Estimating Migration Timelines for Enterprises Transitioning to Post-Quantum Cryptography: A Real-World Analysis of Dependencies and Interconnectedness

Robert Campbell *

Posted Date: 24 November 2025

doi: 10.20944/preprints202511.1764.v1

Keywords: post-quantum cryptography; quantum computing; cryptographic migration; Zero Trust architecture; crypto-agility; enterprise security; NIST standards; ML-KEM; ML-DSA

 doi:10.20944/preprints202511.1764.v1

Article

Estimating Migration Timelines for Enterprises Transitioning to Post-Quantum Cryptography: A Real-World Analysis of Dependencies and Interconnectedness

Robert Campbell

Independent Researcher, Upper Marlboro, MD 20774, USA; rc@medcybersecurity.com

Abstract

The emergence of quantum computing threatens the security of classical cryptographic algorithms such as RSA and ECC. Post-quantum cryptography (PQC) offers mathematically secure alternatives, but migration is a complex, multi-year undertaking. Unlike past transitions (AES, SHA-2, TLS 1.3), PQC migration requires larger parameter sizes, hybrid cryptographic schemes, and unprecedented ecosystem coordination. This paper estimates migration timelines for small, medium, and large enterprises, considering infrastructure upgrades, personnel availability, budget constraints, planning quality, and inter-enterprise synchronization. We argue that realistic timelines extend well beyond initial optimistic estimates: 5–7 years for small enterprises, 8–12 years for medium enterprises, and 12–15+ years for large enterprises. PQC migration is not a siloed technical upgrade but a global synchronization exercise, deeply intertwined with Zero Trust Architecture and long-term crypto-agility. These timelines are contextualized against expected arrival windows for fault-tolerant quantum computers (FTQC), projected between 2028 and 2033 [1–3]. We further analyze the "Store Now, Decrypt Later" threat model, crypto-agility frameworks, and provide comprehensive risk mitigation strategies for enterprises navigating this unprecedented cryptographic transition.

Keywords: post-quantum cryptography; quantum computing; cryptographic migration; Zero Trust architecture; crypto-agility; enterprise security; NIST standards; ML-KEM; ML-DSA

1. Introduction

Quantum computing poses a fundamental and existential threat to classical cryptography that underpins modern digital communications, financial systems, critical infrastructure, and national security. Algorithms such as RSA and elliptic curve cryptography (ECC) are vulnerable to Shor's algorithm once fault-tolerant quantum computers (FTQC) become available [4]. Migration is not merely a technical upgrade but a systemic transformation requiring coordination across enterprises, vendors, regulators, and communication partners spanning multiple jurisdictions and regulatory frameworks.

Unlike past migrations, PQC introduces larger parameter sizes, hybrid cryptographic requirements, and ecosystem-wide dependencies that fundamentally change the operational characteristics of cryptographic systems [5]. Certificate sizes may increase by factors of 5–10×, impacting bandwidth-constrained networks, embedded systems, and high-frequency trading platforms. Signature generation and verification times increase substantially, affecting real-time systems and time-critical applications. Hardware security modules (HSMs), smart cards, and cryptographic accelerators require firmware updates or complete replacement to support lattice-based and hash-based algorithms with different computational profiles than classical schemes.

This paper explores realistic migration timelines for enterprises of varying sizes, grounded in the interconnectedness of modern IT environments and the urgency imposed by FTQC arrival

 doi:10.20944/preprints202511.1764.v1

projections [1,3]. We examine the multi-dimensional challenge space, including technical debt in legacy systems, organizational change management, supply chain coordination, regulatory compliance timelines, and the "Store Now, Decrypt Later" (SNDL) threat model that makes immediate action imperative despite FTQC being years away.

1.1. The Store Now, Decrypt Later Threat

A critical dimension often underestimated in PQC migration planning is the Store Now, Decrypt Later (SNDL) attack vector. Adversaries with sufficient storage capacity and strategic motivation are actively harvesting encrypted communications today with the intent to decrypt them once FTQC becomes available [3]. This represents a binary risk event: once a cryptographically relevant quantum computer exists, all intercepted historical traffic becomes readable. Unlike gradual vulnerabilities, this is a discrete phase transition in threat capability that fundamentally alters the risk calculus for organizations handling sensitive data with long confidentiality requirements.

Data with confidentiality requirements extending beyond 2030 is already at risk. This includes classified national security information, long-term medical research data, financial instruments with extended maturity dates, intellectual property with multi-decade commercial value, and personal identifiable information (PII) subject to privacy regulations like GDPR or CCPA. Organizations must assess their data inventory against SNDL threat timelines and prioritize the migration of systems handling long-shelf-life sensitive data.

The SNDL threat creates an asymmetric advantage for adversaries: they can be patient, investing in harvesting operations today with minimal risk of detection, while defenders must execute complex, costly migrations under resource constraints and coordination challenges. This asymmetry drives the urgency for accelerated PQC adoption even in the absence of near-term FTQC availability [3].

1.2. Quantum Computing Timeline Projections

Recent developments in quantum computing have substantially accelerated timeline projections for cryptographically relevant quantum computers (CRQC). *Note: In this paper, CRQC (Cryptographically Relevant Quantum Computer) and FTQC (Fault-Tolerant Quantum Computer) are used interchangeably to denote quantum computers capable of breaking RSA/ECC encryption.* While early estimates suggested FTQC arrival in the 2035–2040 timeframe, more aggressive recent projections place CRQC capability as early as 2028–2030 [1,15,18]. This acceleration stems from rapid progress in quantum error correction, increases in qubit coherence times, advances in qubit connectivity architectures, and substantial increases in public and private sector investment in quantum computing research and development.

IBM's quantum computing roadmap projects systems with over 4,000 qubits by 2025 and expects fault-tolerant systems capable of executing Shor's algorithm against RSA-2048 within the current decade [2]. IonQ has published roadmaps suggesting cryptographically relevant trapped-ion quantum computers by 2028 [18]. While these timelines remain subject to technical uncertainties, the prudent security posture assumes the more aggressive timelines for risk management purposes.

The convergence of accelerated FTQC timelines with lengthy migration timelines creates a critical security gap. If large enterprises require 12–15 years for complete PQC migration, and FTQC arrives in 2028–2030, enterprises beginning migration in 2025 face a 3–5-year window where significant portions of their infrastructure remain vulnerable to quantum attacks. This gap constitutes a quantifiable risk deficit: the temporal span where mission-critical infrastructure remains vulnerable exceeds the security margin provided by current deployment velocity. For data with confidentiality requirements beyond 2030, the migration timeline is effectively retroactive—such data requires protection today, not when migration completes. The SNDL threat makes this deficit immediate rather than theoretical.

 doi:10.20944/preprints202511.1764.v1

2. Background and Related Work

2.1. Post-Quantum Cryptography Standards

NIST finalized three post-quantum cryptography standards in August 2024 following an eight-year standardization process involving international academic, industry, and government participation: FIPS 203 (ML-KEM, Module-Lattice-Based Key-Encapsulation Mechanism, derived from CRYSTALS-Kyber), FIPS 204 (ML-DSA, Module-Lattice-Based Digital Signature Algorithm, derived from CRYSTALS-Dilithium), and FIPS 205 (SLH-DSA, Stateless Hash-Based Digital Signature Algorithm, derived from SPHINCS+) [6].

ML-KEM (FIPS 203) provides key encapsulation for establishing shared secrets in key exchange protocols. It offers three security levels (ML-KEM-512, ML-KEM-768, ML-KEM-1024) corresponding to AES-128, AES-192, and AES-256 equivalent security. ML-KEM-768 is recommended for most applications, producing ciphertexts of approximately 1,088 bytes and public keys of 1,184 bytes, compared to 32 bytes for classical ECDH public keys. This 30–40× increase for key exchange materials creates a bandwidth tax that impacts network protocols, certificate repositories, and embedded systems with limited memory.

ML-DSA (FIPS 204) provides digital signatures for authentication and non-repudiation. Similarly, offering three security levels (ML-DSA-44, ML-DSA-65, ML-DSA-87), the recommended ML-DSA-65 produces signatures of approximately 3,309 bytes compared to 64 bytes for ECDSA P-256 signatures—a 50× increase. This dramatic expansion affects high-volume signing operations, blockchain systems, secure boot chains, and audit logging systems where signature storage accumulates over time. Second-order effects include database schema extensions: enterprise directory services (Active Directory, LDAP) with fixed-width certificate fields require schema migrations that can break downstream applications, and Certificate Revocation Lists (CRLs), bloating 50× can saturate WAN links during distribution.

SLH-DSA (FIPS 205) provides stateless hash-based signatures as a conservative fallback with stronger security assumptions than lattice-based schemes. However, SLH-DSA signatures range from 7,856 to 49,856 bytes depending on the parameter set, making them impractical for bandwidth-constrained applications. SLH-DSA serves primarily as a hedge against potential future cryptanalytic breakthroughs against lattice assumptions and finds application in high-security, low-frequency signing scenarios such as firmware signing and root certificate authorities.

These algorithms feature fundamentally different performance characteristics compared to classical cryptography. Lattice-based schemes exhibit fast encryption and key generation, but slower signature verification compared to RSA. Hash-based schemes provide conservative security assumptions, but at the cost of significantly larger signatures. These trade-offs impact on infrastructure design, requiring careful parameter selection based on application requirements [7].

2.2. Performance and Implementation Characteristics

Beyond parameter sizes, PQC algorithms exhibit different computational profiles that affect deployment strategies. ML-KEM demonstrates excellent performance on modern CPUs with AVX2 instruction sets, achieving key generation, encapsulation, and decapsulation operations in microseconds. However, embedded systems without vector instructions experience 10–100× performance degradation, necessitating hardware acceleration or protocol modifications to maintain acceptable latency.

ML-DSA signature generation scales linearly with security level, but verification requires sampling operations that introduce variable-time execution risks. Constant-time implementations add 20–40% overhead, which may be unacceptable for real-time systems. Side-channel protections against timing attacks, cache timing, and power analysis attacks add further complexity and performance cost to embedded implementations.

The stateless nature of SLH-DSA eliminates state management vulnerabilities present in earlier hash-based schemes like XMSS, but at the cost of substantially larger signatures. Organizations

 doi:10.20944/preprints202511.1764.v1

must evaluate whether the conservative security assumptions justify the 10–100× size increase over lattice-based signatures in their specific threat models.

2.3. Historical Cryptographic Migrations

Past migrations provide valuable lessons but also reveal why PQC migration presents unprecedented challenges:

AES adoption (∼5 years): The transition from DES/3DES to AES during 2001–2006 was relatively smooth, driven by clear performance advantages and security improvements. However, the cryptographic ecosystem was far less complex, with fewer devices, simpler protocols, and limited internet connectivity among embedded systems. AES adoption primarily affected server infrastructure and high-security applications rather than pervasive embedded devices [8].

SHA-1 deprecation (∼7 years): The transition from SHA-1 to SHA-2 (2010–2017) required coordinated browser vendor enforcement and certificate authority policy changes. Unlike algorithm upgrades, deprecation faces stronger resistance since it provides no immediate benefit to adopters while imposing costs. Browser vendors ultimately forced the transition by rejecting SHA-1 certificates, demonstrating the necessity of coordinated enforcement mechanisms [9].

TLS 1.3 rollout (∼3–5 years): Despite being a simpler protocol upgrade offering clear performance improvements (reduced handshake latency, forward secrecy by default, removed obsolete cryptographic options), TLS 1.3 deployment was slowed by middlebox incompatibility, particularly in enterprise networks with deep packet inspection systems. This illustrated how network infrastructure dependencies extend migration timelines even for well-designed backwards-compatible protocols [10].

Key differences for PQC migration: Compared to these precedents, PQC migration is substantially more complex due to: (1) larger parameters impacting bandwidth, storage, and processing across all layers; (2) hybrid requirements necessitating dual cryptographic operations during transition; (3) vastly more devices, applications, and networks than existed during earlier migrations; (4) deeper integration of cryptography into hardware (TPMs, HSMs, secure enclaves) requiring firmware or hardware replacement; (5) supply chain complexities with multi-tier vendor dependencies; and (6) regulatory compliance requirements across multiple jurisdictions with varying timelines [5,11].

The AES migration primarily affected the centralized server infrastructure. PQC migration affects everything from satellites with 15-year replacement cycles to vehicle telematics units with 10-year operational lifetimes to industrial control systems with 20–30 year deployed lifespans. This orders-of-magnitude increase in scope and heterogeneity fundamentally changes the migration challenge.

2.4. Dependencies Shaping PQC Migration

2.4.1. Infrastructure Upgrades

PKI and Certificate Infrastructure: Public Key Infrastructure repositories must scale to handle 5–10× larger certificates, impacting OCSP responders, CRL distribution, and certificate transparency logs. Certificate chains grow proportionally; a three-certificate chain with ML-DSA-65 signatures totals approximately 10 KB compared to ∼2 KB for classical ECDSA chains. High-volume certificate issuance systems require throughput scaling and storage expansion [7].

Hardware Security Modules face particularly acute challenges. Many deployed HSMs lack sufficient memory or processing power to support PQC algorithms efficiently. Firmware updates may be impossible for end-of-life models, requiring complete HSM replacement. Before deployment, vendors must achieve FIPS 140-3 certification—a process historically requiring 12–24 months. Furthermore, current HSMs optimized for RSA/ECC secure storage will experience 50× faster capacity consumption with PQC keys, potentially requiring enterprises to deploy 5–10× more HSM units to maintain equivalent key volume capacity. The combined procurement, certification, racking, and key ceremony rituals can consume 2–3 years of migration timelines. HSM replacement in high-availability environments requires parallel operation of old and new systems during cutover, effectively doubling infrastructure costs during transition [14].

 doi:10.20944/preprints202511.1764.v1

Network Protocol Impacts: TLS handshakes grow substantially with PQC, particularly when employing hybrid schemes combining classical and post-quantum algorithms for defense-in-depth. A hybrid TLS 1.3 handshake using X25519+ML-KEM-768 and ECDSA+ML-DSA-65 may exceed 15 KB compared to ∼4 KB for classical-only handshakes. This 4× increase creates prohibitive overhead in:

- **Bandwidth-constrained networks:** Satellite links, cellular networks in remote areas, and tactical military communications where larger handshakes fragment across multiple network packets, increasing vulnerability to packet loss and amplifying performance degradation in high-latency networks.
- **Packet fragmentation:** Fragmentation increases packet-loss vulnerability and introduces reassembly overhead that compounds latency in lossy environments.
- **Middlebox compatibility:** Enterprise firewalls, DPI systems, and load balancers with fixed buffer sizes will drop these fragments as anomalies, causing connection failures. Remediation requires network transport layer re-architecture, not merely software updates [13].

Testing network infrastructure for PQC compatibility requires comprehensive protocol analysis across diverse network conditions, which many enterprises lack the capacity to perform without external consulting support.

IoT and Embedded Devices: Internet of Things devices and embedded systems present the most severe migration challenges. Many IoT devices lack over-the-air firmware update capabilities, requiring physical access or field replacement. Devices embedded in critical infrastructure (smart grid meters, industrial sensors, medical implants) have 10–20-year operational lifespans that extend well beyond expected FTQC arrival [12].

Microcontrollers with limited RAM (32–64 KB) cannot accommodate PQC certificate chains and cryptographic operations simultaneously. Even with careful optimization, ML-KEM-768 requires approximately 15 KB of working memory, leaving insufficient space for application logic in resource-constrained devices. Organizations must choose between early device replacement, segmented network architectures isolating non-PQC devices, or accepting quantum vulnerability for legacy systems.

The sheer scale compounds the challenge: large enterprises may operate hundreds of thousands or millions of IoT devices across dispersed locations. A major manufacturer may have 50,000 industrial robots, a utility may deploy 10 million smart meters, and a logistics company may operate 100,000 telematics-equipped vehicles. Replacing these fleets on accelerated timelines requires massive capital expenditure and operational disruption [12].

2.4.2. Personnel and Expertise

Skilled personnel in PQC, PKI architecture, cryptographic engineering, and crypto-agility frameworks are scarce [14]. The cryptographic engineering community is relatively small, and few professionals have hands-on experience with lattice-based or hash-based cryptography beyond academic contexts. Enterprises must train cross-disciplinary teams spanning cryptographers, network engineers, application developers, security architects, and compliance officers to manage hybrid environments and navigate complex interoperability requirements.

Training and Skill Development: Effective PQC migration requires understanding not just the new algorithms, but their security properties, implementation pitfalls, side-channel vulnerabilities, and parameter selection trade-offs. Organizations must invest in:

- Algorithm-specific training for cryptographic engineers on lattice problems, rejection sampling, and side-channel countermeasures
- PKI modernization training for certificate authority operators on hybrid certificates and parameter negotiation
- Developer training on API changes and hybrid cryptographic libraries
- Security operations training on monitoring PQC implementations and detecting quantum-capable threats

 doi:10.20944/preprints202511.1764.v1

- Executive and management training on risk assessment and resource allocation for migration programs

Without adequate staffing, testing, and rollout coordination, personnel bottlenecks extend migration timelines by years. This creates a supply chain constraint on intellectual capital: vendors, enterprises, and government agencies compete simultaneously for the same limited pool of cryptographic engineering expertise. This consultant bottleneck means medium enterprises will queue for 'PQC-as-a-Service' product maturity, directly extending the 8–12-year timeline [14,15]. Organizations cannot simply hire their way out of the skills gap—the global shortage of qualified personnel means training existing staff and phased rollout paced by organizational absorption capacity are necessary constraints.

Organizational Change Management: PQC migration is not purely technical but requires organizational transformation. Governance structures must be established for crypto-agility decision-making. Risk management frameworks must be updated to assess quantum threats alongside traditional threat models. Compliance processes must incorporate PQC requirements as regulatory mandates emerge. Change management requires executive sponsorship, cross-functional working groups, and sustained funding over multi-year timelines [19].

2.4.3. Inter-Enterprise Coordination

Enterprises cannot migrate in isolation. Modern business operations depend on cryptographic interoperability with communication partners, SaaS vendors, cloud providers, financial networks, supply chain partners, and regulatory reporting systems [5,16]. This interdependence creates synchronization requirements that substantially extend timelines.

Vendor Ecosystem Dependencies: Organizations depend on software vendors, appliance manufacturers, and service providers to deliver PQC-capable products. Enterprise software procurement cycles typically span 12–24 months from initial RFP to production deployment, including vendor evaluation, pilot testing, contract negotiation, and staged rollout. If a critical vendor delivers PQC support 2–3 years after standardization, their customers' migrations are delayed by that amount, plus their internal procurement and deployment cycles [17].

Cloud service providers have announced PQC support timelines, but comprehensive availability across all services (compute, storage, database, networking, identity management, and key management) may take 3–5 years. Organizations with hybrid cloud architectures must coordinate migrations across multiple providers with different timelines and implementation approaches. Multi-cloud strategies amplify complexity, as each provider may prioritize different algorithm sets or parameter configurations [14].

Communication Partner Coordination: B2B communications often involve mutual authentication and encrypted channels, requiring both parties to support compatible cryptographic algorithms. Industries with complex supply chains (automotive, aerospace, pharmaceuticals) involve dozens or hundreds of partners that must coordinate upgrades. Without industry-wide coordination mechanisms, organizations face choices between maintaining legacy systems indefinitely, building dual-stack environments supporting both classical and PQC indefinitely, or accepting communication failures with non-PQC partners [16].

Financial networks present acute coordination challenges. Payment card networks, SWIFT, automated clearing houses, and securities trading systems require synchronized upgrades across thousands of participating institutions spanning multiple countries and regulatory jurisdictions. A single laggard institution can block other participants from fully retiring classical cryptography, forcing perpetual hybrid operation [5].

Hybrid Cryptography and Parameter Uniformity: Hybrid cryptographic schemes combine classical and post-quantum algorithms, providing defense-in-depth against cryptanalytic breakthroughs in either family. However, hybrid approaches double cryptographic operations (key generation, signing, verification) and further increase certificate and signature sizes. The operational overhead of hybrid cryptography is substantial but necessary during the multi-year transition period [7].

 doi:10.20944/preprints202511.1764.v1

Parameter uniformity across ecosystems is critical to avoid interoperability failures. If different sectors or geographic regions standardize on incompatible PQC parameter sets, cross-sector communication requires protocol negotiation overhead and increases the attack surface through downgrade attacks. International standardization bodies (NIST, ETSI, ISO) must coordinate to ensure global parameter alignment, but regional variations driven by national security concerns or industrial policy create fragmentation risks [17].

2.4.4. Budget and Planning

Infrastructure upgrades, personnel training, interoperability labs, consulting support, and extended hybrid operation require significant sustained funding [14,18]. Enterprise IT budgets typically allocate 70–80% to operations and maintenance, leaving limited capacity for transformational projects. PQC migration competes with other priorities: cloud adoption, Zero Trust implementation, OT security modernization, and regular security operations.

Capital and Operational Expenditure: Organizations must budget for:

- Hardware replacement: HSMs, cryptographic accelerators, non-upgradeable embedded devices
- Software licensing: upgraded applications, operating systems, security tools with PQC support
- Network infrastructure: middlebox upgrades, bandwidth expansion, testing equipment
- Personnel costs: training, consulting, additional staffing for migration programs
- Opportunity costs: deferred projects, slower feature development during migration

Budget constraints force deferrals and phased approaches that extend timelines by several years. Organizations with limited capital budgets may stretch hardware replacement over 5–7 year refresh cycles rather than accelerated 2–3 year replacement needed for timely PQC adoption [19].

Planning Quality and Program Management: Migration success depends critically on planning quality and program management rigor. Organizations that conduct comprehensive cryptographic inventories, prioritize systems based on risk and data sensitivity, develop detailed migration roadmaps with milestone dependencies, and establish governance structures for decision-making execute faster and more reliably than organizations approaching migration reactively [19].

However, many organizations lack mature asset management and cryptographic inventories. Discovering all cryptographic implementations across thousands of applications and devices is itself a multi-year undertaking. Organizations that defer cryptographic discovery until migration becomes urgent face compressed timelines and higher execution risk [14].

2.5. Zero Trust Architecture Implications

Zero Trust Architecture has emerged as the dominant security paradigm for modern enterprises, predicated on "never trust, always verify" principles. Zero Trust depends fundamentally on strong cryptographic assurances for identity, access control, and secure communication [20]. PQC migration directly impacts every Zero Trust pillar:

2.5.1. Identity and Authentication

PKI and Certificate Management: Zero Trust identity relies on cryptographic certificates and ephemeral tokens (e.g., JSON Web Tokens) for device authentication, user authentication, and service-to-service authentication. ML-DSA-signed tokens can exceed default HTTP header limits: many web servers (Apache, Nginx, IIS) and load balancers enforce 4KB–8KB header size limits. A Dilithium-signed JWT plus Kyber-encapsulated session key can breach these limits, requiring reconfiguration of thousands of web servers and ingress controllers across global estates—a discovery and remediation effort spanning years. Larger PQC certificates additionally impact:

- Certificate enrollment: Increased bandwidth and processing for certificate issuance at scale
- Certificate storage: Limited storage on smart cards, HSMs, and embedded authenticators
- Certificate validation: OCSP and CRL bandwidth requirements scale with certificate size
- Certificate renewal: Automated renewal systems must handle larger payloads

 doi:10.20944/preprints202511.1764.v1

Hybrid certificates combining classical and post-quantum keys double storage requirements and validation overhead. Organizations implementing Zero Trust must plan for a 5–10× expansion of PKI infrastructure capacity to maintain performance [6,7].

Multi-Factor Authentication: MFA systems employing certificate-based authentication or FIDO2 tokens require firmware updates or hardware replacement to support PQC. FIDO Alliance has published PQC specifications, but device availability and organizational deployment timelines lag standardization by 2–4 years. Organizations cannot complete Zero Trust deployments until all authentication factors achieve quantum resistance [14].

2.5.2. Access Control and Policy Enforcement

Latency Impacts: Zero Trust architectures enforce access decisions at the transaction level, requiring cryptographic operations for each request. Increased PQC signature verification times affect:

- API gateway performance: Per-request signature verification becomes a bottleneck
- Microsegmentation: Increased latency between microservices
- Real-time systems: Latency-sensitive applications may violate performance requirements

Organizations must evaluate whether to accept performance degradation, invest in cryptographic acceleration hardware, or redesign applications to reduce per-transaction cryptographic overhead [13].

Crypto-Agility in Policy Enforcement: Zero Trust policy engines must support crypto-agility, allowing gradual rollout of PQC algorithms without disrupting access for legacy systems. Policy engines must negotiate supported algorithms, maintain allowlists of permitted algorithm combinations, and enforce minimum security levels while preventing downgrade attacks. This flexibility adds complexity to policy management and increases the attack surface during transition [25].

2.5.3. Secure Communication Channels

Hybrid TLS and Network Segmentation: Zero Trust assumes all network segments are untrusted, requiring end-to-end encryption for all communications. During PQC transition, networks must support:

- Classical TLS for legacy systems unable to upgrade
- Hybrid TLS for systems in transition
- Pure PQC TLS for fully migrated systems

Network segmentation strategies may isolate non-PQC systems in separate VLANs or security zones, but this complicates network management and may conflict with microsegmentation principles requiring fine-grained access control [10].

Service Mesh and Encryption: Service mesh architectures implementing Zero Trust for microservices face challenges. Sidecar proxies handling encryption must support multiple cryptographic configurations simultaneously, increasing resource consumption and operational complexity. Latency-sensitive microservices may require architectural changes to maintain acceptable performance with PQC overhead [13].

2.5.4. Monitoring and Audit

Log Volume and Storage: Larger PQC signatures affect security event logging and audit trails. If every API transaction logs a 3,300-byte ML-DSA signature for non-repudiation, log storage requirements increase 50× compared to ECDSA. Organizations must expand SIEM capacity, extend log retention periods to accommodate volume, or implement selective signature logging based on risk assessment [7].

Security Monitoring Tools: Security monitoring and threat detection tools must understand PQC protocols to differentiate legitimate traffic from attacks. Signature validation failures may indicate quantum attacks, implementation errors, or configuration mismatches. Security operations teams require training to interpret PQC-related security events and distinguish actual threats from migration-related transient issues [14].

 doi:10.20944/preprints202511.1764.v1

2.5.5. Partner Trust and Federated Identity

Cross-Organization Authentication: Zero Trust principles extend to partner organizations through federated identity and trust brokers (SAML, OAuth, OpenID Connect). Partner migrations operate on independent timelines, requiring long-term hybrid operation at federation boundaries. Trust frameworks must specify minimum cryptographic requirements and upgrade schedules to prevent weakest-link vulnerabilities [5,16].

Supply Chain Security: Zero Trust for supply chains requires cryptographic verification of software components, firmware updates, and hardware authenticity throughout the supply chain. Software Bill of Materials (SBOM) signing, secure boot, and attestation mechanisms must transition to PQC concurrently with other enterprise systems to maintain end-to-end security assurance [12].

2.5.6. Zero Trust Timeline Extension

The interdependencies between Zero Trust implementation and PQC migration mean that organizations pursuing both initiatives simultaneously face extended timelines for either or both. Organizations must carefully sequence initiatives, potentially accepting interim security postures that compromise neither pure Zero Trust nor complete quantum resistance, but represent pragmatic progress toward both goals. This strategic planning requires executive-level risk acceptance and resource commitment [20].

3. Migration Timeline Analysis

3.1. Enterprise Size Definitions

Enterprise size classification varies by jurisdiction and industry, affecting how organizations approach migration planning and resource allocation. In the United States, the Small Business Administration (SBA) defines "small business" using industry-specific thresholds typically expressed in number of employees or average annual receipts [21]. Internationally, "SME" definitions depend on country-specific policy, such as revised thresholds in India reflecting investment and turnover limits [22–24].

For this paper, the following working definitions are used:

Small enterprise: $\leq$500 employees or within SBA "small business" receipts thresholds for respective industry sectors; limited internal security engineering capacity; high reliance on cloud/SaaS vendors; typically, single-location or limited geographic footprint; minimal formal governance structures; usually exempt from most regulatory reporting requirements; budget constraints typically limiting major capital expenditures.

Medium enterprise: Exceeds SBA "small" thresholds but below "large" enterprise characteristics; typically, 500–5,000 employees; multiple business units with some autonomy; hybrid cloud estates combining on-premises and cloud infrastructure; moderate internal engineering capacity supplemented by contractors; established governance structures but not comprehensive; regional or national operations; moderate regulatory burden depending on industry sector; annual IT budgets typically \$5M–\$100M.

Large enterprise: Global or multi-regional operations spanning multiple countries and regulatory jurisdictions; typically >5,000 employees with thousands in IT/security functions; characterized by complex supply chains and extensive partner ecosystems; thousands of applications and business processes; dedicated security, compliance, and architecture teams; comprehensive governance and program management capabilities; extensive regulatory requirements (SOX, PCI-DSS, FISMA, etc.); annual IT budgets exceeding \$100M; substantial legacy system accumulation over decades of operation.

These definitions align broadly with international SME definitions while recognizing that regulatory and industry-specific variations create substantial heterogeneity within each category. Organizations near category boundaries may exhibit characteristics of adjacent categories, requiring flexible migration planning approaches.

 doi:10.20944/preprints202511.1764.v1

3.2. Timeline Estimates by Enterprise Size

Migration timelines vary significantly depending on enterprise size, infrastructure complexity, legacy system prevalence, budget availability, personnel capacity, and inter-enterprise coordination requirements. Table 1 summarizes both optimistic and realistic estimates for PQC migration, alongside the expected arrival window for FTQC and critical dependencies driving timeline variations.

Table 1. PQC Migration Timeline Estimates by Enterprise Size*

Enterprise Size	Optimistic Timeline	Realistic Timeline	FTQC Arrival	Key Dependencies	References
Small Enterprises	3–5 years	5–7 years	2028–2033	Vendor/cloud readiness, limited in-house expertise, SaaS reliance, and budget constraints	[14,17]
Medium Enterprises	6–8 years	8–12 years	2028–2033	Hybrid cloud, multiple business units, moderate legacy systems, partner coordination, and governance establishment	[16,17,20]
Large Enterprises	9–12 years	12–15+ years	2028–2033	Global infrastructure, thousands of applications, extensive IoT/legacy fleets, regulatory compliance across jurisdictions, and complex supply chain synchronization	[11,16,19,20]

*Edge cases with extreme complexity (extensive OT deployments, heavy regulatory burden) may exceed 20 years, as noted in Section 3.2.3.

3.2.1. Small Enterprise Migration Scenarios

Small enterprises typically have simpler IT environments but face distinct challenges. With 500 or fewer employees and limited internal security engineering capacity, small enterprises depend heavily on external vendors, cloud services, and SaaS applications [21]. This dependence creates both advantages and constraints.

Advantages: Small enterprises benefit from lower infrastructure complexity, fewer applications to assess and migrate, limited legacy system burden, and potentially faster decision-making without extensive governance overhead. Organizations heavily reliant on SaaS vendors may achieve rapid migration as vendors update their platforms, requiring minimal internal effort beyond user acceptance testing [17].

Constraints: Limited internal expertise necessitates external consulting support, increasing costs, and introducing scheduling dependencies on consultant availability. Budget constraints may force phased approaches or deferrals. Small enterprises often lack leverage to accelerate vendor timelines, making them dependent on vendor migration priorities. Critical custom applications without vendor support may require expensive rewrites or extended hybrid operation [14].

Timeline Drivers: Realistic 5–7-year timelines for small enterprises assume vendors deliver PQC-capable products within 2–3 years, organizations allocate budget for consulting and infrastructure upgrades within 1–2 years, cryptographic discovery and risk assessment completed within 1 year, and phased migration execution over 2–4 years with contingency for vendor delays or budget constraints.

Organizations in highly regulated industries (healthcare, finance) face extended timelines due to compliance requirements and audit cycles, potentially pushing timelines toward the upper bound or beyond.

 doi:10.20944/preprints202511.1764.v1

3.2.2. Medium Enterprise Migration Scenarios

Medium enterprises occupy the middle ground in complexity and resources. Exceeding SBA small business thresholds but remaining below large enterprise scale, medium enterprises typically operate multiple business units, maintain hybrid cloud estates combining on-premises and cloud infrastructure, and have established but not comprehensive governance structures [22–24].

Complexity Factors: Medium enterprises face infrastructure diversity requiring multiple migration approaches: aging on-premises data centers with limited refresh budgets, growing cloud footprints across multiple providers, business unit autonomy creating siloed technology decisions, and moderate accumulations of technical debt in legacy applications. These enterprises often maintain their own PKI for internal systems while depending on external CAs for public-facing services [16].

Resource Availability: Medium enterprises have dedicated security and infrastructure teams but frequently lack specialized cryptographic engineering expertise. They can afford external consulting support but must carefully manage consultant engagement scope to control costs. Personnel bandwidth remains a constraint, as security teams balance PQC migration against ongoing operations, compliance audits, incident response, and other security initiatives [14].

Governance and Planning: Medium enterprises benefit from more structured planning and governance than small enterprises, but lack the comprehensive program management offices typical of large enterprises. Establishing clear accountability, cross-functional coordination, and sustained executive attention represents a significant organizational challenge. Without dedicated migration program leadership, efforts fragment across business units with inconsistent progress [19].

Timeline Drivers: Realistic 8–12 year timelines for medium enterprises reflect: cryptographic inventory and risk assessment spanning 1–2 years across diverse infrastructure, governance establishment and program planning requiring 6–12 months, phased infrastructure upgrades over 3–5 years aligned with refresh cycles, application migration spanning 4–6 years with complex legacy system remediation, and partner coordination overhead adding 1–2 years for synchronized B2B communication migration [16,20].

Organizations at the lower end of medium enterprise scale (closer to small business thresholds) may achieve timelines toward the 8-year mark, while those approaching large enterprise complexity trend toward 12+ years.

3.2.3. Large Enterprise Migration Scenarios

Large enterprises face the most complex and protracted migration challenges. With global or multi-regional operations, thousands of applications and business processes, extensive IoT and OT deployments, heavy regulatory burden across multiple jurisdictions, and complex supply chains involving hundreds or thousands of partners, large enterprises require comprehensive, well-resourced migration programs sustained over 12–15+ years [11,19,20].

Scale and Complexity: A typical large enterprise may operate: 5,000–50,000 applications across on-premises, cloud, and hybrid environments; hundreds of data centers and thousands of network locations globally; millions of endpoints including laptops, mobile devices, IoT sensors, and OT controllers; complex supply chains with 100–1,000+ technology vendors and thousands of business partners requiring cryptographic interoperability [20].

Discovering, cataloging, and prioritizing this vast attack surface requires dedicated teams and sophisticated asset management systems, often taking 2–3 years for comprehensive visibility. Even with sophisticated tooling, shadow IT, undocumented systems, and acquired company infrastructure create blind spots requiring manual discovery [14].

Legacy System Burden: Large enterprises accumulate substantial technical debt over decades of operation. Mission-critical systems written in COBOL or other legacy languages may lack cryptographic agility or employ cryptography through obsolete libraries without clear upgrade paths. Industrial control systems and building management systems may operate proprietary protocols

 doi:10.20944/preprints202511.1764.v1

with vendor-specific cryptography implementations requiring expensive vendor engagement for upgrades [12].

Aircraft avionics, satellite communications systems, and defense systems have 15–30-year operational lifespans and may require a complete redesign for PQC support. Replacing these systems on accelerated timelines requires enormous capital expenditure and introduces operational risk during cutover [11].

Regulatory Complexity: Large enterprises operate across multiple regulatory jurisdictions with varying PQC mandates and compliance timelines. U.S. federal contractors must comply with DoD and DHS guidance, financial institutions face evolving SEC and Federal Reserve requirements, healthcare organizations must satisfy HIPAA evolution, and European operations must align with ENISA recommendations and potentially emerging EU regulatory mandates [3,6].

Compliance demonstration requires extensive documentation, third-party audits, and regulatory approval cycles that add 6–12 months per major system certification. Organizations must sequence migrations to maintain continuous compliance across overlapping regulatory requirements [19].

Program Management Requirements: Large enterprise PQC migration requires dedicated program management offices with executive sponsorship, sustained multi-year funding, cross-functional governance structures, and sophisticated risk management. Migration programs compete with other enterprise initiatives for resources and executive attention. Without sustained commitment, migrations stall as organizational priorities shift [19].

Timeline Drivers: Realistic 12–15+ year timelines for large enterprises reflect a 'green path' scenario assuming optimal conditions: cryptographic discovery and inventory across global infrastructure requiring 2–3 years, risk assessment and prioritization spanning 1 year, governance establishment and detailed roadmap development requiring 6–12 months, infrastructure upgrades phased over 5–7 years aligned with refresh cycles but accelerated beyond normal pace, application migration across thousands of applications spanning 8–10 years with complex legacy remediation, IoT/OT replacement programs requiring 5–8 years for fleet renewal, partner ecosystem coordination requiring 3–5 years for key partner synchronization, and regulatory compliance demonstration requiring ongoing effort throughout migration [11,16,19,20].

Organizations with particularly complex global footprints, extensive OT deployments, or heavy regulatory burden may experience 20+ year migration cycles, potentially requiring acceptance of residual quantum risk for some systems approaching end-of-life.

3.3. Comparative Analysis

Table 2 provides a comparative view highlighting that migration speed is not solely determined by enterprise size, but by the interplay of infrastructure complexity, personnel capacity, governance maturity, and vendor dependencies.

Large enterprises, despite having greater budgets and personnel, face the longest timelines due to scale, complexity, regulatory obligations, and the necessity of maintaining operational continuity throughout migration [20]. The "slow but thorough" characterization reflects both the burden of complexity and the benefit of comprehensive testing and validation, reducing implementation failures.

Small enterprises face a "fast but risky" scenario where rapid migration through vendor dependence introduces risk if vendors stumble or if custom applications lack proper migration planning. Medium enterprises achieve the most balanced posture, with sufficient resources and governance to manage risk while avoiding the overwhelming complexity of large enterprise scale [17].

 doi:10.20944/preprints202511.1764.v1

Table 2. Comparative Analysis of Enterprise Migration Factors

Factor	Small	Medium	Large
Infrastructure Impact	Low	Moderate	High
Personnel Availability	Limited	Moderate	Extensive but siloed
Governance	Minimal	Structured	Heavy, regulated
Vendor Dependence	High	Medium	Very high
Legacy System Burden	Low	Moderate	Severe
Migration Speed	Fast but risky	Balanced	Slow but thorough
Budget Flexibility	Constrained	Moderate	Available but allocated
Compliance Overhead	Minimal	Moderate	Extensive

4. Risk Mitigation and Strategic Frameworks

4.1. Risk Analysis and Mitigation Strategies

4.1.1. Quantum Threat Risk Assessment

Organizations must conduct quantum-specific threat modeling to prioritize migration efforts. Not all systems face equal quantum risk. Risk factors include:

Data Sensitivity and Longevity: Systems handling high-value intellectual property, national security information, long-term medical records, or multi-decade financial contracts face the highest Store Now Decrypt Later risk. These systems should receive migration priority even if quantum computing remains years away [3].

Cryptographic Algorithm Exposure: Systems employing RSA-1024 or ECC P-256 face a higher risk than those using RSA-4096 or ECC P-384, providing slightly more security margin. However, all classical public-key cryptography should be considered vulnerable within the FTQC arrival window [4].

Attack Surface: Internet-facing systems with direct adversary access face a higher risk than air-gapped or physically controlled systems. However, supply chain attacks may compromise even isolated systems through firmware or software updates [12].

4.1.2. Phased Migration Strategies

Parallel Operation: Maintain classical and PQC systems in parallel during transition, routing traffic based on capability negotiation. This approach provides fallback capability but increases operational complexity and infrastructure costs [7].

Hybrid Cryptography: Employ hybrid schemes combining classical and PQC algorithms during transition. Hybrid approaches provide defense-in-depth but create 'zombie' algorithms: RSA and ECC become cryptographically obsolete (insecure against quantum attacks) yet operationally alive, wrapped inside PQC tunnels. These zombie libraries require continued patching for conventional vulnerabilities (buffer overflows, side-channels) throughout the multi-year transition, creating a long-term maintenance burden. Hybrid approaches double the cryptographic overhead and increase certificate sizes further [6].

Prioritized Rollout: Migrate highest-risk systems first (SNDL-vulnerable data, internet-facing authentication, critical infrastructure), followed by moderate-risk systems, with low-risk or end-of-life systems potentially accepting residual quantum risk [14].

4.1.3. Contingency Planning

Organizations should develop contingency plans for:

 doi:10.20944/preprints202511.1764.v1

FTQC Arrival Earlier Than Expected: Maintain accelerated migration plans that can be activated if quantum computing progress exceeds projections. Identify critical systems that absolutely must achieve quantum resistance and ensure these receive priority regardless of timeline pressures [1,2].

Algorithm Cryptanalysis: Monitor cryptanalytic research for potential vulnerabilities in NIST-standardized PQC algorithms. Maintain crypto-agility, allowing rapid algorithm substitution if needed [25].

Vendor Delays: Identify critical vendor dependencies and develop alternatives (competing vendors, open-source implementations, custom development) to maintain migration momentum if key vendors fail to deliver [17].

Budget Constraints: Develop phased approaches with clear dependencies allowing work to pause and resume if budget constraints force temporary deferrals without losing progress [19].

4.2. Crypto-Agility Framework

4.2.1. Principles of Crypto-Agility

Crypto-agility—the capability to rapidly switch cryptographic algorithms without extensive system redesign—has emerged as a critical discipline for managing PQC transition and future cryptographic evolution [25]. Organizations that design systems with crypto-agility can respond rapidly to cryptanalytic breakthroughs, regulatory mandate changes, or performance optimization opportunities.

Key Principles:

Algorithm Abstraction: Design systems with clear separation between cryptographic operations and application logic. Applications should invoke cryptographic services through well-defined APIs without direct algorithm dependencies [25].

Parameter Flexibility: Avoid hardcoding key sizes, signature formats, or protocol versions. Store cryptographic parameters in configuration systems, allowing updates without code changes [7].

Protocol Negotiation: Implement robust capability negotiation in communication protocols, allowing endpoints to agree on supported algorithms dynamically. Ensure negotiation mechanisms resist downgrade attacks [13].

Monitoring and Metrics: Instrument systems to track cryptographic algorithm usage, performance characteristics, and failure modes. Analytics should identify systems lacking crypto-agility requiring prioritized remediation [14].

4.2.2. Implementation Strategies

Cryptographic Service Layer: Implement centralized cryptographic services providing algorithm-agnostic APIs to applications. Applications request "sign this data at security level X" rather than "generate an ECDSA P-256 signature." The service layer maps security levels to appropriate algorithms based on the current policy [25].

Configuration Management: Maintain cryptographic policies in centralized configuration systems supporting gradual rollout, A/B testing, and rapid rollback. Policy updates should propagate through enterprise systems within minutes to hours, not days or weeks [14].

Testing and Validation: Develop comprehensive test suites validating system behavior across all supported algorithm combinations. Automated testing should prevent regressions when updating cryptographic libraries or introducing new algorithms [19].

4.2.3. Organizational Capabilities

Crypto-agility requires organizational capabilities beyond technical implementation:

Governance: Establish cryptographic review boards with authority to mandate algorithm changes, evaluate new cryptographic techniques, and enforce minimum security levels across the enterprise [19].

Expertise: Develop or acquire cryptographic engineering expertise capable of evaluating algorithm security, understanding implementation vulnerabilities, and advising on parameter selection [14].

 doi:10.20944/preprints202511.1764.v1

Lifecycle Management: Integrate cryptographic algorithm lifecycle management into existing IT governance, treating algorithms as assets requiring regular assessment, planned obsolescence, and replacement [25].

4.3. Policy and Regulatory Considerations

4.3.1. Emerging Regulatory Mandates

Governments worldwide are developing PQC transition mandates with varying timelines and requirements:

United States: The Office of Management and Budget (OMB) and CISA have issued guidance for federal agencies requiring PQC migration planning and inventory completion. DoD has established timelines for quantum-resistant cryptography deployment across defense systems. Financial regulators are evaluating PQC requirements for critical financial infrastructure [3,6].

European Union: ENISA has published PQC implementation guidance and recommendations for EU member states. Individual countries are developing national migration strategies aligned with EU cybersecurity frameworks. Critical infrastructure operators face emerging requirements for quantum-resilient security [20].

International: Other nations, including China, the UK, Canada, Australia, and Japan, have initiated PQC transition programs with varying degrees of mandatory requirements for government systems, critical infrastructure, and regulated industries [16].

4.3.2. Compliance Timeline Challenges

Regulatory mandates face challenges in establishing realistic timelines. Regulators must balance security urgency against industry capacity constraints. Mandates that are too aggressive risk mass non-compliance or prioritization of compliance over security effectiveness. Mandates that are too lenient may fail to drive adequate urgency given SNDL threats and FTQC arrival projections [3].

Enterprises operating across multiple jurisdictions must navigate potentially conflicting requirements, different timeline expectations, and varying cryptographic algorithm approvals. International coordination on regulatory harmonization remains limited, creating compliance complexity for multinational enterprises [16].

5. Conclusions and Future Directions

5.1. Future Research Directions

Several critical areas warrant further investigation:

Automated Migration Tools: Development of automated discovery, assessment, and migration planning tools could substantially reduce timeline and resource requirements. Research into AI-assisted cryptographic code analysis and automated hybrid implementation could accelerate deployment [14].

Performance Optimization: Continued research into PQC algorithm optimization, particularly for embedded systems and resource-constrained environments, could enable broader deployment. Hardware acceleration and specialized cryptographic coprocessors may prove critical for maintaining performance [7].

Post-Quantum Blockchain: Blockchain systems face unique migration challenges given distributed consensus requirements and backward compatibility constraints. Research into PQC-resilient blockchain architectures and migration strategies remains nascent [12].

Supply Chain Coordination: Development of industry-specific coordination frameworks, standardized migration playbooks, and interoperability testing regimens could reduce inter-enterprise synchronization overhead [5,16].

Quantum-Resistant Zero Trust: Further research into optimized Zero Trust architectures accounting for PQC performance characteristics could inform design patterns minimizing migration disruption [20].

 doi:10.20944/preprints202511.1764.v1

5.2. Concluding Remarks

Migration to post-quantum cryptography represents a decade-long undertaking for most enterprises, with realistic timelines of 5–7 years for small enterprises, 8–12 years for medium enterprises, and 12–15+ years for large enterprises. These timelines reflect the compounding effects of infrastructure complexity, non-portable embedded devices, personnel scarcity, budget constraints, planning quality variability, and essential inter-enterprise coordination [11,14,18].

Unlike past cryptographic migrations, PQC requires unprecedented ecosystem-wide synchronization spanning industries, national boundaries, and regulatory frameworks [5,16]. The multi-dimensional challenge space encompasses technical, organizational, economic, and geopolitical factors that resist simple solutions or accelerated timelines through resource allocation alone.

Enterprises must plan for extended hybrid operation, maintaining both classical and post-quantum cryptographic capabilities throughout multi-year transitions. This hybrid operation increases operational complexity, infrastructure costs, and attack surface, but represents the only pragmatic path forward given ecosystem dependencies and vendor timeline constraints [7,25].

Investment in crypto-agility—designing systems capable of rapidly switching cryptographic algorithms—should be viewed not merely as a PQC migration enabler but as a permanent capability for managing future cryptographic evolution. The PQC transition provides an opportunity to establish organizational structures, technical architectures, and governance processes supporting algorithm agility for decades to come [25].

Given FTQC arrival projections between 2028 and 2033 [1,3], and the Store Now Decrypt Later threat affecting data encrypted today, enterprises must initiate migration planning immediately despite lengthy execution timelines. The juxtaposition of migration timelines (12–15 years) against FTQC arrival (5–10 years) reveals a mathematical certainty: systemic risk exposure. Large enterprises face a risk deficit where the time required to secure infrastructure exceeds the time remaining before the threat materializes. This is not a planning failure but an intrinsic property of complex system inertia meeting rapidly advancing threat capability.

Organizations that defer migration planning until FTQC arrives will face crisis scenarios with compressed timelines, emergency resource allocation, and substantially elevated risk of quantum attacks against unprepared systems. Early planning, sustained executive commitment, adequate resource allocation, and ecosystem-wide coordination represent the only path to managing quantum cryptographic risk effectively.

The PQC transition represents not merely a technical upgrade but a fundamental transformation of enterprise cryptographic architectures requiring sustained commitment over more than a decade. Success requires treating migration as a strategic imperative, warranting executive attention, dedicated program management, and sustained funding comparable to other enterprise transformations rather than routine technology refreshes.

Acknowledgments: The authors acknowledge the contributions of the cryptographic research community, NIST PQC standardization participants, and industry practitioners sharing migration experiences that informed this analysis.

Conflicts of Interest: The author declares no competing interests.

References

1. M. Mosca and M. Piani, "Quantum Threat Timeline Report 2023," Global Risk Institute, Dec. 2023. [Online]. Available: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/
2. IBM, "IBM lays out clear path to fault-tolerant quantum computing," IBM Quantum Blog, Jun. 2024. [Online]. Available: https://www.ibm.com/quantum/blog/large-scale-ftqc
3. CISA, NSA, and NIST, "Quantum-Readiness: Migration to Post-Quantum Cryptography," Joint factsheet, Aug. 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-08/Quantum-Readiness%20-%20Migration%20to%20Post-Quantum%20Cryptography_508c.pdf

 doi:10.20944/preprints202511.1764.v1

4. V. Gheorghiu and M. Mosca, "Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes," arXiv:1902.02332, Feb. 2019. [Online]. Available: https://arxiv.org/abs/1902.02332
5. D. Stebila, "Standardizing Post-Quantum Cryptography at the IETF," PKIC 2023, 2023. [Online]. Available: https://www.ietf.org/blog/pqc-standardization
6. National Institute of Standards and Technology, "NIST announces first post-quantum cryptography standards (FIPS 203, 204, 205)," Aug. 2024. [Online]. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
7. National Institute of Standards and Technology, "Getting Ready for Post-Quantum Cryptography," NIST Cybersecurity White Paper, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.2021.pdf
8. National Institute of Standards and Technology, "Announcing the Advanced Encryption Standard (AES)," FIPS PUB 197, Nov. 2001. [Online]. Available: https://csrc.nist.gov/publications/detail/fips/197/final
9. Microsoft, "SHA-1 signed content retired," Microsoft Learn, 2017. [Online]. Available: https://learn.microsoft.com/en-us/lifecycle/announcements/sha1-deprecation
10. E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Aug. 2018. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8446
11. National Institute of Standards and Technology, "Transitioning the Use of Cryptographic Algorithms and Key Lengths," SP 800-131A Rev. 2, 2019. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final
12. National Institute of Standards and Technology, "Post-Quantum Cryptography Standardization Project," 2022. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography
13. IETF, "Post-Quantum Cryptography Recommendations for TLS and Related Protocols (draft-ietf-pqc-tls)," 2023. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-pqc-tls/
14. Cloud Security Alliance, "Preparing Enterprises for Post-Quantum Cryptography," 2022. [Online]. Available: https://cloudsecurityalliance.org/research/post-quantum-cryptography
15. Quantinuum, "Quantinuum accelerates the path to Universal Fully Fault-Tolerant Quantum Computing," Nov. 2024. [Online]. Available: https://www.quantinuum.com/blog/quantinuum-accelerates-the-path-to-universal-fault-tolerant-quantum-computing
16. Netherlands National Communications Security Agency, "The PQC Migration Handbook," Mar. 2023. [Online]. Available: https://english.aivd.nl/publications/publications/2023/04/04/the-pqc-migration-handbook
17. Encryption Consulting, "How to Start Your Enterprise PQC Migration Plan," 2023. [Online]. Available: https://www.encryptionconsulting.com/post-quantum-migration-plan/
18. IonQ, "IonQ Roadmap toward Cryptographically Relevant Quantum Computer by 2028," Jun. 2024. [Online]. Available: https://ionq.com/posts/june-2024-roadmap-update
19. DARPA, "Quantum Benchmarking Initiative (QBI)," Nov. 2024. [Online]. Available: https://www.darpa.mil/program/quantum-benchmarking-initiative
20. BSI, "BSI TR-02102-1. Cryptographic Mechanisms: Recommendations and Key Lengths," 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf
21. U.S. Small Business Administration, "Table of Size Standards," 2025. [Online]. Available: https://www.sba.gov/document/support-table-size-standards
22. Reserve Bank of India, "MSME FAQs," 2025. [Online]. Available: https://www.rbi.org.in/commonman/Upload/English/FAQs/PDFs/MICRO30072025E.pdf
23. IndiaFilings, "MSME Definition: Revised Investment & Turnover Limits," 2025. [Online]. Available: https://www.indiafilings.com/learn/msme-new-definition/
24. Economic Times, "Firms up to Rs 500 crore are now medium; MSMEs get a new definition," 2025. [Online]. Available: https://economictimes.indiatimes.com/small-biz/sme-sector/firms-up-to-rs-500-crore-are-now-medium-msmes-get-a-new-definition/articleshow/117823447.cms
25. NIST National Cybersecurity Center of Excellence, "Migration to Post-Quantum Cryptography," 2021. [Online]. Available: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

 doi:10.20944/preprints202511.1764.v1