and service providers connected to the federal technology ecosystem. Its principal impact on the final framework was the adoption of an understanding of PQC migration as a managed organisational programme rather than as an isolated algorithm-replacement exercise. The roadmap informed the selection of activities related to executive and operational ownership, migration planning, cryptographic inventory, system prioritisation, implementation sequencing, supplier engagement, and continuing governance. It has also reinforced the importance of protecting information that must remain confidential for long periods of time and aligning migration decisions with procurement, national cybersecurity expectations, and supplier readiness. Within the SME framework, these requirements were incorporated as proportionate actions such as assigning a named PQC-readiness owner, maintaining a basic register of critical systems and vendors, monitoring Canadian guidance, identifying long-lived sensitive information, and introducing PQC-readiness questions

into procurement and vendor discussions. Taken together, the four roadmaps established the strategic architecture of the final framework.

2.2 Standards: Normative Cryptographic Baselines

Standards define the technical destination of the migration. While roadmaps explain how organisations should organise and sequence the transition, standards specify the cryptographic mechanisms that systems, products, and services are expected to adopt. The study retained three NIST standards: FIPS 203, FIPS 204, and FIPS 205 [1–3].

FIPS 203 [1] specifies the Module-Lattice-Based Key-Encapsulation Mechanism, commonly referred to as ML-KEM. Its primary contribution to the framework was to establish the approved technical baseline for quantum-resistant key establishment. This mechanism is relevant to systems that depend on public-key cryptography for establishing shared secrets, including secure communications, virtual private networks, cloud connections, web services, and other encrypted exchanges. Although the framework does not instruct SMEs to implement ML-KEM directly, FIPS 203 provides the basis for asking whether vendors, software products, cloud platforms, and managed-service providers are preparing to support approved quantum-resistant key-establishment mechanisms. FIPS 204 [2] specifies the Module-Lattice-Based Digital Signature Standard, commonly referred to as ML-DSA. It contributed the normative baseline for quantum-resistant digital signatures used to support authentication, integrity, software signing, document signing, certificate systems, and trusted communications. Its impact on the framework was reflected in activities involving certificate inventories, code-signing dependencies, software update mechanisms, authentication systems, public key infrastructure, and vendor assurance. For SMEs, the standard was translated into practical questions concerning whether suppliers intend to support recognised PQC signature mechanisms and whether existing products can be upgraded without major replacement. FIPS 205 [3] specifies a Stateless Hash-Based Digital Signature Standard, commonly referred to as SLH-DSA. It provided an additional approved signature mechanism based on a different cryptographic foundation. Its inclusion was important because it demonstrated that PQC migration does not involve a single universal algorithm. Different systems, applications, performance requirements, and assurance contexts may require different standards aligned mechanisms. This supported the framework’s emphasis on vendor-supported solution selection, interoperability testing, performance assessment, and avoidance of unsupported internal algorithm choices.

The direct SME-relevance scores of the three standards [1–3] were relatively low (see Table 2) because the documents do not describe organisational governance, migration programmes, resource allocation, vendor management, or implementation sequencing. Nevertheless, all three were retained as mandatory reference baselines. Their role was normative rather than operational: they established what recognised PQC mechanisms look like, while the roadmaps, practitioner publications, and academic studies informed how organisations should prepare for and manage their adoption.

2.3 Practitioner Publications: Implementation and Ecosystem Guidance

Practitioner publications [8–13] provide strategic and technical guidance to inform the shaping of operational activities that organisations can use in migration planning and implementation. These documents are produced by technology vendors, cybersecurity firms, research organisations, industry coalitions, public agencies, and government-linked implementation bodies. Unlike formal standards, they commonly address how to conduct cryptographic discovery, develop inventories, assess risks, engage vendors, design roadmaps, test systems, manage legacy technologies, select solutions, update procurement requirements, and monitor implementation progress. The initial corpus contained 25 practitioner publications, comprising 19 private-sector documents and six government or consortium documents. The separation was analytically important. Private-sector publications generally provided product, architecture, cryptographic-management, and implementation perspectives. Government and consortium publications provided broader ecosystem, policy, readiness, coordination, and public-interest perspectives. Six practitioner documents were selected for detailed extraction: three private-sector documents [8–10] and three government or consortium documents [11–13].

2.3.1 Private-sector practitioner publications

The three selected private-sector publications were DigiCert’s Ultimate Guide to Post-Quantum Cryptography [8], the IBM-NCS Quantum Security Roadmap [9], and A Banker’s Guide to Quantum-Safe Cryptography, Part 3: Roadmap to PQC Migration, published by Cryptomathic [10]. DigiCert’s Ultimate Guide to Post-Quantum Cryptography [8] contributed practical guidance concerning certificates, public key infrastructure, cryptographic discovery, digital trust, and crypto-agility. Its impact was strongest in the Assess and Implement phases. It supported activities involving certificate

Table 2 The 17 documents selected for more comprehensive practical insight extraction

No	Ref. #	Document	Category	Score	Selection Role
1	[8]	The Ultimate Guide to Post-Quantum Cryptography	Practitioner–Private	12	Top private-sector practitioner source
2	[9]	IBM–NCS Quantum Security Roadmap	Practitioner–Private	11	Top private-sector practitioner source
3	[10]	A Banker’s Guide to Quantum-Safe Cryptography, Part 3: Roadmap	Practitioner–Private	11	Top private-sector practitioner source
4	[11]	The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography	Practitioner–Government/ Consortium	11	Top government/ consortium practitioner source
5	[12]	Transitioning to a Quantum-Secure Economy	Practitioner–Government/ Consortium	11	Top government/ consortium practitioner source
6	[13]	Canadian National Quantum-Readiness: Best Practices and Guidelines	Practitioner–Government/ consortium	11	Top government/ consortium practitioner source
7	[14]	Preparing Your Organisation for the Quantum Threat to Cryptography	Academic	10	Top academic source
8	[15]	Transitioning Organisations to Post-Quantum Cryptography	Academic	10	Top academic source
9	[16]	PMMP – PQC Migration Management Process	Academic	10	Top academic source
10	[17]	Preparing for Post-Quantum Cryptography: Impacts on Classical Cybersecurity Operations of SMEs	Academic	9	Selected at academic threshold; direct SME relevance
11	[5]	PQC Migration Roadmap	Roadmap	9	Supporting strategic roadmap

(Continued)

Table 2 Continued

No	Ref. #	Document	Category	Score	Selection Role
12	[6]	EU Post-Quantum Cryptography Migration Roadmap	Roadmap	9	Supporting strategic roadmap
13	[7]	Planning for Post-Quantum Cryptography	Roadmap	9	Supporting strategic roadmap
14	[4]	Canada PQC Migration Roadmap (ITSM.40.001)	Roadmap	7	Primary national anchor
15	[1]	FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard	Standard	4	Normative reference baseline
16	[2]	FIPS 204: Module-Lattice-Based Digital Signature Standard	Standard	4	Normative reference baseline
17	[3]	FIPS 205: Stateless Hash-Based Digital Signature Standard	Standard	4	Normative reference baseline

inventories, identification of cryptographic use, assessment of PKI dependencies, preparation for certificate and algorithm changes, and engagement with vendors responsible for digital certificates and trust services. For SMEs, these ideas were translated into practical actions such as identifying certificate-dependent systems, recording certificate renewal dates, asking vendors about PQC-ready certificates, and ensuring that systems can accommodate future cryptographic changes.

The IBM-NCS Quantum Security Roadmap [9] suggests a structured enterprise migration perspective covering discovery, assessment, transformation, and continuing management. Its principal impact was the treatment of migration as a multi-stage programme supported by cryptographic inventory, risk assessment, prioritisation, pilot implementation, and cryptology. It informed the four-phase framework, particularly activities relating to discovery, migration roadmaps, controlled experimentation, technology modernisation, and ongoing monitoring. The enterprise framework retained IBM's emphasis on automated discovery, formal programme structures, and large-scale transformation. The SME framework translated these concepts into lightweight inventories, vendor-supported pilots, managed services, and phased upgrades.

Cryptomathic's *A Banker's Guide to Quantum-Safe Cryptography, Part 3: Roadmap to PQC Migration* [10] provided a sector-specific view of

migration in a highly regulated and cryptographically dependent environment. Its impact was most visible in the treatment of risk-based sequencing, key-management systems, regulatory exposure, transaction security, legacy systems, and the need to preserve interoperability during transition. Although the source was written for financial institutions rather than SMEs generally, it contributed important evidence on the need to sequence migration according to system criticality, data sensitivity, dependency, and operational risk. These concepts were adapted for SMEs by replacing complex banking governance structures with simpler prioritisation based on critical systems, sensitive data, vendor dependency, and replacement feasibility.

2.3.2 Government and consortium practitioner publications

The three selected government or consortium practitioner publications were The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography [11], the World Economic Forum's Transitioning to a Quantum-Secure Economy [12], and Canadian National Quantum-Readiness: Best Practices and Guidelines [13]. The PQC Migration Handbook [11] provides detailed planning, readiness, and risk-management recommendations. Its impact included the need to identify cryptographic assets, understand organisational dependencies, evaluate migration feasibility, plan transition stages, and account for operational and supply-chain risks. It strengthened the framework's focus on practical migration preparation rather than premature technology selection. For SMEs, its recommendations were translated into activities such as identifying critical systems, documenting vendor dependencies, estimating whether systems can be upgraded or must be replaced, and aligning migration with existing technology-refresh plans. The World Economic Forum's *Transitioning to a Quantum-Secure Economy* [12] offers an ecosystem and cross-sector perspective. It considers PQC migration as a collective economic and governance challenge involving governments, industry leaders, technology providers, regulators, and supply chains. Its impact was particularly visible in the framework's treatment of leadership awareness, stakeholder coordination, vendor engagement, policy alignment, workforce readiness, and communication. It also reinforced that delayed action by major vendors or infrastructure providers can constrain the migration readiness of dependent organisations. For SMEs, this supported the recommendation to monitor major providers, participate in industry forums, rely on trusted advisory ecosystems, and treat vendor readiness as a central migration factor. Canadian National Quantum-Readiness [13] contributed a Canadian ecosystem perspective by

identifying relevant institutions, market actors, emerging technologies, and readiness considerations within the national quantum environment. Its impact was to contextualise the framework within Canada's evolving quantum-technology ecosystem and to reinforce the importance of external support networks, industry associations, government initiatives, specialist service providers, and national policy developments. For SMEs, these supported actions relate to awareness, access to external expertise, participation in Canadian technology networks, and monitoring of local policy and market signals.

Collectively, the practitioner publications [8–13] provided the strongest operational bridge between standards and organisational implementation. The private-sector documents contributed detailed guidance on certificates, cryptographic management, technical architecture, risk sequencing, and product transition. The government and consortium documents contributed ecosystem coordination, public-policy alignment, readiness planning, external support, and stakeholder engagement. Their combined influence was particularly important in translating high-level roadmap requirements into concrete actions that SMEs and enterprises could implement.

2.4 Academic Studies: Adoption, Migration Design, and Organisational Constraints

Academic studies provide conceptual, empirical, and methodological explanations of why technology standards are adopted unevenly and why migration programmes succeed or fail. The initial corpus contained 20 documents classified as academic or research literature, covering PQC migration, cryptographic readiness, standards adoption, innovation management, organisational performance, information sharing, and technical transition challenges. Following the structured screening process, four of these documents were selected for detailed practical-insight extraction [14–17], while additional research literature was used to inform the insight extraction process, the interpretation and discussion of the results [18–25].

The four research-oriented documents that were selected for detailed analysis are: (a) the Canadian Centre for Cyber Security's Preparing Your Organization for the Quantum Threat to Cryptography [14]; (b) Joseph et al.'s Transitioning Organisations to Post-Quantum Cryptography [15]; (c) Von Nethen et al.'s PMMP-PQC Migration Management Process [16]; and (d) INSECM's Preparing for Post-Quantum Cryptography: Impacts on the Classical Cybersecurity Operations of SMEs [17].

The Canadian Centre for Cyber Security [14] suggests a readiness-oriented perspective focused on inventory, risk exposure, planning, and organisational preparation. Its impact was especially visible in the Assess phase, where the framework requires organisations to identify cryptographic dependencies, evaluate the lifespan of sensitive information, and determine which systems require priority attention. It reinforced the principle that migration planning should begin before quantum-vulnerable systems become immediately obsolete. Joseph et al. [15] adopted a broad organisational migration perspective covering cryptographic discovery, prioritisation, crypto-agility, experimentation, hybrid approaches, and the interaction between technical and organisational change. Its impact extended across all four phases. It supported the interpretation of PQC migration as an organisational transformation requiring governance, architecture, vendor engagement, testing, and continuing adaptation rather than a one-time technical substitution. Von Nethen et al. [16] shaped a process-oriented approach to organising migration activities. Its influence was reflected in the framework's phased structure, explicit assignment of activities, migration planning, sequencing, monitoring, and integration with organisational management processes. It helped support the treatment of migration as a managed lifecycle with feedback between implementation, assessment, and governance. The INSECM publication [17] was especially important because it directly addressed smaller organisations. It contributed evidence concerning SME resource constraints, limited specialist capacity, dependence on existing cybersecurity operations, and the practical difficulty of adding PQC migration to already constrained security functions. Its impact was central to the development of the SME-executable pathway. In addition, it supported the use of lightweight governance, scoped inventories, vendor-dependent implementation, external expertise, managed services, and migration activities integrated into existing IT and cybersecurity processes.

The additional academic studies supported the interpretation of standards adoption, organisational readiness, innovation implementation and information-sharing challenges [18–25]. Collectively, the academic studies indicate that the publication of technical standards does not automatically lead to organisational adoption. Migration depends on perceived risk, governance, leadership support, available skills, financial and technical resources, vendor readiness, interoperability, organisational routines, regulatory pressure, and the ability to convert technical requirements into operational decisions. The academic literature insights have also informed the formulation of the research methodology. Studies on LLM-assisted

information extraction supported the use of a structured model-assisted process for identifying and organising insights from unstructured documents. However, the LLM was treated as an analytical support tool rather than as an evidentiary authority. The extraction schema was defined in advance, outputs were linked to source evidence, and final interpretation, consolidation, prioritisation, and framework design remained under researcher control [26, 27].

2.5 Synthesis of the Four Types of Sources

The four types of sources played complementary roles in the development of the framework. Roadmaps established the strategic transition logic and life-cycle sequencing. Standards defined the approved cryptographic destination. Practitioner publications converted strategic and technical requirements into operational guidance. Academic studies explained organisational adoption, resource constraints, migration barriers, and implementation-management requirements.

The final framework, therefore, did not originate from any single roadmap, standard document, practitioner publication, or academic study. It emerged from the integration of the four different types of textual evidence. This integration enabled the study to preserve the common migration requirements applicable to all organisations while distinguishing between a resource-conscious SME pathway and larger enterprise-focused extensions involving formal governance, automated discovery, internal cryptographic engineering, laboratory testing, and extensive assurance reporting.

3 Research Method

The research design followed a six-step analytical workflow: corpus construction, document-level screening, document selection, practical insight extraction, insight prioritisation, and framework synthesis (Figure 1). The process was designed to be rigorous enough from an academic point of view and practical enough to produce implementable guidance for SMEs and larger business enterprises.

3.1 Corpus Construction and Source Composition

The initial corpus comprised 52 documents: four roadmaps, three standards, 25 practitioner publications, and 20 academic or research-literature

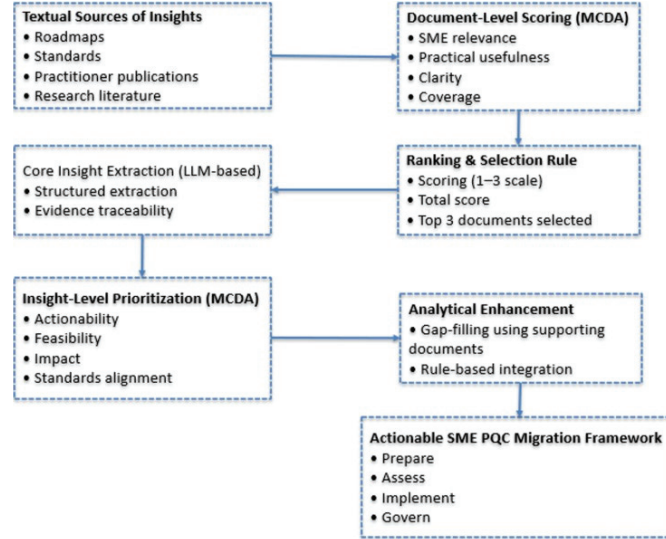


Figure 1 Analytics methodology for translating PQC guidance into an SME migration framework.

documents (Table 3). These documents were systematically screened and evaluated, after which 17 high-value sources were selected for detailed practical-insight extraction. The selected sources are presented in Table 2 and included in the reference list. Documents were included when they addressed at least one of the following: PQC transition planning; cryptographic standards or inventory; crypto-agility; quantum-risk assessment; vendor or ecosystem readiness; organisational adoption; migration governance; testing; or SME operational constraints. Duplicate versions, promotional pages without substantive guidance, and sources lacking sufficient migration content were excluded. This design was intentional: roadmaps supplied strategic sequencing, standards supplied normative baselines, practitioner publications supplied operational guidance, and academic studies supplied adoption and organisational-readiness insights.

3.2 Document-level Multi-criteria Decision Analysis (MCDA) and Selection of the Final Subset of Documents

Each document was evaluated using four MCDA criteria on a three-point ordinal scale: SME relevance, practical usefulness, clarity, and coverage. A score of 1 indicated low contribution, 2 indicated moderate contribution,

Table 3 Composition of the initial corpus of PQC documents

Source Category	Number of Documents	Primary Role in the Study	Interpretive Value
Roadmaps	4	Strategic direction and lifecycle sequencing	Clarified what must be planned and when.
Standards	3	Technical and normative baselines	Anchored the framework in recognised PQC transition requirements.
Practitioner documents	25	Operational guidance from government and private sources	Provided the strongest implementation-level detail for SMEs.
Academic studies	20	Adoption barriers, migration concepts, and methodological insight	Explained organisational constraints, readiness factors, and cross-document synthesis logic.
<i>Total</i>	52	Multi-source evidence-based	Balanced policy, technical, operational, and research evidence.

and 3 indicated high contribution, producing a maximum total of 12. The selection rule retained the top three private practitioner documents, the top three government or consortium practitioner documents, and the top four academic documents. All four roadmaps and all three standards were retained irrespective of score because they served as strategic and normative anchors. This category-balanced rule prevented high-scoring practitioner documents from crowding out standards and roadmaps and produced the 17-document extraction set listed in Table 2.

There is one key empirical pattern that emerged during the selection process: practitioner documents consistently provide strong implementation-level guidance, while roadmaps and standards provide structure, sequencing, and compliance anchors. This realisation matters because it shows that the path from standards to practice is mediated by operational guidance. In other words, SMEs need standards-aware actions, not standards alone.

3.3 Controlled Extraction and Human Validation

The 17 selected documents were processed through a structured extraction prompt designed before analysis. The prompt instructed the LLM to extract discrete, actionable migration insights rather than broad summaries. For every

insight, the schema captured the source document ID, lifecycle phase, migration theme, action statement, practical explanation, responsible role, evidence excerpt or source location, and confidence level. The initially defined phases were Prepare, Assess, Implement, and Govern, and the model was instructed not to infer actions unsupported by the data source. Human validation was organized at three levels. First, extraction-level validation checked whether each action was supported by the cited source and whether the assigned phase and theme were plausible. Second, consolidation-level validation identified semantic duplicates, separated compound actions, removed purely descriptive or excessively technical items, and merged equivalent statements while retaining source provenance. Third, framework-level validation assessed whether the resulting actions formed a coherent organisational lifecycle and whether an action was feasible for an SME, required enterprise capability, or could be expressed in both forms. Quality-control rules included no evidence-free actions, no algorithm recommendations beyond the standards, no treatment of vendor claims as normative requirements, no deletion of enterprise-level evidence merely because it exceeded typical SME capacity, and no automatic acceptance of model-generated classifications. Ambiguous records were resolved through source re-reading and researcher judgement [26, 27]

The validated extraction produced 556 insights. During consolidation, semantically equivalent statements were clustered while their source identifiers and evidence locations were retained. The consolidated actions were then prioritised using MCDA based on importance for PQC readiness and practicality in an SME context, with standards alignment and evidence breadth used as interpretive checks. This process yielded 73 actions: 16 Prepare, 20 Assess, 18 Implement, and 19 Govern. During framework synthesis, each action was expressed in an SME-executable form and, where supported by the evidence, an enterprise-focused extension. The model's role was therefore equivalent to assisted coding and normalisation; it accelerated identification and structuring but did not determine source credibility, final interpretation, prioritisation, or framework design.

4 Developing an Actionable SME-focused PQC Migration Framework

4.1 Textual Evidence-to-Action Pipeline

The full pipeline moved from 52 documents to 17 high-value sources, then to 556 evidence-linked insights, and finally to 73 prioritised actions (Figure 2).

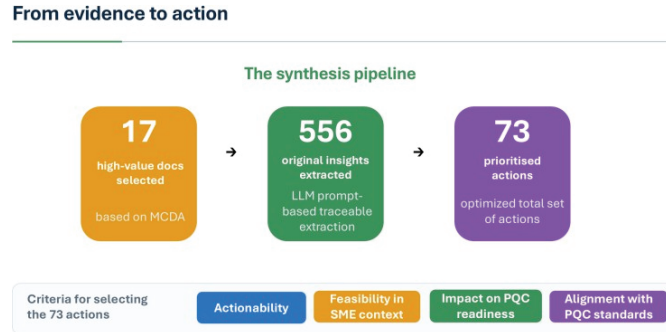


Figure 2 Transitioning from 17 high-value documents to 556 extracted insights and 73 prioritised actions.

Table 4 Distribution of extracted insights across migration phases

Phase	Extracted Insights	Share of 556	Dominant Activity Logic	Interpretation
Prepare	158	28.42%	Governance, strategy, resourcing, crypto-agility foundations	Readiness must be created before algorithm decisions become executable.
Assess	189	33.99%	Inventory, dependency mapping, CBOM, risk evaluation	Visibility and risk analysis are the analytical core of migration.
Implement	118	21.22%	Pilots, phased rollout, hybrid approaches, vendor coordination	Execution should be staged and system-dependent, not rip-and-replace.
Govern	91	16.37%	Monitoring, policy updates, compliance, reporting, capability building	PQC readiness becomes a continuous organisational capability.

This progression is important because it shows that the framework was not invented conceptually. It was derived through systematic filtering, extraction, consolidation, and prioritisation.

4.2 Distribution of the 556 Extracted Insights

The 556 extracted insights were distributed across the four migration phases, with Assess and Prepare accounting for the largest share (Table 4). Assess produced 189 insights (33.99%), Prepare produced 158 insights (28.42%),

Table 5 Distribution of the 73 prioritised actions

Phase	Number of Prioritised Actions	Share of 73	Meaning
Prepare	16	22%	Establish ownership, governance, scope, strategy, and organisational readiness.
Assess	20	27%	Build cryptographic visibility, map dependencies, evaluate risk, and define priorities.
Implement	18	25%	Execute pilots, vendor-aligned migration waves, testing, and system transition.
Govern	19	26%	Maintain policies, standards tracking, reporting, incident readiness, and continuous capability.
Total	73	100%	A balanced lifecycle action set for SME PQC migration.

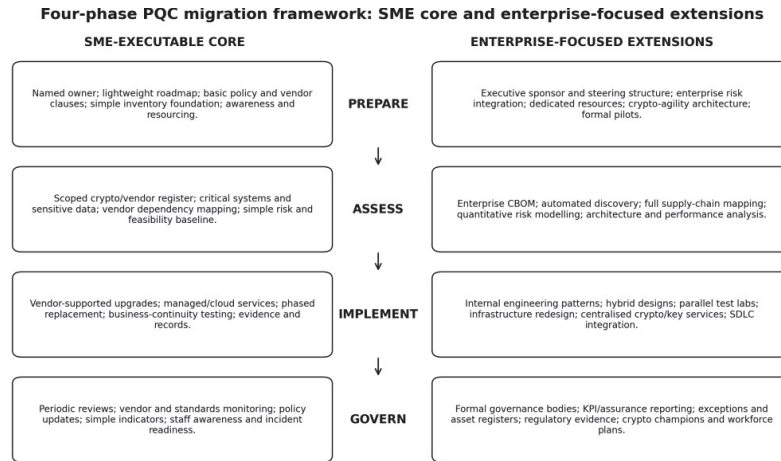
Implement produced 118 insights (21.22%), and Govern produced 91 insights (16.37%). This distribution indicates that PQC migration is heavily front-loaded around readiness, discovery, and risk analysis. SMEs cannot migrate what they cannot see, prioritise, or govern.

4.3 Transforming 556 Insights into 73 Prioritised Actions

The extracted insights contained semantic overlap across documents. Similar actions appeared in different languages across government roadmaps, vendor guidance, standards, and academic sources. The consolidation stage merged duplicates, removed weak items, and clustered the remaining material into recurring organisational themes such as governance, inventory management, cryptographic bill of materials development (CBOM), risk management, vendor coordination, testing, crypto-agility, and continuous monitoring. The prioritisation stage then evaluated the consolidated actions using actionability, SME feasibility, impact on PQC readiness, and alignment with standards. The final 73 actions represent a minimum viable but sufficient action set (Table 5): broad enough to cover the migration lifecycle but narrow enough to be usable by SMEs and advisors.

4.4 The SME PQC Migration Framework

The final framework organises PQC migration into four phases (Figure 3). The framework is iterative rather than strictly linear: learning from the Govern phase feeds back into Prepare and Assess; implementation outcomes update inventories and risk decisions; and new standards, vendor updates and incident lessons reshape priorities over time.



Common lifecycle; different governance depth, discovery scale, engineering capability, and assurance burden.

Figure 3 Four-phase PQC migration framework: SME-executable core and enterprise-focused extensions.

4.5 Distinguishing Between SME and Larger Enterprise Pathways in PQC Migration

Although PQC migration affects both SMEs and large enterprises, the organisational conditions under which each group must act are substantially different. The evidence analysed in this study showed that most existing PQC guidance is written with enterprise-level assumptions: dedicated cybersecurity teams, mature governance structures, formal risk management processes, asset visibility, procurement capacity, and budget flexibility. These assumptions do not always hold for SMEs. The enterprise pathway is typically characterised by formal programme ownership, enterprise-wide cryptographic inventory, structured vendor management, internal security architecture teams, and the ability to run parallel pilots, testing environments, and phased deployment programmes.

In contrast, the SME pathway requires a more constrained and practical approach. SMEs often depend heavily on external vendors, cloud platforms, managed service providers, and software suppliers. Their migration capacity is therefore shaped less by internal cryptographic engineering capability and more by visibility, prioritisation, vendor readiness, and practical sequencing.

The distinction made above became critically important in interpreting the results (Table 6). The same four migration phases – Prepare, Assess,

Table 6 Phase activities and enterprise-focused extensions

Phase	Activity Themes	SME-executable Pathway	Enterprise-focused Extensions
Prepare	Governance and leadership; strategy, roadmap, and risk management; policy and external engagement; crypto-agility and asset-management foundations; stakeholder alignment; resourcing; early experimentation.	Named owner or small leadership group; simple roadmap tied to business criticality and vendor renewal cycles; basic policy/procurement clauses; lightweight inventory foundation; reliance on trusted vendor pilots and managed services.	Formal steering committee and executive sponsorship; enterprise risk integration; dedicated programme resources; crypto-agility architecture across infrastructure and development; internal pilots and structured programme documentation.
Assess	CBOM management; cryptographic discovery and inventory; dependency mapping; quantum risk and data criticality; baselines; feasibility; effort and timeline estimation; standards review.	Scoped crypto/vendor register; identify critical systems, certificates, SaaS, cloud, backups, sensitive data, and renewal dates; ask vendors about roadmaps; simple low/medium/high risk and feasibility classifications.	Comprehensive CBOM with detailed attributes; automated discovery; enterprise and supply chain dependency mapping; quantitative risk modelling; architecture, performance, interoperability, and infrastructure analysis.
Implement	Engineering and remediation patterns; planning and sequencing; solution selection; infrastructure modernisation; pilots and validation; vendor execution; SDLC integration; legacy mitigation; QA; key management.	Vendor-supported, standards-aligned products; managed/cloud PQC capabilities; maintenance-window upgrades; business-continuity and userimpact testing; phased replacement; interim controls; evidence retention.	Internal remediation engineering; system-specific cutover and hybrid designs; parallel laboratory and proof-of-concept environments; architecture redesign; centralised cryptographic/key services; deep SDLC and automated compliance integration.
Govern	Governance roles; roadmap tracking; monitoring and reporting; control adaptation; standards horizon scanning; policy lifecycle; risk and regulatory alignment; vendor governance; training; collaboration; incident response; communications and trust.	Maintain readiness tracker; periodic reviews; monitor vendor and standards updates; refresh registers; update basic policies and contracts; simple indicators; targeted awareness; incident and continuity updates.	Formal governance bodies and crypto champions; KPI, assurance, audit, and regulatory evidence; exception and asset registers; product-level cryptographic governance; enterprise workforce plans; formal stakeholder and supervisory reporting.

Implement, and Govern – apply to both SMEs and enterprises, but the emphasis differs. For enterprises, the framework supports coordination across business units, infrastructure domains, compliance functions, and technical teams. For SMEs, the framework must first reduce complexity by identifying the minimum viable set of actions required to begin migration responsibly. In the Prepare phase, enterprises may establish formal PQC steering committees, enterprise risk registers, and multi-year migration programmes. SMEs, however, require lightweight governance: clear ownership, executive awareness, basic policy alignment, and a realistic roadmap tied to available resources. In the Assess phase, enterprises may conduct large-scale cryptographic discovery across applications, infrastructure, data repositories, and supply chains. SMEs are more likely to begin with a scoped inventory of critical systems, sensitive data, vendor-managed services, and high-risk dependencies. For SMEs, the key question is not only “where is cryptography used?” but also “which systems are controlled internally, and which depend on third parties?” In the Implement phase, enterprises may have the technical capacity to test PQC algorithms, redesign infrastructure, and coordinate hybrid cryptographic deployments internally. SMEs are more likely to implement PQC through vendor upgrades, managed services, cloud-provider roadmaps, procurement decisions, and phased replacement of vulnerable systems. In the Govern phase, enterprises may integrate PQC into formal compliance, audit, architecture, and security monitoring structures. SMEs require a simpler but continuous governance model: monitoring vendor updates, reviewing cryptographic dependencies periodically, updating policies, training staff, and ensuring that future technology purchases support crypto-agility.

The SME framework developed in this study should not be understood as a smaller version of an enterprise roadmap. It is an adapted migration pathway that translates enterprise-oriented PQC guidance into feasible, prioritised, and resource-aware actions for smaller organisations. The contribution of this study is precisely in making that translation explicit: moving from broad enterprise guidance to an SME-executable framework.

5 Phase Interpretation of the PQC Migration Framework

5.1 Prepare: Readiness Before Technology

The Prepare phase establishes the organisational foundation for migration. Its core activities include assigning ownership, creating a lightweight

governance structure, defining scope, securing executive sponsorship, developing a roadmap, setting risk appetite, identifying resource needs, and building crypto-agility awareness. The results show that SMEs should not begin by asking which PQC algorithm to deploy first. The more appropriate starting point is determining who owns the transition, what business risks matter most, and how the organisation will make migration decisions with limited capacity. For SMEs, this phase converts PQC from an abstract future threat into a manageable programme. It can be executed through a small cross-functional working group involving management, IT, security, procurement, legal or compliance, and key vendor-facing roles. The emphasis should be on clarity of responsibility, practical scope, and realistic sequencing. [4, 5, 9, 12, 14–16]

5.2 Assess: Visibility and Risk Management as the Analytical Core

The Assess phase produced the largest number of extracted insights, indicating that visibility is central to PQC readiness. The main activities include cryptographic inventory, certificate and key discovery, CBOM development, application and protocol mapping, third-party dependency mapping, data sensitivity assessment, confidentiality-lifespan analysis, and migration feasibility assessment [4, 5, 8, 9, 11, 14, 15, 21]. The practical implication is straightforward: without inventory and dependency visibility, migration prioritisation becomes guesswork. SMEs must understand where cryptography is used, what it protects, which systems depend on it, which vendors control it, and which assets face higher long-term confidentiality risk. This phase turns general quantum risk into a set of concrete migration decisions. [4–12, 15, 16, 21].

5.3 Implement: Phased, Hybrid, and Vendor-aware Execution

The Implement phase covers the execution of prioritised migration activities. The results reject a simple rip-and-replace model. Many SMEs will need phased implementation, pilot testing, hybrid cryptography, infrastructure updates, application changes, vendor coordination, interoperability testing, and exception handling for legacy systems or unavailable source code.

This phase should be sequenced by business criticality, exposure, feasibility, vendor readiness, and asset lifecycle. Low-risk pilots can generate learning before the organisation attempts more complex changes. Hybrid approaches may reduce transition risk where immediate full migration is

impractical. Vendor coordination is not an optional activity; for many SMEs, external providers will determine the timing and feasibility of migration [4–7, 9, 12, 15, 16].

5.4 Govern: Continuous Adaptation and Capability Building

The Govern phase transforms PQC migration into an ongoing organisational capability. Its activities include standards monitoring, policy updates, KPI reporting, periodic inventory refresh, vendor assurance, contract updates, compliance alignment, incident-response adaptation, workforce awareness, and continuous improvement. Although Govern is the smallest phase in the original extracted dataset, it becomes strongly represented in the prioritised actions. This shift suggests that governance may be underemphasised in raw guidance but becomes essential when actions are evaluated for practical SME readiness. PQC migration does not end after deployment; it must be maintained as standards, vendor capabilities, and threat assumptions evolve.

6 Discussion

The findings lead to five major observations. First, PQC migration is an organisational transformation, not merely a cryptographic substitution [4, 5, 9, 12, 15, 16, 21]. The work involves decision-ownership, governance, risk trade-offs, vendor coordination, reporting, and change management. Second, discovery and risk assessment drive the transition: inventory, dependency mapping, CBOMs, and data-criticality analysis are prerequisites for intelligent sequencing [4, 5, 8, 9, 11, 14, 15, 21]. Third, vendor and ecosystem dependence is central. SMEs rarely control all cryptographic layers in their environments; cloud services, software vendors, certificate authorities, managed service providers, and sector-specific platforms shape the migration path [5, 8–13, 17]. Fourth, implementation must be phased and adaptive. The evidence supports pilots, hybrid approaches, testing, lifecycle sequencing, and legacy-system planning rather than one-time replacement [4–12, 15, 16, 21]. Fifth, governance converts migration into a durable capability. PQC readiness must be monitored, measured, updated, and communicated over time [4–7, 9, 12, 15, 16]. The most important implication is that SMEs need a readiness model before they need a deployment checklist. A deployment checklist assumes that assets, dependencies, priorities, and owners are known. The evidence shows that those assumptions are often false. The

framework, therefore, begins with preparation and assessment, then moves into implementation and governance.

The framework can be projected into seven explicit recommendations for SME leaders, IT managers, advisors, and service providers:

- Assign a named owner for PQC readiness, even if the role is part-time or shared across IT, security, and operations [4, 5, 9, 12, 15, 16].
- Create a lightweight PQC roadmap that identifies scope, risk appetite, business priorities, resource constraints, and initial milestones [4, 8, 9, 11, 14, 15].
- Build cryptographic visibility first through certificate discovery, cryptographic inventory, CBOM development, and third-party dependency mapping [4, 7, 10, 11, 14, 15].
- Prioritise assets based on data sensitivity, confidentiality lifespan, business criticality, exposure, vendor dependency, and migration feasibility [5, 8–12].
- Engage vendors early and request their PQC readiness plans, timelines, supported algorithms, hybrid options, testing guidance, and contractual assurances [4–7, 9–12, 15, 16].
- Start implementation with controlled pilots and phased transition waves rather than attempting full-system replacement [4–7, 9, 12, 15, 16].
- Govern continuously through updated policies, inventory refresh, standards monitoring, KPI reporting, training, and incident-response alignment.

For cybersecurity advisors and management service providers, the framework provides a defensible structure for SME-focused advisory engagements. It can support readiness assessments, client workshops, executive reporting, procurement reviews, and migration roadmap design. The 73-action structure also creates a foundation for scorecards, dashboards, and maturity models [4, 5, 8–17]. For vendors, the findings emphasise the importance of transparent roadmaps, cryptographic posture visibility, hybrid deployment support, and clear communication with SME customers. Vendor readiness can either accelerate or block SME migration. Suppliers that provide practical transition guidance may become trusted partners in the quantum-safe transition [5, 8–13, 17]. For policymakers and industry associations, the study demonstrates that publishing high-level guidance is not enough. SMEs need simplified, contextualised, and operationally sequenced guidance. Sector-specific playbooks, funding supports, procurement templates, awareness campaigns, and shared CBOM practices could reduce the implementation gap [4–7, 12–17].

7 Limitations and Suggestions for Future Research

The present research study has several limitations. First, it relies on documentary evidence and structured extraction rather than direct field implementation across multiple SMEs. Second, the corpus reflects available roadmaps, standards, practitioner documents, and academic sources at the time of analysis; PQC guidance however will continue to evolve. Third, while the LLM-assisted method improves scale and consistency, extracted insights still depend on schema design, prompt control, and researcher validation. Future research should focus on testing and refining the framework in live SME settings, compare readiness patterns across industries, validate the 73 actions with cybersecurity practitioners, and develop quantitative maturity scoring instruments. Additional work could also examine how CBOM adoption, vendor assurance, and procurement language affect SME PQC readiness. A dashboard-based implementation of the framework would further support reporting, prioritisation, and continuous monitoring.

8 Conclusion

PQC migration has entered the organisational execution phase. SMEs need more than awareness of quantum risk; they need a practical way to translate standards, roadmaps, and expert guidance into sequenced, evidence-based action. This paper presents an SME PQC migration framework derived from a structured evidence pipeline that began with 52 documents, selected 17 high-value sources, extracted 556 migration insights, and consolidated them into 73 prioritised actions. The suggested Prepare-Assess-Implement-Govern framework shows that quantum-safe migration depends on governance, visibility, risk-based prioritisation, vendor coordination, phased execution, and continuous capability development. The central conclusion is clear: PQC migration is not only a cybersecurity upgrade. It is a challenge for business, governance, reporting, and ecosystem-coordination. SMEs that begin with readiness, visibility, and evidence-based sequencing will be better positioned to manage the quantum-safe transition.

References

- [1] National Institute of Standards and Technology, FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard, Federal Information Processing Standards Publication 203, U.S. Department of Commerce, 2024. DOI: <https://doi.org/10.6028/NIST.FIPS.203>.

- [2] National Institute of Standards and Technology, FIPS 204: Module-Lattice-Based Digital Signature Standard, Federal Information Processing Standards Publication 204, U.S. Department of Commerce, 2024. DOI: <https://doi.org/10.6028/NIST.FIPS.204>.
- [3] National Institute of Standards and Technology, FIPS 205: Stateless Hash-Based Digital Signature Standard, Federal Information Processing Standards Publication 205, U.S. Department of Commerce, 2024. DOI: <https://doi.org/10.6028/NIST.FIPS.205>.
- [4] Canadian Centre for Cyber Security, Roadmap for the Migration to Post-Quantum Cryptography for the Government of Canada (ITSM.40.001), Communications Security Establishment Canada, June 2025. [Online]. Available: <https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001>.
- [5] Post-Quantum Cryptography Coalition, Post-Quantum Cryptography Migration Roadmap, May 2025. [Online]. Available: <https://pqcc.org/wp-content/uploads/2025/05/PQC-Migration-Roadmap-PQCC-2.pdf>.
- [6] NIS Cooperation Group, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, European Commission, June 2025. [Online]. Available: https://securitydelta.nl/media/com_hsd/report/750/document/Roadmap-on-postquantum-cryptography-PzBJxNUYyeuEdVUacWL696DofZQ-117507.pdf.
- [7] Australian Signals Directorate, Australian Cyber Security Centre, Planning for Post-Quantum Cryptography, September 2025. Available: <https://www.cyber.gov.au/sites/default/files/2025-09/Planning%20for%20post-quantum%20cryptography%20%28September%202025%29.pdf>.
- [8] DigiCert, The Ultimate Guide to Post-Quantum Cryptography, DigiCert. [Online]. Available: <https://www.digicert.com/content/dam/digicert/pdfs/guide/ultimate-guide-to-pqc.pdf>.
- [9] NCS and IBM, Managing Risks and Opportunities for Quantum-Safe Development: IBM-NCS Quantum Security, Version 1.0, 2024. [Online]. Available: https://www.ncs.co/dam/jcr:81bb243e-0cdd-4c04-92e2-d110c01fa0e8/IBM_NCS_Quantum_Security_v1.0.pdf.
- [10] Cryptomathic, A Banker's Guide to Quantum-Safe Cryptography, Part 3: Roadmap to PQC Migration for Financial Institutions. [Online]. Available: <https://www.cryptomathic.com/a-bankers-guide-to-quantum-safe-cryptography-part-3-roadmap-to-pqc-migration-for-financial-institutions-cryptomathic>.
- [11] AIVD, CWI, and TNO, The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography, 2nd ed., December 2024.

- [Online]. Available: <https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf>.
- [12] World Economic Forum, Transitioning to a Quantum-Secure Economy, September 2022. [Online]. Available: <https://www.weforum.org/publications/transitioning-to-a-quantum-secure-economy/>.
- [13] Canadian Forum for Digital Infrastructure Resilience, Canadian National Quantum-Readiness: Best Practices and Guidelines, July 7, 2021. [Online]. Available: <https://quantum-safe.ca/wp-content/uploads/2022/01/CFDIR-Prati-Tech-Quant-EN.pdf>.
- [14] Canadian Centre for Cyber Security, Preparing Your Organization for the Quantum Threat to Cryptography (ITSAP.00.017), February 2025. [Online]. Available: <https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017>.
- [15] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, “Transitioning organisations to post-quantum cryptography,” *Nature*, vol. 605, no. 7909, pp. 237–243, 2022. [https://info.quintessencelabs.com/hubfs/2022-05-11_Nature_Transitioning%20organizations%20to%20post-quantum%20cryptography%20\(1\).pdf](https://info.quintessencelabs.com/hubfs/2022-05-11_Nature_Transitioning%20organizations%20to%20post-quantum%20cryptography%20(1).pdf).
- [16] N. von Nethen, A. Wiesmaier, N. Alnahawi, and J. Henrich, “PMMP-PQC Migration Management Process,” in *Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference*, pp. 144–154, 2024. <https://arxiv.org/pdf/2301.04491>.
- [17] INSECM, “Preparing for Post-Quantum Cryptography: Impacts on the Classical Cybersecurity Operations of SMEs,” April 3, 2025. [Online]. Available: <https://insecm.ca/en/newsletter/preparing-for-post-quantum-cryptography-pqc-impacts-on-the-classical-cybersecurity-operations-of-smes/>.
- [18] I. Kong, M. Janssen, and N. Bharosa, “Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions,” *Government Information Quarterly*, vol. 41, no. 1, article 101884, 2024. DOI: <https://doi.org/10.1016/j.giq.2023.101884>.
- [19] K. C. Dekkaki, I. Tasic, and M. Cano, “Exploring post-quantum cryptography: A review and directions for the transition process,” *Technologies*, vol. 12, no. 12, article 241, 2024. DOI: <https://doi.org/10.3390/technologies12120241>.
- [20] D. Chawla and P. S. Mehra, “A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges,

- opportunities and solutions,” *Internet of Things*, vol. 24, article 100950, 2023. DOI: <https://doi.org/10.1016/j.iot.2023.100950>.
- [21] D. Ott, D. Moreau, and M. Gaur, “Planning for cryptographic readiness in an era of quantum computing advancement,” in *Proceedings of the International Conference on Information Systems Security and Privacy*, pp. 491–498, 2022. <https://www.scitepress.org/PublishedPapers/2022/108860/pdf/index.html>.
- [22] S. A. Käppler and B. Schneider, “Post-Quantum Cryptography: An Introductory Overview and Implementation Challenges of Quantum-Resistant Algorithms,” in *Proceedings of the Society 5.0 Conference 2022-Integrating Digital World and Real World to Resolve Challenges in Business and Society*, EPiC Series in Computing, vol. 84, pp. 61–71, 2022. Available: <https://irf.fhnw.ch/server/api/core/bitstreams/37e2bb44-2600-4e6a-bfe6-0571089b7253/content>.
- [23] N. Abdelkafi, R. Bekkers, R. Bolla, A. Rodriguez-Ascaso, and M. Wetterwald, *Understanding ICT Standardisation: Principles and Practice*, European Telecommunications Standards Institute, 2021. [Online]. Available: <https://acrobat.adobe.com/id/urn:aaid:sc:EU:ea05cb13-45ab-4f40-80cc-e82a263817ff>.
- [24] M.-C. Idris and A. Durmuşoğlu, “Innovation management systems and standards: A systematic literature review and guidance for future research,” *Sustainability*, vol. 13, no. 15, article 8151, 2021. DOI: <https://doi.org/10.3390/su13158151>.
- [25] G. van de Kaa, “Standards adoption: A comprehensive multidisciplinary review,” *Heliyon*, vol. 9, no. 8, article e19203, 2023. DOI: <https://doi.org/10.1016/j.heliyon.2023.e19203>.
- [26] N. Schwitter, “Using large language models for preprocessing and information extraction from unstructured text: A proof-of-concept application in the social sciences,” *Methodological Innovations*, vol. 18, no. 1, pp. 61–65, 2025. DOI: <https://doi.org/10.1177/20597991251313876>.
- [27] D. Xu, W. Chen, W. Peng, C. Zhang, T. Xu, X. Zhao, X. Wu, Y. Zheng, Y. Wang, and E. Chen, “Large language models for generative information extraction: A survey,” *Frontiers of Computer Science*, vol. 18, article 186357, 2024. DOI: <https://doi.org/10.1007/s11704-024-40555-y>.

Biographies

Babatunde Oladoja is a Master of Applied Business Analytics graduate of the Technology Innovation Management (TIM) program, Sprott School of Business, Carleton University, Ottawa, ON, Canada. His research focuses on post-quantum cryptography migration readiness, particularly and how small and medium-sized enterprises can prepare for the transition to quantum-safe cybersecurity. The present article is based on Babatunde's final research project within the TIM program, focusing on developing an SME-focused migration framework supported by evidence from technical, policy, and research literature. The key results of his research were presented at the ETSI/IQC Quantum Safe Cryptography Conference, June 16–18, 2026, in Ottawa, Canada. Babatunde has a multidisciplinary background in business analytics, technology management, process improvement, operational reporting, and data visualisation. His professional interests focus on addressing complex cybersecurity and innovation challenges for SMEs and larger organisations.

Stoyan Tanev, PhD, MSc, MEng, MA, is Associate Professor in the TIM program. Dr Tanev has a multidisciplinary educational background, including a PhD in Physics (1995, University Pierre and Marie Curie, Paris, France), MEng in Technology Management (2005, Carleton University, Ottawa, Canada), and a PhD in Theology (2012, Sofia University, Bulgaria). Stoyan joined the TIM program as an Assistant Professor in 2006. Between 2009 and 2017, he was an Associate Professor in the Department of Technology and Innovation at the University of Southern Denmark. In 2017, Stoyan Tanev returned to Carleton University and the TIM program, joining the Sprott School of Business. His broader research and teaching interests focus on quantum technology adoption, digital transformation and entrepreneurship, design thinking and Ai-enabled competitive business intelligence. Stoyan's main current focus is on the adoption and entrepreneurial opportunities associated with emerging quantum technologies. Weblink: <https://sprott.carleton.ca/cu-people/stoyan-tanev-2/>.

