Q-Day Clock: Enterprise Post-Quantum Migration Imperative

Strategic Roadmap for the 2026–2031 Transition Window

Unofficial AI-assisted Research

Cloud Security Alliance AI Safety Initiative

2026-03-15

© 2026 Cloud Security Alliance. Unofficial AI-assisted Research.

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Executive Summary

For years, Q-Day – the date on which a sufficiently powerful quantum computer could break mainstream public-key cryptography – occupied a comfortable position on the distant horizon of enterprise risk registers. That comfort is no longer warranted. Forrester Research's "State Of Quantum Computing, 2026" report, published in March 2026, assessed practical quantum utility as feasible within five years and explicitly characterized Q-Day as a plausible risk by 2030 [1][2]. Simultaneously, hardware milestones from Google, IBM, and other vendors have demonstrated that key physics barriers to scalable fault-tolerant quantum computing appear tractable – transforming the timeline from speculative to engineering-bounded.

The cryptographic implications are structural. Today's dominant public-key infrastructure – RSA, elliptic curve cryptography (ECC), and Diffie-Hellman key exchange – rests on mathematical problems that a sufficiently large quantum computer could solve efficiently using Shor's algorithm. These algorithms protect virtually every encrypted communication, authenticated identity, and signed software artifact in modern enterprise environments. A cryptographically relevant quantum computer (CRQC) does not merely degrade this protection; it eliminates it entirely.

The standards response is largely complete. The National Institute of Standards and Technology (NIST) finalized its first three post-quantum cryptography standards on August 13, 2024: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) [3][4][5][6]. The National Security Agency's CNSA 2.0 framework provides a concrete implementation timeline extending through 2031 for national security systems [7]. What remains critically incomplete is enterprise adoption. A May 2025 survey of over one thousand senior cybersecurity managers found that only 5% of enterprises had quantum-safe encryption actually deployed, while 81% reported that cryptographic libraries and hardware security modules were not ready for PQC integration [8]. The gap between standard finalization and enterprise deployment – less than two years after the August 2024 standards release and only 5% deployment – is striking given the urgency of the underlying risk.

Compounding this readiness crisis is the Harvest Now, Decrypt Later (HNDL) threat, which renders the migration timeline critically asymmetric. Adversaries need not wait for Q-Day to act; they may be collecting encrypted enterprise data today, storing it for decryption once a CRQC becomes available. For data with multi-year sensitivity – intellectual property, financial records, strategic communications,

cryptographic key material — this means the effective security window may already be closing. Organizations that delay migration until quantum capability is proven are very likely to have already lost the data that most needed protection.

This whitepaper synthesizes current quantum hardware trajectories, the regulatory and standards landscape as of early 2026, enterprise readiness data, and proven migration methodologies into a structured roadmap for the 2026–2031 transition window. Its guidance is intended for CISOs, security architects, risk managers, and cloud security practitioners who must translate quantum risk from an abstract future scenario into a funded, sequenced program of work.

Introduction: The 2026 Inflection Point

Security professionals who have monitored quantum computing risk over the past decade are accustomed to a particular pattern: periodic claims of remarkable progress, followed by expert consensus that practical, cryptographically relevant quantum computers remain ten to fifteen years away. That pattern has broken. The combination of demonstrable error correction milestones, accelerating industry investment, and a new generation of Forrester and analyst forecasting projecting Q-Day risk within five years signals a genuine shift in the threat trajectory [1][2].

The conceptual framework for understanding why this shift matters requires distinguishing between physical qubits and logical qubits. Physical qubits — the raw computational elements in today's quantum processors — are fragile and error-prone; their decoherence rates make large-scale computation unreliable. Logical qubits are error-corrected units built from many physical qubits, capable of sustained reliable computation. The cryptographic relevance of quantum computers depends not on raw qubit counts but on the number of logical qubits available to execute Shor's algorithm at scale. Theoretical analyses, as synthesized by Forrester [2], suggest that factoring RSA-2048 using Shor's algorithm would require approximately 1,399 logical qubits under optimized conditions. While this represents a hardware scale not yet achieved, the engineering path to reach it has clarified substantially.

The urgency of 2026 specifically stems from the convergence of three developments. First, NIST's finalization of post-quantum standards in August 2024 removed the most significant technical barrier to enterprise adoption; organizations now have standardized, vetted algorithms available for immediate deployment. Second, hardware milestones in late 2024 and throughout 2025 demonstrated that quantum error correction now scales in the right direction — adding more physical qubits demonstrably reduces error rates rather than amplifying them, as was previously the norm. Third, regulatory deadlines are beginning to bite: by 2025, vendors of national security systems were expected to support and prefer CNSA 2.0 algorithms in new software and firmware, with January 1, 2027 set as the deadline by

which all new national security system acquisitions must be CNSA 2.0-compliant by default [7]. NSM-10 established a federal target of quantum-resistant systems by 2035 [15]. Executive Order 14306, signed in June 2025, further reinforced federal cybersecurity modernization priorities including quantum-safe cryptography requirements [26]. The intersection of technical feasibility, available standards, and regulatory pressure defines 2026 as the year enterprises must shift from awareness to action.

The Quantum Threat to Cryptography

To appreciate the severity of the post-quantum transition challenge, it is necessary to understand which cryptographic mechanisms are threatened, how severely, and which are not. The threat picture is not uniform, and conflating symmetric and asymmetric cryptographic vulnerabilities leads to distorted risk assessments and misprioritized migration efforts.

Public-key cryptography — the family of algorithms that enables two parties to securely establish shared keys without prior contact — is existentially threatened by sufficiently large quantum computers. RSA encryption and digital signatures rely on the difficulty of factoring the product of two large primes, a problem solvable in polynomial time by Shor's algorithm on a quantum processor [23]. Elliptic curve cryptography (ECC), used pervasively in TLS key exchange, code signing, and certificate infrastructure, relies on the elliptic curve discrete logarithm problem — similarly vulnerable to Shor's algorithm. Diffie-Hellman key exchange, including its elliptic curve variant (ECDH), is likewise affected. The practical consequence is that every TLS handshake, every code-signing certificate, every PKI-based identity assertion, and every SSH connection currently secured with these algorithms will offer no cryptographic protection against an adversary possessing a sufficiently powerful quantum computer.

Symmetric cryptography faces a categorically different, and more manageable, threat. Grover's algorithm can search an unsorted database of N entries in approximately $\sqrt{N}$ operations on a quantum processor, which effectively halves the security strength of symmetric algorithms. AES-128 would be reduced to 64-bit equivalent security under quantum attack, falling below acceptable thresholds; AES-256, reduced to 128-bit equivalent, remains within margins current guidance considers acceptable. Hash functions such as SHA-256 experience a similar reduction, which is why NIST guidance for post-quantum symmetric security recommends minimum 256-bit hash lengths and AES-256 for symmetric key operations [21]. Critically, the quantum attack on symmetric cryptography requires an operational CRQC to execute — the Grover speedup does not assist in passive data collection. This means symmetric protection of data in storage remains meaningful even under HNDL threat models, whereas public-key-encrypted data in transit is vulnerable to collection today for decryption later.

The threat boundary within public-key cryptography is also important to understand. Not all asymmetric algorithms are equally vulnerable. Lattice-based, hash-based, and code-based mathematical structures form the foundation of NIST's post-quantum algorithms precisely because no efficient quantum algorithm is known to solve them. The NIST finalists and approved standards were selected through a rigorous eight-year process involving global cryptanalytic scrutiny, providing strong grounds for confidence that they offer post-quantum security under current cryptanalytic knowledge [3], though NIST explicitly maintains SLH-DSA as a backup to hedge against unforeseen lattice cryptanalysis advances.

Hardware Milestones Accelerating the Timeline

Three quantum hardware milestones between late 2024 and early 2026 materially changed consensus expectations about the Q-Day timeline. Taken together, they suggest the path to a cryptographically relevant quantum computer is an engineering problem with a plausible solution trajectory within this decade, not a theoretical barrier requiring fundamental scientific breakthroughs.

Google's announcement of the Willow quantum processor on December 9, 2024 attracted widespread attention primarily because of a single property: for the first time, increasing the number of physical qubits used in an error-correction code demonstrably reduced the error rate [10][11]. Prior to Willow, most quantum processors exhibited the opposite behavior — more qubits meant more opportunities for decoherence and cross-talk, making error correction increasingly difficult at scale. Willow's 105-qubit chip, using surface code error correction, achieved a logical error rate reduction of approximately 2.14x for each increase in code distance, ultimately producing a 101-qubit distance-7 code with 0.143% error per correction cycle [11]. Google's chief executive indicated the trajectory toward a fully useful error-corrected quantum computer by approximately 2029. Importantly, Google itself acknowledged that Willow is not a cryptographic threat in its current form; breaking RSA would require thousands of logical qubits, which in turn implies millions of physical qubits. What Willow demonstrated was that the hardware scaling law now favors the builders rather than working against them.

IBM's 2025 roadmap disclosures provided complementary evidence. IBM's Quantum Nighthawk processor, delivering 120 qubits with 218 tunable couplers, advanced the density of high-fidelity two-qubit gates available to algorithms. IBM's parallel Quantum Loon experimental system demonstrated all key processor components required for fault-tolerant operation, functioning as a proof of concept for IBM's fault-tolerant architecture [12]. IBM's published roadmap projects the first large-scale fault-tolerant quantum computer carrying approximately 200 logical qubits by 2029 [12]. IBM's roadmap describes further scaling ambitions in subsequent system generations, with aspirational targets toward qubit counts at which Shor's algorithm against RSA-2048 would become a practical operation. IBM also

announced manufacturing transitions to 300mm wafer fabrication during 2025, which doubled R&D throughput and achieved a tenfold increase in chip physical complexity, suggesting the industrial production base for fault-tolerant quantum computing is being established in parallel with its scientific foundations [12].

Perhaps the most aggressive public timeline projection comes from IonQ, whose roadmap — as analyzed by McKinsey in its survey of major vendor timelines — reportedly targets a cryptographically relevant quantum computer by 2028 [25]. IonQ's trapped-ion architecture offers different error characteristics than superconducting approaches, and its roadmap is the most bullish among major vendors. The diversity of credible players each independently projecting CRQC capability between 2028 and 2031 should be read as a coherent signal rather than outlier speculation. Forrester's "State Of Quantum Computing, 2026" explicitly synthesizes this hardware trajectory into the assessment that Q-Day is a plausible risk by 2030 [1][2] — a framing consistent with the hardware evidence if not certain.

Harvest Now, Decrypt Later: The Active Threat Today

The preceding sections describe the Q-Day risk as a future problem — an adversary who, in a few years, could decrypt today's communications. This framing is dangerously incomplete. The adversary side of the HNDL equation is not a future state; it is a present one. An adversary who wishes to harvest encrypted data today for quantum decryption later needs no quantum capability at scale. They need only network access, storage capacity, and patience — resources that well-resourced nation-state actors demonstrably possess.

The intelligence community assessments most directly relevant here are not publicly detailed, but NSA has explicitly warned in its CNSA 2.0 guidance that adversaries may already be harvesting encrypted data with long-term strategic value, intending to hold that ciphertext until quantum decryption capability matures [7]. CISA and other agencies have reinforced this concern in the context of critical infrastructure protection. The pattern of network traffic anomalies consistent with bulk collection is observable in public routing data. Traffic interception incidents in 2016, 2019, and 2020 — in which internet traffic destined for South Korean, European, and major internet service provider networks was rerouted through China and Russia, respectively — have been documented by network routing monitors and security researchers. These incidents are consistent with bulk ciphertext collection methodology, though the forensic verification problem inherent to HNDL means definitive attribution to quantum-motivated collection remains impossible until decryption capability exists.

The asymmetry of the HNDL threat model reframes the urgency of PQC migration for enterprises. Traditional security migration timelines are assessed against the question: when will the current approach become insecure? Under HNDL, the question becomes: when was sensitive data collected? For data whose confidentiality must hold for more than the estimated interval to Q-Day, that data is already at risk. This reframing is particularly consequential for several categories of enterprise data: long-term contracts and intellectual property with multi-year competitive value, regulated personal data subject to long retention periods, cryptographic key material that protects other assets, authentication credentials and identity artifacts, and communications between executives and legal counsel with attorney-client privilege implications. Each of these categories warrants immediate re-examination of the encryption methods used during transmission and, where feasible, re-encryption of archived data under quantum-resistant algorithms.

The practical implication is that Harvest Now, Decrypt Later converts the migration timeline from a future deadline into a retroactive exposure window. If CRQCs arrive by approximately 2030 and adversaries have been conducting HNDL collection since 2025 or earlier, organizations that begin migration in 2030 will not have protected data collected in the preceding five years. The correct mental model is not "when must I finish?" but rather "what is the sensitivity horizon of my most valuable data, and am I already past the point where collection has compromised that sensitivity?"

The Standards Arsenal: FIPS 203, 204, 205, and CNSA 2.0

The post-quantum cryptography standards landscape stabilized significantly in 2024 and 2025, providing enterprises with a clear algorithmic foundation for migration planning. The key development was NIST's simultaneous publication of three final Federal Information Processing Standards on August 13, 2024, completing a standardization process that began with the initial call for submissions in 2016 [3].

The three finalized standards address the two primary use cases in public-key cryptography: key establishment and digital signatures.

FIPS 203 – ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) is NIST's primary standard for key establishment, derived from the CRYSTALS-Kyber submission [4]. It specifies three parameter sets – ML-KEM-512, ML-KEM-768, and ML-KEM-1024 – corresponding to NIST security levels 1, 3, and 5 respectively. ML-KEM-768 provides security broadly comparable to AES-192, while ML-

KEM-1024 achieves a security level comparable to AES-256 and is the variant mandated by NSA's CNSA 2.0 for national security systems. ML-KEM replaces the classical key exchange mechanisms — RSA-KEM and ECDH — in TLS and similar protocols.

FIPS 204 — ML-DSA (Module-Lattice-Based Digital Signature Standard) is NIST's primary standard for general-purpose digital signatures, derived from CRYSTALS-Dilithium [5]. Its three parameter sets — ML-DSA-44, ML-DSA-65, and ML-DSA-87 — similarly map to increasing security levels. ML-DSA-87, mandated by CNSA 2.0 for national security system use, replaces RSA signatures and ECDSA across code signing, certificate authorities, and protocol authentication.

FIPS 205 — SLH-DSA (Stateless Hash-Based Digital Signature Standard) provides an alternative signature standard derived from SPHINCS+, offering security diversity through its hash-based mathematical foundation rather than lattice structures [6]. SLH-DSA produces larger signatures and operates more slowly than ML-DSA, but its security rests on a fundamentally different mathematical assumption. NIST explicitly recommends it as a backup to ML-DSA to hedge against the possibility — considered unlikely but non-negligible — of advances in lattice cryptanalysis.

Beyond these three standards, NIST continues to expand the portfolio. FIPS 206 (FN-DSA, based on FALCON), which produces compact signatures approximately 666 bytes in size, was submitted for Department of Commerce clearance in August 2025 and is expected to finalize in 2026 [28]. A code-based key encapsulation mechanism (HQC) was selected in March 2025 and is proceeding through the draft standard process with finalization expected around 2027 [20]. The expanding portfolio reflects deliberate diversity strategy — spreading cryptographic risk across multiple mathematical foundations to ensure that a breakthrough in one area does not eliminate all protection simultaneously.

NSA's CNSA 2.0 framework, published in September 2022 and refined since, provides the most concrete regulatory timeline currently in force for enterprises serving national security system customers. By 2025, vendors of national security systems were expected to support and prefer CNSA 2.0 algorithms in new software and firmware [7]. By January 1, 2027, all new national security system acquisitions must be CNSA 2.0-compliant by default. Full enforcement — requiring all NSS cryptographic implementations to exclusively use CNSA 2.0 algorithms — takes effect December 31, 2031. For commercial organizations supporting government contracts, defense supply chains, or critical infrastructure that intersects with national security systems, these dates are not aspirational; they are contractual prerequisites.

The broader federal context is anchored by NSM-10 (May 2022), which directs all national security systems to be quantum-resistant by 2035 [15]. NIST IR 8547 — the draft guidance on deprecation timelines — proposes deprecating all algorithms providing 112 bits or fewer of security by 2030, and disallowing all quantum-vulnerable public-key algorithms by 2035 [14]. The White House estimated the

total cost of government-wide PQC migration at approximately $7.1 billion over the 2025–2035 decade [27]. That figure, staggering as it is, applies only to the federal government; private sector migration costs at aggregate scale are likely to be considerably higher.

The Enterprise Readiness Gap

The gap between regulatory direction and enterprise implementation is acute. Despite the finalization of NIST standards in August 2024 and years of advance notice, enterprise adoption of quantum-safe cryptography remains dramatically limited. A May 2025 survey commissioned by DigiCert and conducted by Propeller Insights across 1,042 senior and C-level cybersecurity managers in the United States, United Kingdom, and Australia found that only 5% of enterprises had quantum-safe encryption actually deployed [8]. Sixty-nine percent recognized that quantum computing posed a threat to their current encryption, and 46.4% reported substantial encrypted data at risk, yet the gap between recognition and implementation is enormous.

The 2026 Entrust/Ponemon study offered a somewhat more encouraging figure — 40% of organizations reported actively transitioning to PQC — though this likely reflects a different sample composition and broader definition of "transitioning" that may include assessment and planning work rather than deployed cryptographic changes [9]. Both figures confirm that the majority of enterprises have not completed meaningful PQC deployment as of early 2026.

The reasons for this gap are not primarily attitudinal — most security leaders understand the risk — but operational. The technical complexity of cryptographic migration is substantial. Cryptographic algorithms are not cleanly isolated components in modern enterprise infrastructure; they are embedded throughout applications, middleware, network devices, cloud services, hardware security modules (HSMs), certificate authorities, identity providers, and endpoint agents. Identifying and inventorying all cryptographic usage across a large enterprise is itself a multi-year project. Eighty-one percent of survey respondents reported that cryptographic libraries and hardware security modules were not ready for PQC integration, indicating that the vendor ecosystem, while rapidly advancing, had not fully reached enterprise-grade readiness as of mid-2025 [8].

Enterprise migration timelines depend heavily on organizational scale, architectural complexity, and the breadth of hardware-constrained systems in scope. Large enterprises with diverse application portfolios face the most extensive migration challenge, while smaller organizations with more uniform technology stacks can typically complete migration faster. Even under optimistic assumptions, the combination of inventory complexity, vendor ecosystem readiness gaps, and hardware replacement cycles means that large enterprises beginning migration in 2026 should not expect full completion before the early 2030s

– which means those that do not begin in earnest this year face a credible risk that their most sensitive historical communications will still be quantum-vulnerable when CRQCs arrive. The NCCoE's SP 1800-38 practice guide, produced with 47 industry collaborators, found approximately 50% throughput reduction in hybrid classical/PQC deployment configurations [16] – a performance impact that enterprises must budget for and test against their service-level requirements.

The performance implications extend beyond raw throughput. ML-KEM-768 keys are approximately 18 times larger than P-256 keys [19], requiring re-evaluation of bandwidth budgets, memory allocations in embedded systems, certificate chain lengths in PKI infrastructure, and storage capacity in HSMs with fixed key storage limits. For IoT devices, embedded systems, and legacy network equipment with constrained resources, the transition may require hardware replacement rather than software upgrade – making the migration a capital expenditure program in addition to an operational one.

A Phased Migration Roadmap

The complexity of enterprise PQC migration should not be an argument for delay; it is an argument for structured, prioritized sequencing. The following five-phase framework synthesizes guidance from CSA's "Practical Preparations for the Post-Quantum World" [21], NIST's NCCoE migration practice guide [16], and current enterprise deployment experience.

Phase 1 – Discovery and Inventory (Now through end of 2026)

The foundational work of any cryptographic migration program is a comprehensive inventory of cryptographic usage across the enterprise. This means cataloging every system, application, protocol, and data store that uses public-key cryptography – not at the application layer only, but including cloud service endpoints, network infrastructure, identity and access management systems, certificate authorities, code signing pipelines, API gateways, and any third-party vendor dependencies that perform cryptographic operations on enterprise data. Most large enterprises will find this inventory to be a significant project in its own right, requiring purpose-built tooling or commercial crypto-agility platforms rather than manual documentation.

The output of Phase 1 should be a prioritized risk register that correlates cryptographic usage with data sensitivity and confidentiality horizon. Systems protecting data that must remain confidential for ten or more years from the time of collection should be treated as highest priority – these are the assets most exposed to HNDL attacks. Systems managing long-lived credentials, certificate authorities, and key management infrastructure warrant special attention because their compromise extends vulnerabilities

downstream into every dependent system. This phase should also assess vendor quantum readiness through formal attestation requests, particularly for cloud service providers, HSM vendors, and PKI solution vendors.

Phase 2 – Architecture and Crypto-Agility Design (2026–2027)

Crypto-agility – the architectural principle of designing systems so that cryptographic algorithms can be replaced without re-engineering the surrounding application – is the most durable investment an enterprise can make in quantum readiness. Organizations that hard-coded RSA or ECDH into protocol implementations in the 1990s and 2000s face re-engineering costs today that properly agile architectures would largely avoid. Phase 2 establishes crypto-agility as an architectural standard for all new development and modernization projects.

Hybrid cryptographic approaches – simultaneously using both classical and post-quantum algorithms during the transition period – provide a meaningful interim risk reduction posture. A hybrid key exchange combining ECDH with ML-KEM means that an attacker must break both algorithms to recover the session key; it protects against HNDL attacks to the extent that ML-KEM provides quantum resistance, while retaining classical algorithm protection against any theoretical weaknesses in the newer post-quantum standards. NIST SP 800-227 [13] and the NCCoE practice guide provide specific guidance on hybrid deployment configurations. Several cloud providers, including AWS, Microsoft Azure, and Google Cloud, have deployed hybrid schemes in their managed services as a practical model enterprises can follow [17][18][19].

Phase 3 – High-Priority System Migration (2027–2028)

Phase 3 applies the PQC algorithms to the highest-risk systems identified in Phase 1, using the architectures established in Phase 2. Practical migration priorities in this phase include TLS certificates and certificate authorities (transitioning to ML-DSA signatures), key management infrastructure (transitioning to ML-KEM for key encapsulation), VPN and secure communication gateways, identity and access management platforms, and code signing systems. These are the systems most exposed to real-time HNDL risk and the most likely to be directly targeted in any future quantum-enabled attack.

This phase requires close coordination with cloud service providers, HSM vendors, and PKI vendors. Enterprises should require that vendor product roadmaps include FIPS 203/204/205 compliance commitments with specific delivery dates and contractual SLAs. Vendors who cannot provide a credible PQC roadmap should be treated as a migration risk requiring contingency planning.

Phase 4 – Broad Enterprise Migration (2028–2030)

Phase 4 extends post-quantum cryptography to the broader enterprise application and infrastructure estate, including internal applications, data-at-rest encryption programs, archive decryption and re-encryption for sensitive historical data, supply chain partner communications, and customer-facing services. This is typically the most operationally complex phase, because it involves the widest range of system types and the most diverse set of change management challenges.

Hardware-constrained systems – IoT devices, embedded industrial control systems, legacy network equipment – may require separate procurement cycles and multi-year device replacement programs that must be initiated during earlier phases to be ready by 2030. Enterprises should conduct hardware readiness assessments during Phase 1 and include PQC capability requirements in procurement specifications beginning in Phase 2, even before PQC deployment is required for those systems.

Phase 5 – Verification and Continuous Cryptographic Governance (2030 and beyond)

PQC migration is not a one-time project but a permanent shift in cryptographic governance. Phase 5 establishes the monitoring, audit, and governance processes that ensure cryptographic practices remain current as standards evolve, new vulnerabilities are discovered, and the threat landscape shifts. The NIST deprecation timeline – disallowing all quantum-vulnerable public-key algorithms by 2035 [14] – provides the hard deadline against which Phase 5 verification must demonstrate complete compliance. Organizations should also monitor the NIST PQC standardization pipeline for FIPS 206 (FN-DSA) finalization and HQC standardization, and evaluate whether their cryptographic portfolios should incorporate these additional standards for redundancy.

Cloud and Vendor Ecosystem Readiness

Enterprise PQC migration does not occur in isolation from the vendor ecosystem, and understanding the current state of cloud provider and tooling support is essential for migration planning. The major cloud hyperscalers have made substantial progress, though adoption remains uneven across service types.

Amazon Web Services has deployed post-quantum cryptography across a broad and growing range of customer-facing managed services. AWS deployed ML-KEM across customer-facing service endpoints by late 2025, with hybrid ECDH + ML-KEM TLS protection active across AWS KMS, Amazon S3, Amazon CloudFront, Application Load Balancers, Network Load Balancers, AWS Payments Cryptography, ACM (Certificate Manager), and Secrets Manager [17]. AWS Private CA supports ML-DSA for digital signatures, and AWS-LC (the open-source AWS cryptographic library) achieved FIPS 140-3 validation as

the first module to include ML-KEM. AWS has announced plans to complete ML-KEM deployment across all services with HTTPS endpoints and to remove legacy CRYSTALS-Kyber (pre-standard) support in 2026.

Microsoft has integrated ML-KEM and ML-DSA into SymCrypt, its primary cryptographic library, which underpins Windows, Azure, Microsoft 365, and related platforms [18]. Post-quantum cryptography APIs became generally available on Windows Server 2025 and Windows 11 through the November 2025 Windows update, and PQC support shipped as generally available in .NET 10. Azure Key Vault offers hybrid ECDH + ML-KEM key exchange, and Azure Entra incorporates hybrid key exchange in identity operations. Microsoft's stated strategic objective is quantum-safe security across its entire product and services portfolio.

Google Cloud launched quantum-safe key encapsulation mechanisms in Cloud KMS in preview in October 2025, using X-Wing KEM — a hybrid combining X25519 (classical) with ML-KEM-768 (post-quantum) [19]. Google also announced quantum-safe digital signatures in Cloud KMS. The company's open-source BoringCrypto and Tink cryptographic libraries include PQC implementations, giving developers building on Google Cloud infrastructure accessible paths to PQC integration. Full availability of PQC across Google Cloud infrastructure connections is expected by end of 2026 [19].

For enterprises, the practical takeaway is that managed cloud services are increasingly PQC-capable, and using those capabilities — even in hybrid mode — represents meaningful risk reduction with relatively low migration friction. Enterprises should audit their cloud configurations to confirm that PQC-capable TLS configurations are active where available, rather than defaulting to legacy classical settings that cloud providers continue to support for backward compatibility.

Sector-Specific Considerations

While the post-quantum migration imperative applies universally to any organization using public-key cryptography, certain sectors face distinct risk profiles, regulatory pressures, or operational constraints that warrant differentiated attention.

Financial services organizations sit at the intersection of several acute quantum risk factors: they hold high-value, long-term sensitive data (account credentials, transaction histories, client identities), operate critical shared infrastructure (SWIFT, payment card networks, clearinghouse systems) that would amplify any cryptographic failure, and face overlapping regulatory requirements from prudential regulators increasingly focused on quantum risk. The financial sector also has particular exposure to HNDL attacks targeting transaction records, merger and acquisition communications, and client identity

data. Guidance from financial regulators in the United States and European Union, as well as SWIFT's own PQC working group, should be monitored for mandates that may emerge before NSM-10's 2035 horizon.

Healthcare organizations face a distinct challenge: the sensitivity of patient health information under HIPAA, GDPR, and analogous regulations extends for decades, aligning directly with the confidentiality horizon most threatened by HNDL attacks. Medical device manufacturers face the additional constraint that cryptographic algorithms embedded in implantable or long-lifecycle devices may be non-updatable after deployment, requiring PQC algorithm selection before those devices ship. The FDA has already begun examining the cryptographic lifecycle of connected medical devices as part of its cybersecurity guidance for premarket submissions.

Government and defense contractors are subject to CNSA 2.0 and NSM-10 mandates that are neither voluntary nor aspirational — they are procurement prerequisites. Enterprises in the defense industrial base that do not have a credible PQC migration roadmap are exposed to contract loss and security clearance risk. Federal IT leadership surveys conducted in 2025 document broad awareness of these mandates across defense agencies, though implementation maturity varies considerably [24]. The CMMC (Cybersecurity Maturity Model Certification) framework is likely to incorporate PQC requirements in future revisions, further tightening the compliance pressure on defense contractors.

Critical infrastructure operators — electric utilities, water systems, transportation networks, telecommunications providers — face a specific challenge in that much of their operational technology (OT) and industrial control system (ICS) environments involves long-lifecycle equipment with limited or no mechanism for cryptographic algorithm updates, where firmware changes require extensive qualification and operational downtime. PQC migration for these environments requires proactive equipment procurement standards and may involve extended hybrid operation periods while legacy equipment is gradually replaced.

CSA Resource Alignment

The Cloud Security Alliance has developed an extensive body of guidance on quantum-safe security that provides direct support for enterprise PQC migration efforts. Organizations undertaking migration should treat CSA's existing Quantum-Safe Security Working Group outputs as primary reference materials rather than supplementary reading.

CSA's **Cloud Controls Matrix (CCM)** provides the governance framework for systematically assessing and mitigating quantum computing risks in cloud environments [22]. The July 2024 publication "Quantum-Safe Security Governance with the Cloud Controls Matrix" maps specific CCM control domains to quantum risk scenarios, identifying the highest-priority controls for cloud security practitioners. The following domains are most directly relevant to post-quantum migration:

CCM Domain	Code	PQC Migration Relevance
Cryptography, Encryption & Key Management	CEK	Algorithm selection and key lifecycle management; highest-priority domain
Governance, Risk & Compliance	GRC	Incorporate quantum risk scenarios into enterprise risk registers
Data Security & Privacy	DSP	Assess confidentiality horizon of sensitive data assets
Business Continuity & Operational Resilience	BCR	Address cryptographic infrastructure disruption scenarios
Supply Chain Management	STA	Evaluate vendor quantum readiness
Interoperability & Portability	IPY	Govern portability of cryptographic operations across cloud environments

The specific CCM control identifiers most directly relevant to PQC migration include CEK-03 (Cryptographic Key Generation), CEK-04 (Cryptographic Key Management), CEK-09 (Encryption Algorithm), CEK-10 (Encryption Change Management), and GRC-02 (Risk Management Program) [22]. Organizations conducting STAR assessments should evaluate their quantum readiness posture against these controls as part of the standard cloud security governance cycle.

Organizations deploying agentic AI systems should explicitly include PQC requirements in the security architecture of AI agent communication channels. AI agents that handle sensitive communications, manage key material, negotiate cryptographic parameters, or authenticate identities on behalf of users inherit the same cryptographic vulnerabilities as the underlying systems — and in autonomous operation, may do so without the human oversight that typically prompts security review. CSA's **MAESTRO framework** for agentic AI threat modeling provides a structured approach for identifying where these cryptographic vulnerabilities emerge within AI system architectures.

CSA's **Zero Trust guidance** reinforces PQC migration by making the explicit principle that network-layer encryption provides only provisional trust — a principle that aligns naturally with the HNDL threat model. Under Zero Trust architecture, the assumption that encrypted communications in transit are permanently private is already treated with skepticism; the quantum threat model formalizes this skepticism into a concrete risk with a definable timeline. Organizations implementing Zero Trust should treat PQC for data in transit as a core component of their trust enforcement model rather than a separate workstream.

CSA's "Practical Preparations for the Post-Quantum World" [21] remains the most comprehensive practitioner guide for enterprise PQC migration from a CSA perspective, providing a five-phase implementation framework, sample management communication templates, and vendor attestation questionnaires. The 2019 publication "Preparing Enterprises for the Quantum Computing Cybersecurity Threats" [23] offers foundational conceptual coverage relevant to executive education programs. Together these documents form a coherent corpus for organizations at all stages of PQC migration maturity.

Conclusions and Recommendations

The post-quantum migration imperative has arrived. The convergence of credible hardware timelines (Q-Day by 2030 per Forrester [1][2]), finalized and deployable standards (FIPS 203, 204, 205 as of August 2024 [3]), active regulatory mandates (CNSA 2.0, NSM-10), and an active HNDL threat from nation-state adversaries means that organizations which treat quantum risk as a future planning item rather than a present operational priority are accepting material, demonstrable risk to their most sensitive data. The 5% enterprise deployment rate confirmed by the May 2025 DigiCert survey [8] demonstrates that this risk is widely underacknowledged.

The recommendations for immediate action follow directly from the analysis.

CISOs and risk leaders should initiate a cryptographic inventory program in 2026 if one is not already underway. No meaningful migration planning is possible without knowing what needs to be migrated. This inventory must span the entire enterprise ecosystem including cloud services, supply chain dependencies, and hardware-constrained systems.

Security architects should adopt crypto-agility as a mandatory architectural standard for all new systems and modernization projects beginning immediately. The cost of building in algorithm agility during initial development is far lower than retrofitting it during migration. All new TLS implementations, key

management systems, and certificate infrastructure should be architected to support ML-KEM and ML-DSA alongside classical algorithms in hybrid mode.

Procurement and vendor management programs should begin requiring PQC roadmaps with specific delivery commitments from technology vendors, particularly HSM vendors, PKI solution providers, network equipment manufacturers, and cloud service providers. Vendors who cannot provide credible PQC commitments represent migration risk that must be factored into contract renewals and technology refresh cycles.

Security operations teams should re-examine data classification and retention policies through the lens of the HNDL confidentiality horizon. Data that must remain confidential for five or more years from the date of creation or transmission should be treated as subject to quantum-level risk and prioritized for quantum-safe re-encryption or migration – with data in the ten-or-more-year sensitivity range representing the highest-priority asset class for immediate action.

Boards and executive leadership should receive a quantum risk briefing that includes an enterprise-specific assessment of exposure, a proposed migration roadmap with cost estimates, and a clear statement of the regulatory compliance timeline. The federal government's estimate of $7.1 billion for its own migration [27] provides a reference point; enterprise costs will vary based on scale and architectural complexity.

The quantum transition is not unique in the history of cryptographic migration – the transitions from DES to AES and from SSL to TLS provide relevant precedents – but it is distinctive in scope, in the irreversibility of HNDL exposure for data already collected, and in the compressed interval between standards finalization and a credible threat materialization. Organizations that establish a funded, sequenced migration program in 2026 will preserve their options throughout the transition. Those that defer meaningful action to 2028 or beyond face a narrowing window in which to protect data already subject to HNDL collection.

References

[1] Brian Hopkins, Forrester Research, "Practical Quantum Computing By 2030 Is Likely — And So Is Q-Day," Forrester Blogs, March 11, 2026. https://www.forrester.com/blogs/practical-quantum-computing-by-2030-is-likely-and-so-is-q-day/

[2] Forrester Research, "The State Of Quantum Computing, 2026," Forrester Research, Inc., 2026 (referenced in [1]).

[3] National Institute of Standards and Technology, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," NIST News, August 13, 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[4] National Institute of Standards and Technology, Federal Information Processing Standard 203 (FIPS 203): Module-Lattice-Based Key-Encapsulation Mechanism Standard, August 13, 2024. https://csrc.nist.gov/pubs/fips/203/final

[5] National Institute of Standards and Technology, Federal Information Processing Standard 204 (FIPS 204): Module-Lattice-Based Digital Signature Standard, August 13, 2024. https://csrc.nist.gov/pubs/fips/204/final

[6] National Institute of Standards and Technology, Federal Information Processing Standard 205 (FIPS 205): Stateless Hash-Based Digital Signature Standard, August 13, 2024. https://csrc.nist.gov/pubs/fips/205/final

[7] National Security Agency, "NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems," NSA Press Room, September 2022. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/

[8] DigiCert / Propeller Insights, "Quantum Readiness Gap: DigiCert Study Finds Just 5% of Enterprises Have Quantum-Safe Encryption in Place," GlobeNewswire, May 8, 2025. https://www.globenewswire.com/news-release/2025/05/08/3077339/0/en/Quantum-Readiness-Gap-DigiCert-Study-Finds-Just-5-of-Enterprises-Have-Quantum-Safe-Encryption-in-Place.html

[9] Entrust / Ponemon Institute, "2026 Post-Quantum Cryptography Study," 2026 (survey data; full report via Entrust).

[10] Google, "Introducing Willow, our state-of-the-art quantum chip," Google Blog, December 9, 2024. https://blog.google/innovation-and-ai/technology/research/google-willow-quantum-chip/

[11] Acharya, et al., "Quantum error correction below the surface code threshold," Nature, Vol. 638, 2025. https://doi.org/10.1038/s41586-024-08449-y

[12] IBM, "IBM Delivers New Quantum Processors, Software, and Algorithm Breakthroughs on Path to Advantage and Fault Tolerance," IBM Newsroom, November 12, 2025. https://newsroom.ibm.com/2025-11-12-ibm-delivers-new-quantum-processors,-software,-and-algorithm-breakthroughs-on-path-to-advantage-and-fault-tolerance

[13] National Institute of Standards and Technology, SP 800-227: Recommendations for Key-Encapsulation Mechanisms, September 18, 2025. https://csrc.nist.gov/pubs/sp/800/227/final

[14] National Institute of Standards and Technology, NIST IR 8547 (Initial Public Draft): Transition to Post-Quantum Cryptography Standards, 2024/2025. https://csrc.nist.gov/pubs/ir/8547/ipd

[15] The White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems" (NSM-10), May 4, 2022. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[16] National Cybersecurity Center of Excellence (NCCoE), NIST SP 1800-38: Migration to Post-Quantum Cryptography (ongoing practice guide). https://www.nccoe.nist.gov/projects/migration-post-quantum-cryptography

[17] Amazon Web Services, "Post-Quantum Cryptography," AWS Security documentation, 2025–2026. https://aws.amazon.com/security/post-quantum-cryptography/

[18] Microsoft Corporation, "Quantum-safe security: Progress towards next-generation cryptography," Microsoft Security Blog, August 20, 2025. https://www.microsoft.com/en-us/security/blog/2025/08/20/quantum-safe-security-progress-towards-next-generation-cryptography/

[19] Google Cloud, "Announcing quantum-safe key encapsulation mechanisms in Cloud KMS," Google Cloud Blog, October 2025. https://cloud.google.com/blog/products/identity-security/announcing-quantum-safe-key-encapsulation-mechanisms-in-cloud-kms

[20] National Institute of Standards and Technology, NIST IR 8545: Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process (HQC selection), March 2025. https://csrc.nist.gov/pubs/ir/8545/final

[21] Cloud Security Alliance Quantum-Safe Security Working Group (Roger Grimes, lead), "Practical Preparations for the Post-Quantum World: Tasks Every Organization Should be Performing Now to Prepare," Cloud Security Alliance, 2021. https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

[22] Cloud Security Alliance Quantum-Safe Security Working Group (John Jiang, lead), "Quantum-Safe Security Governance with the Cloud Controls Matrix," v1.1, Cloud Security Alliance, July 30, 2024. https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

[23] Cloud Security Alliance Quantum-Safe Security Working Group (Edward Chiu, lead), "Preparing Enterprises for the Quantum Computing Cybersecurity Threats," Cloud Security Alliance, 2019. https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

[24] General Dynamics Information Technology, "Quantum Waves: Federal Perspectives on Post-Quantum Cryptography Readiness" (federal IT leader survey), 2025.

[25] McKinsey & Company, "The year of quantum: From concept to reality in 2025," McKinsey Technology, 2025. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025

[26] Executive Order 14306 (Trump administration), "Strengthening and Promoting Innovation in the Nation's Cybersecurity," June 6, 2025.

[27] Office of the National Cyber Director / Office of Management and Budget, "Report on Post-Quantum Cryptography," July 2024. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf

[28] National Institute of Standards and Technology, NIST FIPS 206 project page, NIST Computer Security Resource Center. https://csrc.nist.gov/pubs/fips/206