



Transitioning To **Quantum Cyber Readiness**

A white paper by **CERT-In**
in collaboration with **SISA**

TABLE OF CONTENTS

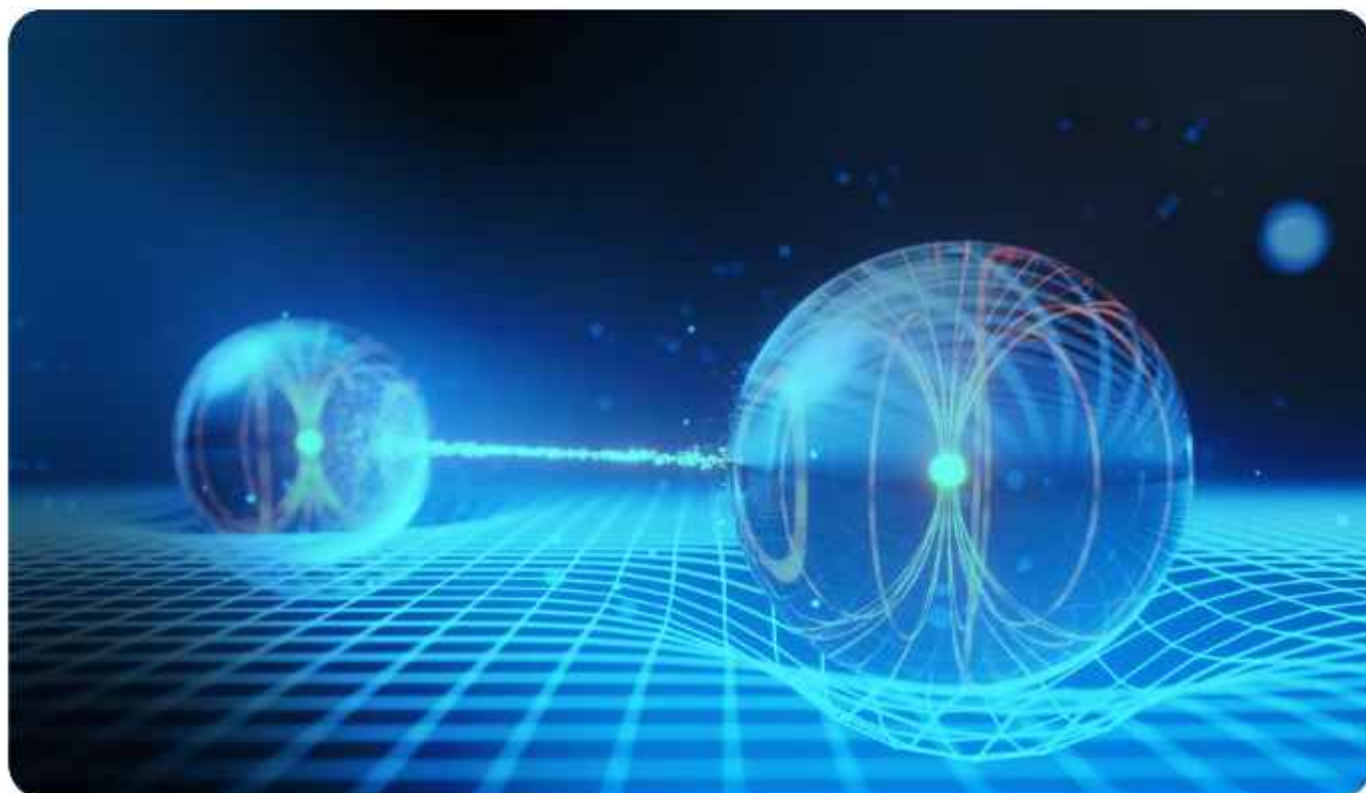
Background	03	03 Phased Organizational Rollout	32
Challenges	04	3.1 Groundwork & Discovery (Immediate)	33
Roadmap for quantum cyber readiness	07	3.2 Targeted Upgrades (Mid Term – 1 to 3 Years)	34
01 Foundational Assessment & Strategic Planning	08	3.3 Enterprise-Wide Deployment (Long Term – 3+ Years)	35
1.1 Risk Assessment & Cryptographic Inventory	09	04 Resilience, Monitoring & Futureproofing	37
1.2 Stakeholder & Governance Alignment	11	4.1 Crypto-Agile Architecture & Lifecycle Management	38
1.3 Quantum Bill of Materials (QBOM)	13	4.2 Continuous Monitoring & Compliance	38
1.4 Automated Cryptographic Discovery Tools	15	4.3 Quantum Key Distribution (QKD) Exploration	39
02 Technology Readiness & Capability Building	17	4.4 Quantum Networking and Communication Infrastructure	39
2.1 Hybrid Cryptography Adoption	18	4.5 Quantum Cyber Readiness Implementation	41
2.2 Testing, Validation & Vendor Collaboration	21	Conclusion	50
2.3 Infrastructure Evaluation & Upgrade Planning	22	References	51
2.4 AI-Enhanced Implementation and Management	30	Acronyms used	52

This whitepaper titled 'Transitioning to Quantum Cyber Readiness' has been written by The Indian Computer Emergency Response Team (CERT-In) in collaboration with SISA.

Background

Today, enhanced computation is being achieved by leveraging quantum mechanics through computational devices known as quantum computers. The quantum computing era is no longer a distant horizon, but a present-day inflection point with far-reaching implications for cyber security, digital infrastructure and technological leadership. The world is now on the brink of a transformation from a digital economy to a quantum economy.

The technology has matured and transitioned from the research labs to reality. Various players have announced their quantum ready products. Google's Willow chip (December 2024) achieved exponential error reduction with 105 qubits, demonstrating breakthrough quantum error correction. Microsoft's Majorana-1 processor launched in February 2025, designed to scale to a million qubits. IBM's quantum roadmap now targets fault-tolerant computing by 2029 with the Starling system. Quantinuum achieved industry-first 56-qubit trapped-ion quantum computers with record-breaking fidelity, while Nokia continues advancing quantum networking communications. The United Nations' has declared 2025 as the International Year of Quantum Science and Technology. The players in the quantum computing supply chain network are growing rapidly - whether in semiconductors, nanotechnology, integrated photonics, component manufacturing, hardware manufacturing, system software, application software, or services.



Challenges

Quantum computers can solve complex, intractable mathematical problems - and perform tasks in machine learning, optimization, and logistics - orders of magnitude faster than classical or conventional computers. While quantum computers offer significant advantages, they also pose a serious threat to current encryption algorithms by breaking asymmetric cryptographic protocols such as Rivest-Shamir-Adleman (RSA). This makes all encrypted data immediately vulnerable, jeopardizing the digital economy by putting the confidentiality and integrity of data at risk. The type of risks includes data breaches involving financial and health data, internet traffic and instant messaging, digital certificates, digitally signed documents, blockchains, cryptocurrencies and the risk of "harvest now, decrypt later" attacks by malicious cyber actors. This is a global single point of failure. Digital certificates, secure key exchanges, blockchain protocols, secure messaging and identity management, all rely on encryption standards that quantum computing will be able to dismantle.

To build resilience against quantum computing risks,
there is a need to:

Develop a better understanding of the issue, the risks involved, and strategies to mitigate those risks.



Develop a plan for mitigating quantum computing risks and implementing quantum-resistant encryption.

Assess quantum computing risks in the Business Domain.

Adding to the challenge is a widespread lack of cryptographic visibility. In a world racing toward post-quantum cryptography, such blind spots are not just risky, but untenable. The migration to quantum resilience will require not only new algorithms, but an enterprise-wide transformation of key management, information and certificate infrastructure, software development and supply chain coordination.

Transitioning to post-quantum cryptography (PQC) is complex because it requires organizations to replace foundational public-key algorithms, used in TLS, VPNs, digital signatures, and key exchanges, with entirely new mathematical constructs. Upgrading existing ICT infrastructure to be quantum-safe using PQC algorithms often involves larger key sizes, higher computational overhead, and integration challenges, especially across legacy and resource-constrained systems. Additionally, the evolving nature of PQC standards, vendor readiness gaps and global interdependencies make coordination and implementation significantly more demanding at both the technical and organizational levels. Hence, the migration to quantum cyber ready needs to begin immediately.

Depending on an organization's risk appetite and posture, the transition to quantum-safe cryptography can be evaluated using three key parameters:

Shelf-life time (X)

The number of years the data must remain secure. For instance, in the financial sector, this is typically 5 to 10 years.

Migration time (Y)

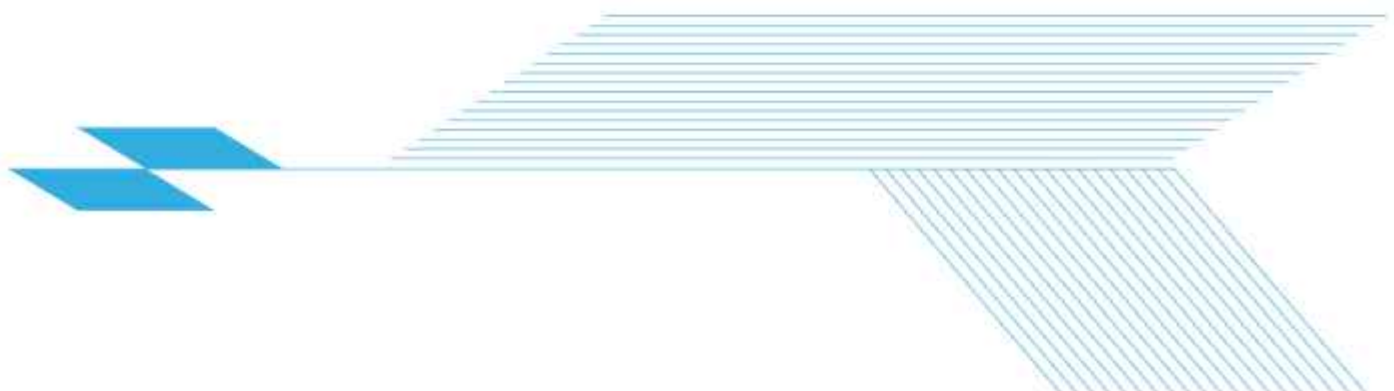
The estimated time required to safely transition the organization's systems to a quantum-safe framework. Depending on the size and complexity of the ICT infrastructure, this can range from 6 months to 3 years.

Threat timeline (Z)

The estimated number of years until cryptographically relevant quantum computers (CRQCs) become available to threat actors; predicted to be within the next 3 to 5 years (around 2028 to 2030).

Organizations can apply Mosca's Theorem: $X + Y > Z$.

If the sum of the data shelf-life and migration time exceeds the expected arrival of CRQCs, the risk becomes urgent. In such cases, organizations must act now to begin their transition to quantum-safe cryptography.



A Harvest Now, Decrypt Later (HNDL) Attacks

A.1. Current Threat Status:

The quantum threat is not merely future-oriented; it represents an immediate risk through "Harvest Now, Decrypt Later" (HNDL) attacks. These attacks involve adversaries collecting and storing encrypted data today with the intention of decrypting it once quantum computers become capable of breaking current cryptographic systems.



Nation-states and sophisticated threat actors are likely already harvesting and storing encrypted data, anticipating future quantum decryption capabilities.



Executive Order 14144, issued January 16, 2025, formally ordered U.S. governmental departments to start post-quantum cryptography transitions within specified timeframes (60-270 days).



Any data requiring protection beyond 2030 should be considered at immediate risk.

A.2. Risk Categories:



Critical Risk

Long-term sensitive data with 10+ year confidentiality requirements.



High Risk

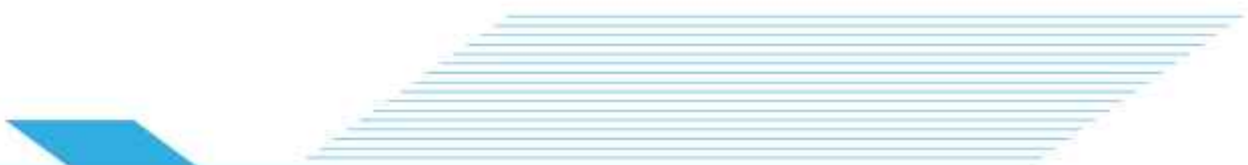
Financial records, healthcare data, government secrets, intellectual property, legal documents.



Medium Risk

Corporate communications, customer databases, research data.

Organizations must understand that the quantum threat clock started ticking the moment sensitive data was first transmitted or stored using quantum-vulnerable encryption. The threat is immediate for any information that must remain confidential beyond the estimated arrival of cryptographically relevant quantum computers.



Roadmap for quantum cyber readiness

Transitioning to quantum-resistant cryptographic solutions may introduce challenges, including interoperability issues, performance concerns, regulatory compliance and financial implications. However, by adopting a structured approach to quantum-safe migration, organisations can mitigate risks while ensuring a smooth transition through a phased strategy comprising of following 4 phases:

01



Foundational Assessment & Strategic Planning.

03



Phased Organizational Rollout.

02



Technology Readiness & Capability Building.

04



Resilience, Monitoring & Futureproofing.

Each of the phases is further detailed in the subsequent sections.



01

Foundational Assessment & Strategic Planning

A structured methodology for identifying, classifying and prioritizing systems vulnerable to quantum threats should be identified. Before transitioning to quantum-safe cryptography, organizations must establish a strong foundation through detailed assessment and strategic planning. This preparatory stage brings visibility into where quantum-vulnerable cryptography resides, how it functions within the environment and which components demand immediate focus. This can be achieved by making an inventory often referred to as a Cryptographic Bill of Materials (CBOM), of the components. Without this baseline, migration efforts risk becoming inefficient, disjointed, or unsuccessful.

1.1

Risk Assessment & Cryptographic Inventory

A critical first step in achieving a quantum-safe migration is conducting a comprehensive inventory and assessment of all cryptographic dependencies within the organization's environment. This process involves identifying all cryptographic assets, such as encryption algorithms, certificates, keys, protocols and cryptographic libraries in use. The assessment should also include locating databases, applications, devices and infrastructure components where cryptography is deployed. This can be achieved through automated discovery tools or manual assessments to ensure a complete and accurate view of the cryptographic landscape.

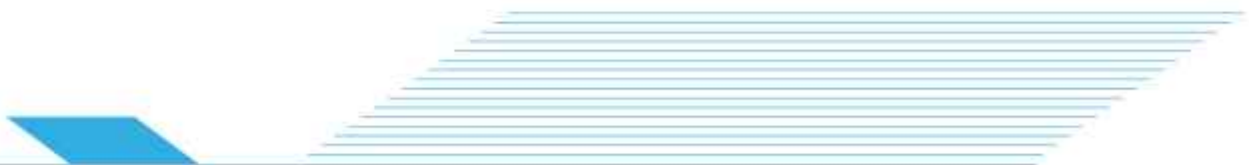
1.1.1

Audit of Applications, Devices, Protocols, Data Flows

To effectively transition to quantum-safe cryptography, organizations must first develop a comprehensive understanding of where and how encryption is currently used. This includes evaluating applications, devices, communication protocols, data flows and cryptographic assets. All applications whether developed in-house or sourced from third parties should be assessed for the encryption libraries they use, the algorithms implemented and key management practices, particularly within Transport Layer Security/Secure Sockets Layer (TLS/SSL), application program interfaces (APIs), cloud environments and virtual private networks (VPNs).

Devices such as servers, endpoints, mobile devices, Internet of Things (IoT) systems and Supervisory Control And Data Acquisition (SCADA) components should be reviewed for embedded encryption mechanisms and the presence of secure hardware modules like Hardware Security Models (HSM). Key communication protocols including TLS, SSH, IPsec and blockchain consensus algorithms must be scrutinized for their algorithmic strength, cipher suite settings and certificate handling.

Equally vital is the mapping of data flows across the organization, both in storage and in transit, to identify weak points or legacy encryption. A detailed inventory of cryptographic files such as pem, .key, .crt, .pfx and .p12 is crucial, with particular attention to PKCS #12 formats that package private keys and certificates together. This level of visibility helps organizations determine which systems need urgent updates, which can be retained securely, and how to strategically plan and prioritize their migration to quantum-resistant cryptographic solutions.



1.1.2

Identification of Quantum-Vulnerable Assets

Identifying quantum-vulnerable assets is a crucial milestone in any organisation's journey toward achieving quantum-safe cryptography. Once the discovery and inventory of cryptographic components are complete, the next step is to identify systems and processes that rely on algorithms vulnerable to quantum attacks. This step lays the groundwork for prioritizing remediation efforts based on exposure and criticality.

The highest risk areas include public-key algorithms such as Rivest–Shamir–Adleman (RSA), Digital Signature Algorithm (DSA), Diffie-Hellman (DH), Elliptic Curve Digital Signature Algorithm (ECDSA), Elliptic Curve Diffie-Hellman (ECDH), which are directly threatened by Shor's algorithm. Symmetric cryptography, though more resilient, still faces reduced security for example, Grover's algorithm reduces the strength of symmetric cryptography by as much as half; i.e. AES 256 = AES 128, AES 128 = AES 64. Attention must also be given to protocols like TLS, VPNs, secure email and PKI systems, particularly where outdated cipher suites or key exchange methods are still in use.

Additional red flags include hardcoded keys and certificates that are difficult to replace, legacy systems running outdated or unsupported cryptographic libraries and key infrastructure components like PKI hierarchies and root Certificate Authority (CAs). These elements form the trust backbone of enterprise security and must be addressed early in the quantum-safe migration plan to avoid systemic vulnerabilities.

1.1.3

Categorization by Risk Level and Data Longevity

Migrating to quantum-safe cryptography does not mean replacing everything at once. A risk-based approach is needed that considers how sensitive the data is, how long it needs to be protected and what level of risk is involved. This ensures that critical areas are addressed first, while lower-risk components are managed more gradually and efficiently.

Three main factors guide this prioritization:

Risk level: High-risk systems are those exposed to the internet or handling sensitive data such as Personally Identifiable Information (PII), requiring strict compliance. Medium-risk systems are internal but can still impact business operations. Low-risk systems typically handle short-term or non-sensitive data.

Data longevity: Data that needs to remain secure for over 10 years—such as medical records or intellectual property—requires immediate protection against quantum threats. Short-lived data may not necessitate urgent changes.

Compliance: Systems governed by Indian and global regulations must align cryptographic upgrades with applicable compliance requirements.

By classifying cryptographic assets along these lines, organizations can structure a phased migration focusing first on high-risk, long-term and compliance-driven areas. This ensures that quantum readiness strengthens existing security and compliance programs without unnecessary disruption or resource strain.



Enhanced Risk Assessment Framework:

With the emergence of HNDL attacks, organizations must reassess their risk categorization to include temporal factors:



Immediate Risk (0-2 years)

Data currently transmitted or stored that attackers may be harvesting now for future decryption.



Short-term Risk (2-5 years)

Systems and data that will be vulnerable once early quantum computers become available to adversaries.



Long-term Risk (5+ years)

Infrastructure and processes that must be quantum-safe before mature quantum computers become widespread.

This temporal risk assessment must be integrated with data sensitivity classification to prioritize migration efforts effectively.

1.2

Stakeholder & Governance Alignment

This phase is about securing top-down commitment and cross-functional alignment to ensure the organisation is truly prepared for the shift to quantum-safe cryptography. It's not just a technical fix but a strategic transformation that reshapes how people, processes, and technology work together to protect the business in the long term.

A key priority is educating executive leadership about the real risks of quantum computing and ensuring they understand that preparing for it is a business-critical initiative. Strong executive sponsorship enables the organization to unlock the resources, focus, and momentum needed to drive meaningful change. At the same time, departments must coordinate closely to avoid working in silos, ensuring every team from IT and security to legal and compliance is on the same page.

Governance structures, risk frameworks and regulatory obligations must all be built into the planning process, early on. Defining clear accountability and tracking progress across teams is essential. Without strong leadership and collaboration, even the best technical plans can lose momentum. Building organizational readiness today lays the foundation for a smooth, well-managed migration to a quantum-resilient future.



1.2.1

Executive Awareness

Though quantum computing might still seem distant to many in the boardroom, its threat to today's cryptographic systems is becoming increasingly urgent. One of the first and most important steps toward readiness is ensuring that executive leaders understand quantum risk not as a technical issue, but as a strategic business threat that could impact compliance, continuity, competitiveness and reputation.

To build this awareness, leaders should be briefed with focused, impactful sessions that explain what quantum threats are, how they can disrupt the business and why action is needed now.

Early action is essential, as cryptographic migration can take a significant time. Gaining executive buy-in means securing funding, embedding quantum-safe efforts into enterprise security strategies and aligning policies and procurement. This awareness-building is not a one-time effort but evolves with ongoing advances in quantum technology, cryptographic standards and regulations. Sustained leadership engagement ensures the organization stays ahead of the threat curve and is prepared for a secure, quantum-resilient future.

1.2.2

Cross-Functional Task Force

A successful quantum-safe migration requires coordinated collaboration across the entire enterprise, rather than isolated efforts by individual teams. Operating in departmental silos increases the risk of inconsistent implementations, missed compliance requirements and duplicated work. Establishing a dedicated cross-functional task force or steering committee is essential to unify strategy, execution and oversight.

This task force should bring together key stakeholders across the organization: cybersecurity and cryptography experts to lead technical remediation; IT and DevOps teams to manage infrastructure updates and ensure compatibility; legal and compliance personnel to oversee regulatory alignment; risk managers to prioritize actions based on business impact; and enterprise architecture and procurement teams to address third-party and lifecycle dependencies. An executive sponsor, typically the CISO, should champion the initiative, secure funding, and align it with the organization's strategic goals.

Core responsibilities include identifying priority systems, managing risks and keeping leadership informed through structured updates. To ensure accountability, the task force must define clear roles, deliverables and reporting mechanisms. Engaging external advisors such as PQC vendors, standards contributors and auditors adds further rigor and validation. This governance model ensures that the migration is transparent, compliant and effectively integrated across the organization.



1.2.3

Regulatory Alignment

Ensuring compliance is a core pillar of any post-quantum migration strategy, especially as regulatory frameworks across industries begin to introduce expectations around quantum-readiness. Acting early allows organizations to stay audit-ready, avoid future legal pitfalls and gain a strategic edge by demonstrating foresight and operational maturity.

The first step is to identify which national and international regulations apply, based on the organization's industry and data footprint. It is equally important to monitor evolving guidance from standards bodies and engage with sector-specific forums to stay ahead of the curve. Comprehensive documentation including cryptographic inventories, quantum risk assessments and migration plans must be maintained to support governance, audits and regulatory reporting.

1.3

Quantum Bill of Materials (QBOM)

Once quantum-vulnerable cryptographic assets have been identified and categorized, the next critical step is to build a centralized, living inventory - known as a Quantum Bill of Materials (QBOM). This document acts as the backbone of the quantum-safe migration strategy, detailing every cryptographic component across the organization along with its quantum exposure, role in operations and readiness for transition.

It supports key initiatives including risk prioritization, procurement decisions that demand post-quantum compatibility, upgrade planning and compliance audits. It also ensures teams are working from a consistent, authoritative source of information.

When embedded into the organization's broader enterprise architecture and governance frameworks, it brings structure, accountability, and transparency to every stage of the post-quantum migration. This ensures that cryptographic modernization efforts are efficient, compliant, and resilient to future threats.



1.3.1

Crypto Asset Documentation

Creating a reliable Quantum Bill of Materials (QBOM) is a foundational step in managing the complexity of the transition to post-quantum cryptography. Built from the initial cryptographic inventory, the QBOM serves as a continuously updated reference that documents the location, usage and quantum risk level of every cryptographic element across the organization.

Each QBOM entry should capture key fields such as the asset identifier, cryptographic function (e.g., encryption, digital signature), algorithm and key size, usage context (e.g., TLS, VPN), library or module used (e.g., OpenSSL, Microsoft CryptoAPI) and key management details (e.g., PKI integration, expiration). Importantly, it should include a quantum risk rating and current migration status to track upgrade progress over time.

Beyond cataloguing technical details, the QBOM brings strategic value by enabling clear risk prioritization, system ownership and lifecycle planning. It ensures cryptographic assets are not only visible but also actionable helping teams coordinate remediation, align vendor expectations and meet regulatory demands. When integrated into governance and procurement processes, a well-maintained QBOM becomes a vital tool for building a secure, compliant and quantum-resilient enterprise.

1.3.2

Phased Upgrade Planning

The QBOM plays a central role, not just in documenting cryptographic assets, but in guiding a structured, phased migration to quantum-safe alternatives. By aligning upgrade priorities with quantum risk levels, system criticality and data sensitivity, organizations can reduce operational disruption while maintaining compliance and business continuity. This method ensures that the most exposed and impactful assets are addressed first, rather than attempting a costly, organization-wide overhaul all at once.

The recommended phased strategy begins with immediate risk mitigation, focusing on high-risk assets like internet-facing systems using RSA, ECDSA, or ECDH. Hybrid cryptographic approaches (e.g., RSA + Kyber) can help ease the transition while maintaining compatibility. The second phase, targets internal systems and cryptographic libraries that pose medium risk, followed by long-term modernization efforts involving long-lived data, archives and legacy systems such as IoT and SCADA. The final phase emphasizes continuous monitoring reviewing the QBOM regularly and integrating quantum-readiness checks into Continuous Integration / Continuous Deployment pipelines and audit processes.

This QBOM-driven, phased migration model ensures repeatability, reduces last-minute fixes and supports ongoing compliance efforts. It aligns with guidance from standards bodies like NIST while embedding long-term cryptographic agility into enterprise architecture and positioning organizations to adapt quickly as quantum threats evolve.

1.4

Automated Cryptographic Discovery Tools

As organizations move beyond initial discovery and pilot phases, the focus should shift to systematically upgrading high-risk, business-critical systems over a strategic 1–3-year transition period. Key priorities include migrating externally facing applications, long-lived data stores and authentication systems, while refining processes based on pilot insights. Staying adaptable to evolving PQC standards, vendor timelines and performance feedback is essential. This measured approach ensures a secure, resilient and low-risk expansion of quantum-safe cryptographic capabilities across core enterprise systems.

1.4.1

Manual cryptographic inventory creation is time-consuming and error-prone. For example, CISA's strategy for automated Post-Quantum Cryptography discovery and inventory tools provides a framework for systematic, technology-assisted discovery:

Automated Discovery Benefits:

-  Comprehensive scanning of network traffic, applications, and systems
-  Real-time identification of cryptographic dependencies
-  Continuous monitoring for new cryptographic implementations
-  Integration with existing security tools and SIEM systems

Implementation Approach:

-  Deploy network scanning tools to identify TLS configurations and certificate usage
-  Implement application scanning for embedded cryptographic libraries
-  Use code analysis tools to identify cryptographic API calls and implementations
-  Establish continuous monitoring for cryptographic drift and unauthorized changes

AI-Enhanced Risk Assessment:

-  Machine learning algorithms for pattern recognition in cryptographic usage
-  Automated risk scoring based on algorithm type, key length, and usage context
-  Predictive analytics for migration planning and resource allocation
-  Intelligent recommendations for upgrade prioritization

1.4.2

Dynamic QBOM Management

The traditional static approach to QBOM creation must evolve to support dynamic, continuously updated inventories:

Real-Time Updates:

Integration with Continuous Integration/Continuous Deployment (or Delivery) (CI/CD) pipelines for automatic QBOM updates

Cloud-native discovery for containerized and serverless environments

API-driven inventory management with automated change detection

Integration with IT asset management and configuration management databases

AI-Driven Analysis:

Natural language processing for documentation analysis and gap identification.

Intelligent grouping and categorization of cryptographic assets.

Automated compliance checking against organizational policies and regulatory requirements.

Risk correlation analysis across interconnected systems.





02

Technology Readiness & Capability Building

This phase focuses on the adoption of hybrid cryptography as a transitional strategy to bridge existing classical systems with emerging post-quantum cryptographic (PQC) solutions, while simultaneously building organizational capability and expertise.

Transitioning to post-quantum cryptography requires more than just awareness and planning. It calls for a mature, adaptable technology foundation capable of securely integrating quantum-resistant algorithms alongside existing legacy cryptographic infrastructure. This includes preparing and updating:



Software libraries (e.g., OpenSSL, Bouncy Castle, liboqs)



Communication protocols (e.g., TLS, SSH, VPN)



Enterprise platforms (e.g., cloud environments, operating systems)



Skilled personnel capable of maintaining and evolving these systems over time.

2.1

Hybrid Cryptography Adoption

A hybrid cryptographic approach provides a strategic pathway for organizations transitioning to quantum-safe security by integrating both classical and quantum-resistant algorithms during the migration phase. This ensures backward compatibility with existing systems while gradually introducing post-quantum cryptographic (PQC) standards.

2.1.1

Classical + PQC for Resilience

By combining traditional encryption methods such as RSA, ECC and AES with emerging quantum-resistant algorithms like Kyber, Dilithium and Falcon, organizations can mitigate the risks of sudden cryptographic failures while maintaining secure operations. This approach is particularly beneficial for industries with long-term data protection requirements, such as finance, healthcare and government sectors.

However, implementing hybrid cryptography comes with challenges, including performance overhead, interoperability concerns, and increased complexity in key management. Organizations must ensure that their existing security infrastructure, hardware security modules (HSMs) and cryptographic libraries can support hybrid models without introducing vulnerabilities. Rigorous testing and validation are essential to evaluate the impact on system performance and ensure seamless integration. Additionally, working with vendors, cloud providers and industry bodies will help ensure compliance with emerging PQC standards. By adopting a phased hybrid approach, organizations can minimize disruptions while gradually enhancing their cryptographic resilience against quantum threats.

2.1.2

Legacy Compatibility

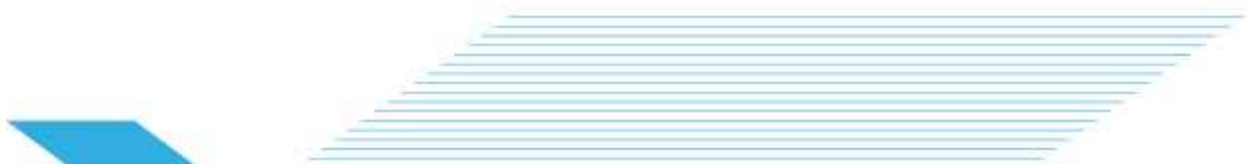
One of the most significant challenges in any cryptographic migration is supporting legacy systems that are not yet capable or may never be able to handle modern algorithm types. These limitations often arise from hardware constraints, outdated cryptographic libraries, or vendor lock-in, making a full replacement strategy complex and high-risk.



Upgrade cryptographic libraries and security tools to support dual-mode encryption (classical + PQC).



Work with hardware security module (HSM) vendors and certificate authorities (CAs) to adopt hybrid cryptographic models.



2.1.3

Pilot
Implementations

Pilot projects provide a low-risk, high-learning opportunity to gain hands-on experience with hybrid cryptography and post-quantum primitives. They help validate technical feasibility, measure performance impacts and identify integration challenges before enterprise-wide deployment.



Begin implementing PQC algorithms in environments handling long-term sensitive data, such as government archives, financial transactions and healthcare records.



Test performance trade-offs between classical and quantum-resistant encryption to optimize for real-world use cases.

It is important to note that TLS is currently in the process of being upgraded globally. During this transition phase, organizations may need to consider bridge solutions that apply quantum-safe post-quantum cryptography (PQC) algorithms at the application layer. This approach encrypts the data end-to-end without modifying the TLS stack, RSA, Diffie-Hellman (DH), Public Key Infrastructure (PKI), or the application logic itself. Application-layer encryption could ensure that even if TLS is broken at some point in time, the core data remains safe. This could act as an interim or bridge approach which allows hybrid encryption and an intermediary step to complete PQC migration, achievable in a very short duration of time.




2.1.4

Algorithm Diversification Strategy

The selection of Hamming Quasi-Cyclic (HQC) as NIST's fifth post-quantum algorithm introduces the concept of cryptographic diversification based on different mathematical foundations:

Mathematical Diversity Benefits:



Module Lattice – Key Encapsulation Mechanism (ML - KEM) (lattice-based) + HQC (code-based) provides protection against algorithm-specific attacks.



Reduced risk from potential cryptanalytic breakthroughs affecting single algorithm families.



Different performance characteristics allow optimization for specific use cases.

Implementation Strategy:



Deploy ML-KEM as primary algorithm for most applications.



Implement algorithm negotiation protocols for automatic fallback.




Use HQC as backup for highest-security applications.



Establish monitoring for algorithm-specific vulnerabilities.

Performance Optimization:



ML-KEM: Faster operations, smaller key sizes for bandwidth-constrained environments.



Dynamic algorithm selection based on network conditions and security requirements.



HQC: Larger keys but different security assumptions for ultra-high-security applications.



2.2

Testing, Validation & Vendor Collaboration

Organizations must rigorously test and validate Post-Quantum Cryptography (PQC) implementations before deploying them into production environments to ensure security, performance and interoperability. Given that PQC algorithms introduce larger key sizes, increased computational overhead and potential integration challenges, it is crucial to conduct controlled pilot deployments in test environments. These pilots should evaluate algorithm efficiency, key management mechanisms and the impact on existing encryption workflows. Testing should also include compatibility assessments with legacy systems, network infrastructure and cryptographic libraries to prevent disruptions during full-scale adoption.

Additionally, collaborating with industry vendors, cybersecurity experts and cloud providers can help organizations align their PQC implementation with emerging NIST, ISO and IEEE standards. Performance benchmarking should measure latency, encryption speed and system resource utilization to optimize cryptographic transitions. Organizations must also conduct security audits, penetration testing and risk assessments to identify vulnerabilities before widespread deployment. By taking a phased and methodical approach to PQC testing, businesses can ensure a smooth transition to quantum-resistant encryption while maintaining operational stability and compliance.

2.2.1

PQC Sandbox Testing

Creating a controlled testing environment or sandbox is a critical step in preparing for PQC deployment in production systems. A well-designed sandbox allows organizations to evaluate new cryptographic algorithms and integration patterns without risking disruption to live environments.



Establish test environments or sandboxes to deploy and evaluate PQC algorithms.

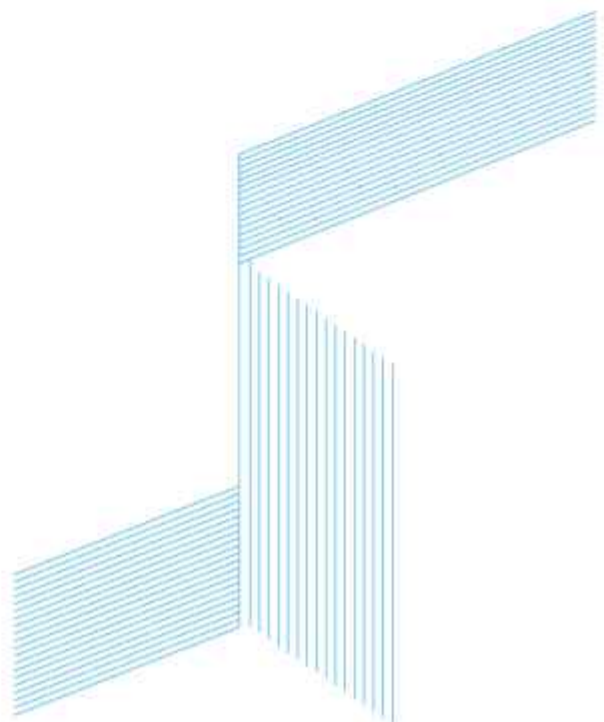


Implement quantum-safe encryption in non-critical applications first, analysing integration challenges.



AI-Enhanced Testing Framework: Modern sandbox testing should incorporate artificial intelligence to accelerate validation and optimization:

- Automated performance benchmarking across multiple algorithm combinations.
- Machine learning-based anomaly detection for cryptographic implementations.
- AI-driven load testing and stress analysis for hybrid configurations.
- Intelligent test case generation for edge conditions and failure scenarios.



Quantum-Classical Hybrid Testing:



Test Quantum Processing Unit (QPU) integration with classical processing units for specialized cryptographic operations.



Validate AI-enhanced key management and algorithm selection.



Assess quantum-safe algorithm performance under varying network conditions.



Evaluate integration with existing security infrastructure and monitoring systems.

2.2.2

Vendor Engagement

Vendors can play a critical role in the success of any cryptographic migration. From network appliances and endpoint security tools to Software as a Service (SaaS) platforms, certificate authorities and hardware vendors, third-party technologies must align with your organization's PQC adoption timeline and architectural strategy.

Failure to account for vendor cryptographic dependencies can lead to integration delays, security blind spots and compliance gaps. Early and structured engagement ensures alignment, reduces disruption and promotes collective momentum in the broader supply chain.



Work closely with security solution providers, cloud service providers and cryptographic hardware vendors to ensure compatibility.



Validate compliance with NIST PQC standards before full-scale deployment.

2.3

Infrastructure Evaluation & Upgrade Planning

Supporting quantum-safe cryptography (QSC) requires a careful assessment and modernization of enterprise infrastructure to ensure that performance and reliability are not compromised. The adoption of post-quantum algorithms introduces increased demands on computational resources, larger key sizes and greater bandwidth and storage requirements, posing new challenges for existing systems.

To enable a smooth and effective transition, organizations must go beyond software readiness and thoroughly evaluate the underlying hardware, cryptographic modules and infrastructure components.



2.3.1

Compute and Storage Audits

Post-quantum algorithms especially lattice-based schemes such as ML - KEM and Module Lattice – Digital Signature Algorithm (ML - DSA) introduce larger cryptographic payloads and significantly increased computational demands. Preparing infrastructure for these changes is essential to maintain performance, scalability and user experience.

To prepare for quantum-safe cryptography, organizations should assess infrastructure across CPU, memory, network, storage and scalability. This includes evaluating hardware readiness for PQC workloads, network impact from larger keys and certificates, storage demands for encrypted data and logs and the ability of cloud environments to scale without performance loss. The outcome should be a gap analysis identifying components needing upgrades and areas at risk of PQC-related slowdowns, ensuring a smooth and stable transition.

2.3.2

HSM and Server Upgrade Plans

Hardware Security Modules (HSMs), Trusted Platform Modules (TPMs) and crypto-accelerated servers form the backbone of enterprise cryptography. However, most legacy hardware does not natively support post-quantum algorithms, making hardware evaluation and upgrade planning a critical component of quantum-safe migration.

Organizations should review current HSMs for PQC or hybrid algorithm support, confirm vendor upgrade plans and ensure Federal Information Processing Standards (FIPS) 140-3 alignment. Server firmware must support extended key sizes, secure boot and updated hardware RNGs or secure enclaves.

Dedicated test environments using PQC-compatible stacks (e.g., OpenSSL + LibOQS) should simulate real-world usage and certificate handling. Procurement policies must mandate PQC readiness and vendor transparency. A phased, risk-based upgrade strategy should begin with critical, public-facing systems and expand to internal, IoT and industrial assets enabling cost-effective, low-disruption adoption of quantum-safe infrastructure.

2.3.3

Backup/ Recovery Readiness

In many organizations, backup and disaster recovery (DR) systems are inadvertently overlooked during cryptographic modernization. This creates a critical blind spot, as these systems often contain large volumes of sensitive data protected by legacy encryption that is vulnerable to quantum attacks.

To achieve full cryptographic resilience, organizations must include backup and disaster recovery (DR) systems in their quantum-safe transition plans. This involves auditing backup encryption schemes for quantum-vulnerable algorithms, testing data restores using PQC or hybrid keys and ensuring integration with modern key vaults and recovery workflows. Long-term backups should be re-encrypted if retention exceeds 7–10 years to prevent future decryption failures or "harvest now, decrypt later" risks. DR sites must mirror the primary site's cryptographic setup, including HSMs, libraries and PQC-ready applications. Addressing these areas ensures end-to-end data protection and regulatory compliance in the post-quantum era.

2.3.4

Quantum Random Number Generation (QRNG) Implementation

Background and Importance

Cryptographic security fundamentally depends on the quality of random number generation for key creation, nonce generation, and other security-critical operations. As organizations transition to post-quantum cryptography, the need for high-quality entropy becomes even more critical, as PQC algorithms often require larger key sizes and more random data than classical algorithms.

Quantum Random Number Generators (QRNGs) leverage quantum mechanical processes to produce true randomness, offering provably unpredictable random numbers that cannot be reproduced or predicted, even with complete knowledge of the generation process. Unlike pseudo-random number generators (PRNGs) that rely on mathematical algorithms, QRNGs harness quantum phenomena such as photon detection, quantum tunnelling, or vacuum fluctuations to generate genuinely random data.

Security Enhancement for Quantum-Safe Systems

Strengthening Cryptographic Foundations: QRNGs provide enhanced security for both current cryptographic systems and post-quantum implementations:



High-quality random numbers for generating stronger cryptographic keys in ML-KEM, ML-DSA, and SLH-DSA implementations.



Unpredictable values for cryptographic protocols that require unique, non-repeating inputs.



True randomness for encryption algorithms and secure communication protocols.



Enhanced entropy for signature generation in post-quantum digital signature schemes.

Addressing PQC Requirements:

Post-quantum algorithms often have more stringent randomness requirements compared to classical cryptography:

Larger key sizes requiring more random bits for secure key generation.

Lattice-based algorithms (ML-KEM, ML-DSA) that benefit from high-quality entropy for parameter generation.

Hash-based signatures (SLH-DSA) requiring significant amounts of random data for secure implementation.

Implementation Considerations

QRNG Integration Options:

Hardware-Based Implementation:



Dedicated QRNG Devices

Standalone quantum random number generators for high-security applications.



HSM Integration

Incorporation of QRNG capabilities into Hardware Security Modules for centralized key management.



Network-Accessible QRNGs

Centralized QRNG services accessible across organizational infrastructure.



Chip-Level Integration

QRNG capabilities embedded in processors and cryptographic accelerators.

Performance and Scalability:



Generation Rate

Assess QRNG output rates against organizational randomness consumption requirements.



Quality Assurance

Implement continuous testing and validation of QRNG output quality.



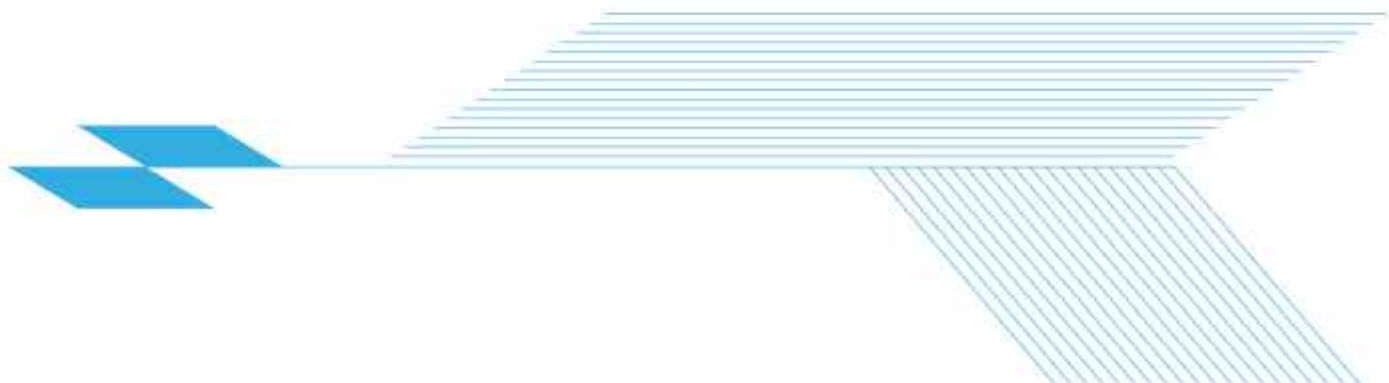
Backup Mechanisms

Maintain conventional entropy sources as backup for QRNG systems.



Distribution Architecture

Design secure distribution of quantum-generated random data across systems.



Technical Evaluation Criteria

QRNG Technology Assessment:



Photonic QRNGs

Based on photon detection and quantum superposition states.



Quantum Tunneling QRNGs

Using quantum tunneling effects in semiconductor devices.



Vacuum Fluctuation QRNGs

Leveraging quantum vacuum noise for randomness generation.



Quantum Phase Noise QRNGs

Exploiting quantum phase fluctuations in laser systems.

Compliance and Certification:



NIST SP 800-90 Compliance

Ensure QRNG outputs meet NIST statistical randomness requirements.



FIPS 140-2 Validation

Integration with FIPS-validated cryptographic modules and systems.



Common Criteria Evaluation

Assessment against international security evaluation standards.



Industry Standards

Compliance with relevant quantum technology and cryptographic standards.



Deployment Strategy

Phased QRNG Implementation:

Phase 1

Critical Systems (Immediate)



Deploy QRNGs for highest-security applications including government classified systems, financial transaction processing, and critical infrastructure control systems.



Integrate with HSMs and key management systems for enhanced cryptographic key generation.



Implement for post-quantum algorithm implementations requiring high-quality entropy.

Phase 2

Enterprise Systems (1-2 Years)



Extend QRNG deployment to enterprise cryptographic infrastructure and secure communication systems.



Integrate with PKI systems and certificate authorities for enhanced digital certificate security.



Deploy for VPN concentrators, secure email systems, and other enterprise security applications.

Phase 3

Comprehensive Deployment (2-3 Years)



Implement QRNG capabilities across all cryptographic applications and security systems.



Integrate with cloud infrastructure and distributed systems for scalable quantum randomness.



Establish QRNG as standard requirement for all new cryptographic system deployments.

Vendor Ecosystem and Commercial Availability

QRNG Technology Providers:

The quantum random number generation market has matured with several commercial providers offering certified solutions:



Hardware-based QRNG devices suitable for enterprise and government deployment.



Integrated solutions combining QRNG with HSMs and cryptographic infrastructure.



Cloud-based QRNG services for organizations requiring quantum randomness without hardware investment.



Chip-level QRNG solutions for embedded systems and IoT device applications.

Procurement Considerations:



Security Certification

Prioritize solutions with appropriate security certifications and compliance validation.



Performance Specifications

Evaluate generation rates, entropy quality, and integration capabilities.



Support and Maintenance

Assess vendor capabilities for ongoing support and system maintenance.



Cost-Benefit Analysis

Compare QRNG implementation costs against security enhancement benefits.

Integration with Quantum-Safe Architecture

Architectural Considerations:

Cryptographic Infrastructure Integration:



Key Management Systems

Enhanced entropy for cryptographic key lifecycle management.



Secure Communication

QRNG integration with TLS, VPN, and other secure communication protocols.



PKI Enhancement

Improved random number quality for certificate generation and digital signatures.



Post-Quantum Implementations

Native QRNG support for ML-KEM, ML-DSA, and SLH-DSA implementations.

Monitoring and Validation:



Continuous Testing

Implement ongoing statistical testing of QRNG output quality.



Entropy Pool Management

Intelligent management of quantum-generated entropy across systems.



Health Monitoring

Real-time monitoring of QRNG system status and performance.



Audit and Compliance

Regular assessment of QRNG implementation and security effectiveness.

Organizations should evaluate QRNG implementation as part of their comprehensive quantum-safe infrastructure upgrade, recognizing that high-quality randomness forms the foundation of all cryptographic security, whether classical or post-quantum. The integration of QRNG capabilities provides an immediate security enhancement while supporting the long-term transition to quantum-safe cryptographic systems.



2.4


AI-Enhanced Implementation and Management

The integration of artificial intelligence with quantum-safe cryptography represents a paradigm shift in implementation and management approaches:

2.4.1

AI-Assisted Migration Planning

Intelligent Analysis:



Machine learning models for cryptographic performance prediction across different algorithms.



AI-driven testing and validation of hybrid cryptographic implementations.



Automated impact assessment for system modifications and upgrades.




Predictive modeling for resource requirements and migration timelines.

Implementation Benefits:



Reduced manual effort in complex migration planning.



Automated optimization of hybrid algorithm configurations.



Improved accuracy in risk assessment and prioritization.



Real-time adaptation to changing threat landscapes.

2.4.2

Quantum-AI Hybrid Computing Architecture

Quantum Processing Units (QPUs) are being integrated with CPUs, GPUs, and LPUs for specialized problem classes:

Hybrid Architecture Benefits:



QPUs handle specialized cryptographic operations and optimization problems.



AI systems optimize resource allocation and performance tuning.



Classical processors manage standard computing tasks and user interfaces.



Integrated approach reduces overall computational overhead.

Applications in Cryptography:



Quantum-enhanced key generation and random number generation.



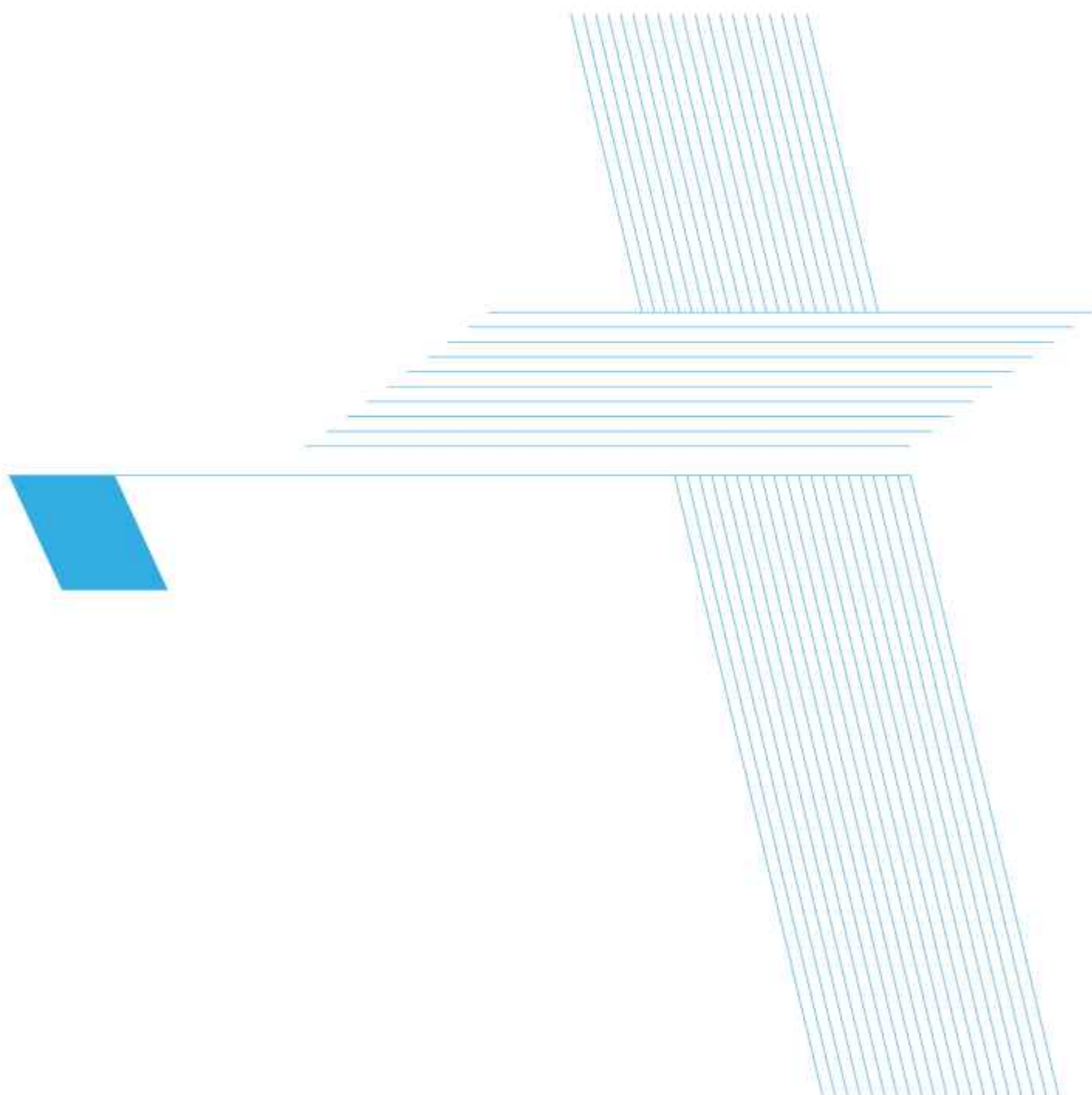
Advanced threat detection using quantum machine learning.



Optimization of cryptographic parameter selection.



Quantum-safe algorithm testing and validation.



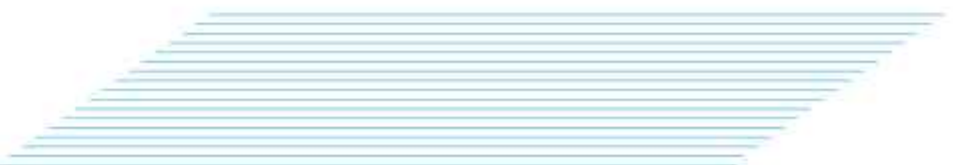


03

Phased Organizational Rollout

Migrating to quantum-safe cryptography is not a one-time event but a multi-phase transformation that must be aligned with an organization's architecture, strategic priorities, resource availability and risk appetite. A carefully planned rollout strategy minimizes operational disruption, fosters stakeholder alignment and enables the introduction of quantum-resistant protections in a controlled and scalable way.

This section introduces the first phase of the migration journey - Groundwork & Discovery - where strategic intent is translated into practical action plans that lay the foundation for successful execution.



3.1

Groundwork & Discovery (Immediate)

The Groundwork phase serves as the critical bridge between strategic planning and practical implementation. Its core objective is to establish a clear understanding of quantum risk exposure, align with business priorities and set stakeholder expectations to guide the overall migration roadmap.

This phase ensures quantum-safe migration is driven by risk-based priorities, operational feasibility and alignment with business and regulatory objectives. Key actions include defining the transition scope, identifying early wins to showcase value and engaging leadership and technical teams to build internal momentum. Establishing this foundation is critical for executing a smooth, phased rollout of quantum-resistant cryptographic protections.

3.1.1

Migration Priority Mapping

With the cryptographic inventory and QBOM in place, the next step is to determine migration priorities by assessing each system's business impact, quantum risk exposure and technical readiness. This ensures that optimal resources are allocated where they will deliver the greatest risk reduction and operational value.

To guide a strategic quantum-safe rollout, organizations should segment cryptographic assets by risk and readiness. Start by categorizing systems into high, medium, or low impact prioritizing customer-facing platforms, payment systems and identity services. Identify assets protecting long-lived sensitive data (e.g., medical or legal records) to mitigate "harvest now, decrypt later" risks. Highlight systems with public exposure or strict compliance requirements, such as PKI, VPNs and secure messaging. Also, pinpoint assets using PQC-ready technologies (e.g., OpenSSL + LibOQS, supportive cloud services) for early migration. This structured approach ensures high-risk systems are upgraded first, migrations align with business needs and resources are efficiently utilized.

3.1.2

Business-Aligned Strategy

A successful quantum-safe migration must align not only with technical risk profiles, but also with the organization's strategic priorities, operational timelines and business context. The objective is to ensure that cryptographic modernization efforts support and enhance broader business goals such as growth, regulatory compliance, customer trust and digital transformation.

Post-quantum cryptography (PQC) migration should be embedded into the fabric of the business, integrated with enterprise initiatives, and given the visibility, funding, and support required for long-term success.

3.2

Targeted Upgrades (Mid Term – 1 to 3 Years)

As organizations move beyond initial discovery and pilot phases, the focus should shift to systematically upgrading high-risk, business-critical systems over a strategic 1–3-year transition period. Key priorities include migrating externally facing applications, long-lived data stores and authentication systems, while refining processes based on pilot insights. Staying adaptable to evolving PQC standards, vendor timelines and performance feedback is essential. This measured approach ensures a secure, resilient and low-risk expansion of quantum-safe cryptographic capabilities across core enterprise systems.

3.2.1

PQC Migration for High-Risk Systems

In this phase of migration, the focus shifts to replacing or strengthening legacy cryptography in high-impact, high-risk environments, particularly those with significant business value, regulatory obligations, or long-term data confidentiality needs.

Key targets include public-facing web applications (upgrading TLS with hybrid or PQC suites), internal IAM systems (modernizing PKI and SSO signature mechanisms) and secure communication platforms (adopting PQC signatures like Dilithium or Falcon for document signing and email encryption).

Regulated systems handling sensitive data should be prioritized, especially those under strict retention or confidentiality mandates. This stage leverages insights from early pilots, mature PQC libraries (e.g., LibOQS, BoringSSL), vendor-supported hybrid cryptography and modern HSMs to reduce early risk while boosting operational confidence in enterprise-wide quantum readiness.



3.2.2**Iterative
Strategy Updates**

A key success factor in the mid-term phase of post-quantum migration is maintaining agility. As PQC standards mature and best practices evolve, organizations must continuously refine their strategies to align with emerging technologies, regulatory developments and shifting business priorities. This includes regularly updating the QBOM with insights from vendor assessments, audits and system upgrades, while dynamically adjusting migration plans based on changes in risk posture, customer expectations, or organizational shifts such as mergers or digital transformation efforts.

Staying ahead also requires active monitoring of regulatory trends and sector-specific compliance mandates related to quantum readiness. Engaging with standards bodies through pilots or feedback initiatives helps organizations anticipate changes and influence future directions. By embracing an iterative approach and remaining responsive to new intelligence and requirements, organizations can ensure a resilient migration path and establish themselves as forward-thinking leaders in the quantum-secure era.

3.3**Enterprise-Wide Deployment
(Long Term – 3+ Years)**

The final phase of the post-quantum migration journey centres on full enterprise-wide adoption, where post-quantum cryptography is seamlessly embedded across all systems, processes and policies. This ensures the organization operates with a fully quantum-resilient security posture.

In this stage, PQC is comprehensively integrated into core business operations, ICT infrastructure, security protocols and third-party ecosystems. Quantum-safe cryptography becomes the default standard for protecting data, communications and identities, establishing long-term resilience as a foundational element of the enterprise's digital strategy.

3.3.1**Full PQC
Implementation**

At this stage, the organization should solidify its quantum-safe posture by fully phasing out legacy cryptographic algorithms, removing RSA, ECC and outdated hybrid schemes from critical systems in favour of PQC-only implementations. PQC should be standardized across the entire infrastructure, including TLS, VPNs, identity systems, IoT and data encryption protocols to ensure consistent protection.

Long-term data archives must be re-encrypted or re-signed with PQC to safeguard confidentiality well into the future. PQC should also be embedded into CI/CD pipelines and DevSecOps workflows, ensuring secure software development, automated key management and signing processes. Finally, cryptographic upgrades should extend to edge and embedded systems such as mobile apps, firmware and IoT devices, to close any remaining gaps and complete the organization's transition to a quantum-resilient ecosystem.

3.3.2

Policy and Operational
Integration

Achieving full quantum-safe maturity goes beyond deploying algorithms. It requires embedding PQC awareness, enforcement and sustainability into the organization's core policies, operations and governance. This long-term phase ensures that quantum-safe practices become a permanent part of cybersecurity, risk management and compliance frameworks.

Key actions include updating security and ICT policies to mandate standards bodies approved PQC algorithms, define approved toolsets and enforce standards across internal and vendor systems. Organizations must also invest in training programs to build team-wide PQC competence and integrate these topics into ongoing education. Audit and compliance protocols should evolve to include PQC-specific controls, cryptographic agility checks and third-party evaluations. Operational processes, including key management and incident response, must be adapted for PQC's technical requirements. Finally, supply chain integrity should be reinforced by requiring PQC readiness in procurement, contracts and vendor engagements. This phase transforms PQC from an initiative into a foundational element of a secure and future-ready enterprise.





04

Resilience, Monitoring & Futureproofing

Achieving a quantum-safe baseline is a significant milestone but it is not the endpoint. Cryptography is a dynamic discipline, constantly shaped by new vulnerabilities, evolving technologies and shifting regulatory landscapes.

This part focuses on embedding resilience and adaptability into cryptographic systems, ensuring they deliver continuous assurance as conditions change. This includes exploring advanced technologies like Quantum Key Distribution (QKD) to lay the groundwork for next-generation security models.

This final phase transforms the quantum-safe journey from a finite migration project into an ongoing capability, one that evolves with the threat landscape and secures the enterprise well into the future.

4.1

Crypto-Agile Architecture & Lifecycle Management

Crypto agility, the ability to swiftly adapt cryptographic algorithms, parameters and protocols is vital for long-term security, especially in a post-quantum world where even PQC schemes may eventually face cryptanalysis. Building crypto-agile systems starts with using abstraction layers and modular libraries (e.g., OpenSSL, PKCS#11) to decouple cryptographic logic from application code, enabling seamless algorithm swaps and hybrid testing. A centralized cryptographic control plane helps enforce policies around algorithm choices, key sizes and protocol settings.

Agile key management is also crucial, supporting rapid key rotation, cross-domain orchestration and integration with automated certificate systems. Systems should support parallel algorithm modes classical, hybrid and PQC to ensure backward compatibility and ease phased migrations. Lifecycle governance must be embedded across development, procurement and decommissioning processes to maintain visibility and auditability of cryptographic assets. By establishing crypto agility, organizations can adapt quickly to new threats, comply with evolving standards, handle vendor transitions smoothly and avoid costly refactoring turning cryptography into a dynamic and resilient security capability.

4.2

Continuous Monitoring & Compliance

Achieving a quantum-safe environment is just the starting point. True resilience requires shifting from a static "set-and-forget" model to one of continuous cryptographic hygiene and assurance. As standards evolve and environments change, ongoing monitoring becomes essential to maintain compliance, security and operational stability. Key practices include deploying real-time cryptographic health dashboards to track algorithm usage, certificate status, key lifecycles and compliance metrics, along with implementing drift detection to catch unauthorized changes or regressions to insecure algorithms.

To sustain audit readiness and regulatory alignment, organizations should maintain thorough documentation of PQC deployment progress, risk assessments and audit artifacts. Integrating threat intelligence such as PQC vulnerability updates and industry alerts ensures proactive risk mitigation. Automated enforcement through CI/CD hooks, Infrastructure-as-Code scanning and endpoint policy tools helps maintain cryptographic integrity across the environment. Together, these practices turn cryptography into a dynamic, continuously validated security layer ensuring long-term trust and adaptability in the post-quantum era.



4.3

QKD Exploration

While PQC algorithms offer strong software-based defenses, QKD introduces a complementary, physics-based security model grounded in the principles of quantum mechanics. QKD enables the generation and secure exchange of encryption keys that are theoretically immune to compromise even by quantum computers making it especially valuable for environments requiring ultra-high levels of confidentiality. Though still emerging and limited by infrastructure demands such as specialized hardware and optical links, QKD holds strong potential for critical use cases in government, defence, healthcare and financial systems.

As part of long-term digital trust strategies, organizations should evaluate QKD for select high-assurance applications. Key considerations include assessing viable use cases like inter-data centre links or secure diplomatic communications, understanding the infrastructure requirements (fibre-based for metro use, satellite-based for global reach) and exploring hybrid models that combine QKD with classical or PQC encryption for resilience. While QKD is not yet scalable for broad enterprise use due to cost and interoperability challenges, it should be viewed as a strategic supplement and not a replacement for PQC, especially for national security planning.

4.4

Quantum Networking and Communication Infrastructure

4.4.1

QKD Implementation

Quantum Key Distribution represents the most mature quantum technology for secure communications:

Current Deployment Status:



Operational QKD networks in China (Beijing–Shanghai backbone), Europe (Geneva), and other regions.





Record-breaking 12,900 km quantum key distribution achieved between South Africa and China using satellite (2024).



Commercial QKD services available from multiple vendors for high-security applications.

Implementation Considerations:


 QKD provides theoretically unbreakable key distribution but requires specialized infrastructure.


 Distance limitations for fiber-based QKD (typically 100-200 km without repeaters).

 Satellite-based QKD for long-distance and intercontinental communications.

 Integration with post-quantum cryptography for comprehensive security.

Deployment Strategy:

 Point-to-point QKD links for highest-security government and financial communications.

 Hybrid QKD + PQC implementations for defense-in-depth security.

 Metropolitan area QKD networks for critical infrastructure protection.

 Satellite QKD for global secure communications backbone.

4.4.2

Quantum Internet Development

The evolution toward a global quantum internet represents the long-term vision for quantum communications:

Current Status:

 Small-scale quantum networks operational in research and government environments

 Standards development for quantum network protocols and interoperability

 Quantum repeater technology in development for long-distance quantum communication

Future Applications:

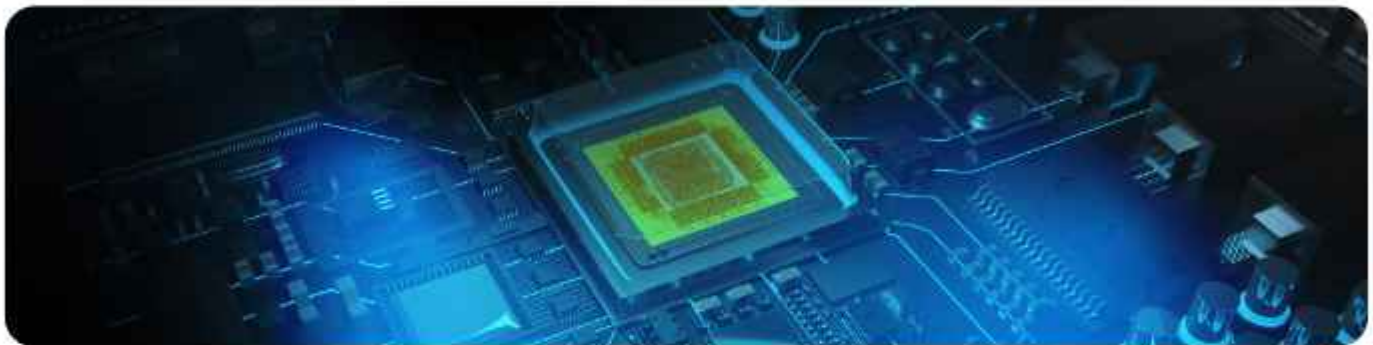
 Distributed quantum computing across multiple locations

 Quantum-enhanced sensing and timing networks

 Global quantum-secure communications infrastructure

 Integration with classical internet for hybrid services

Implementation Timeline:



4.5

Quantum Cyber Readiness Implementation

4.5.1

Algorithm Diversification Implementation for Indian Organizations

High-risk systems in Indian government, defense, and critical infrastructure sectors should implement multiple PQC algorithms to ensure cryptographic resilience against quantum threats.

4.5.1.1

Primary + Backup Strategy

Implementation Framework:



4.5.1.2 Multi-Algorithm Signatures

Digital Signature Strategy:



Use both ML-DSA and SLH-DSA for critical document signing in government applications, financial transactions, and legal document authentication



Implement SLH-DSA as backup for highest-security applications where hash-based signatures provide additional confidence



Maintain compatibility with existing digital certificate infrastructure and PKI systems

4.5.1.3 Performance Optimization

System-Based Algorithm Selection:



High-performance systems

Prioritize ML-KEM and ML-DSA for faster operations in core banking and real-time government services



Resource-constrained environments

Implement intelligent algorithm selection based on available computational resources and network bandwidth



Legacy system integration

Develop hybrid approaches that maintain compatibility with existing government and PSU infrastructure

4.5.1.4 Continuous Monitoring

AI-Enhanced Monitoring Framework:



Deploy automated monitoring for algorithm performance and security status across government networks



Implement real-time analysis of cryptographic performance and security metrics



Integrate with CERT-In infrastructure for threat intelligence, situational awareness and incident response



Establish alerting mechanisms for algorithm vulnerabilities and performance degradation

4.5.2 Government and Defense Sector Specific Requirements

4.5.2.1 Immediate Implementation Priorities

Software and Firmware Signing:



Begin transitions immediately for all government software and firmware signing using quantum-safe algorithms



Prioritize critical systems including Aadhaar, core banking systems, and defense communication networks



Implement quantum-safe signing for Digital India initiative platforms and e-Governance applications

4.5.2.2 Phased Migration Timeline

Phase 1: Critical Infrastructure (2025)



Support and prefer quantum-safe algorithms for all new government system deployments



Begin migration of existing high-risk systems including financial infrastructure and defense networks



Establish quantum-safe standards for government procurement and vendor requirements

Phase 2: Complete Transition (2025-2030)



Exclusively use quantum-safe algorithms for all classified and sensitive government systems



Complete migration of all government digital infrastructure and citizen services



Ensure interoperability with international partners and allied nation systems

4.5.2.3

Critical Component Prioritization

Firmware Roots of Trust:



Prioritize firmware upgrades as critical early migration components for government infrastructure



Implement quantum-safe boot processes for all critical government and defense systems



Establish secure supply chain requirements for quantum-safe firmware and hardware components

4.5.3

Sector-Specific Implementation Guidelines

4.5.3.1

Banking and Financial Services

Implementation Priorities:



Core banking systems

Immediate quantum-safe upgrade for central banking infrastructure and payment processing systems.



Digital payment platforms

Quantum-safe implementation for UPI and other digital payment infrastructure.



Regulatory compliance

Align with RBI cybersecurity guidelines and emerging quantum-safe regulatory requirements.

4.5.3.2

Telecommunications and Critical Infrastructure

Deployment Strategy:



Network infrastructure

Integrate quantum-safe protocols into telecommunications and internet infrastructure.



5G networks

Implement quantum-safe security measures in ongoing 5G deployment.



Control systems

Quantum-safe upgrade for power grid, transportation, and water management systems.

4.5.3.3

Healthcare and Public Services

Security Requirements:



Electronic health records

Quantum-safe protection for national health data infrastructure.



Citizen services

Secure quantum-safe implementation for government service delivery platforms.



Identity systems

Enhanced quantum-safe protection for Aadhaar.

4.5.4

Technical Implementation Considerations

4.5.4.1

Infrastructure Compatibility

Legacy System Integration:



Assess existing PKI infrastructure for quantum-safe algorithm compatibility.



Implement hybrid approaches during transition period to maintain service continuity.



Address performance impact of larger key sizes and computational overhead on existing systems.

4.5.4.2

Vendor and Supply Chain Management

Procurement Requirements:



Establish quantum-safe requirements for all government technology procurement.



Vendor assessment criteria for quantum-safe algorithm implementation and support.



Supply chain security measures for quantum-safe hardware and software components.

4.5.4.3

Standards and Interoperability

Compliance Framework:



Align with international standards while maintaining compatibility with existing Indian technology infrastructure.



Ensure interoperability across government departments and agencies.



Coordinate with sectoral regulators for consistent quantum-safe implementation across industries.

4.5.5

Risk Assessment and Prioritization

4.5.5.1

High-Priority Systems

Immediate Migration Requirements:



National security systems

Defense communication networks and strategic infrastructure.



Critical infrastructure

Power grid control systems and telecommunications infrastructure.



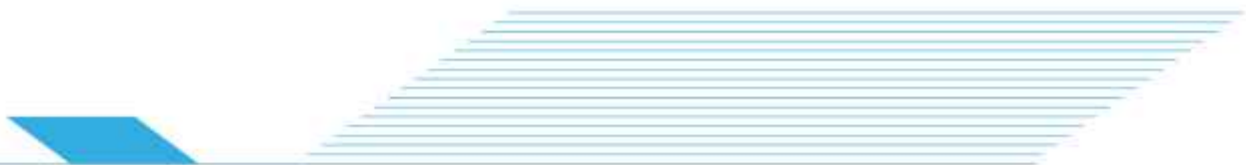
Financial infrastructure

Core banking systems and payment processing networks.



Government services

Digital identity systems and citizen service platforms.



4.5.5.2

Risk-Based Implementation

Threat Assessment Framework:



Data sensitivity classification

Prioritize systems handling classified, financial, or personal data.



Exposure evaluation

Assess internet-facing systems and external communication channels.



System criticality assessment

Focus on systems essential for national security and public safety.



Lifecycle planning

Consider system refresh cycles and upgrade schedules in migration planning.

4.5.6

Monitoring and Compliance

4.5.6.1

Security Monitoring

Continuous Assessment:



Implement automated scanning for quantum-vulnerable cryptographic implementations



Monitor algorithm performance and security effectiveness across government systems



Establish incident response procedures for quantum-related security events



Regular security assessments to validate quantum-safe implementation effectiveness



4.5.6.2 Compliance Validation

Audit and Verification:



Regular compliance audits to ensure adherence to quantum-safe requirements



Performance monitoring to assess impact of quantum-safe algorithms on system operations



Documentation maintenance for cryptographic inventories and implementation status



Stakeholder reporting on quantum-safe migration progress and security posture

4.5.7 Implementation Timeline and Milestones

4.5.7.1 Immediate Actions (2025)



Complete quantum-safe algorithm deployment for all new government system implementations



Begin migration of highest-risk systems including financial infrastructure and defense networks



Establish quantum-safe requirements for government procurement and vendor management



Implement monitoring and compliance frameworks for quantum-safe migration tracking

4.5.7.2 Medium-term Goals (2025-2027)



Complete migration of all critical infrastructure and government service systems



Achieve quantum-safe interoperability across all government departments and agencies



Implement comprehensive monitoring and incident response capabilities for quantum threats



Establish India-specific quantum-safe standards and implementation guidelines

4.5.7.3

Long-term Objectives (2027-2030)



Complete national quantum-safe infrastructure deployment across all sectors



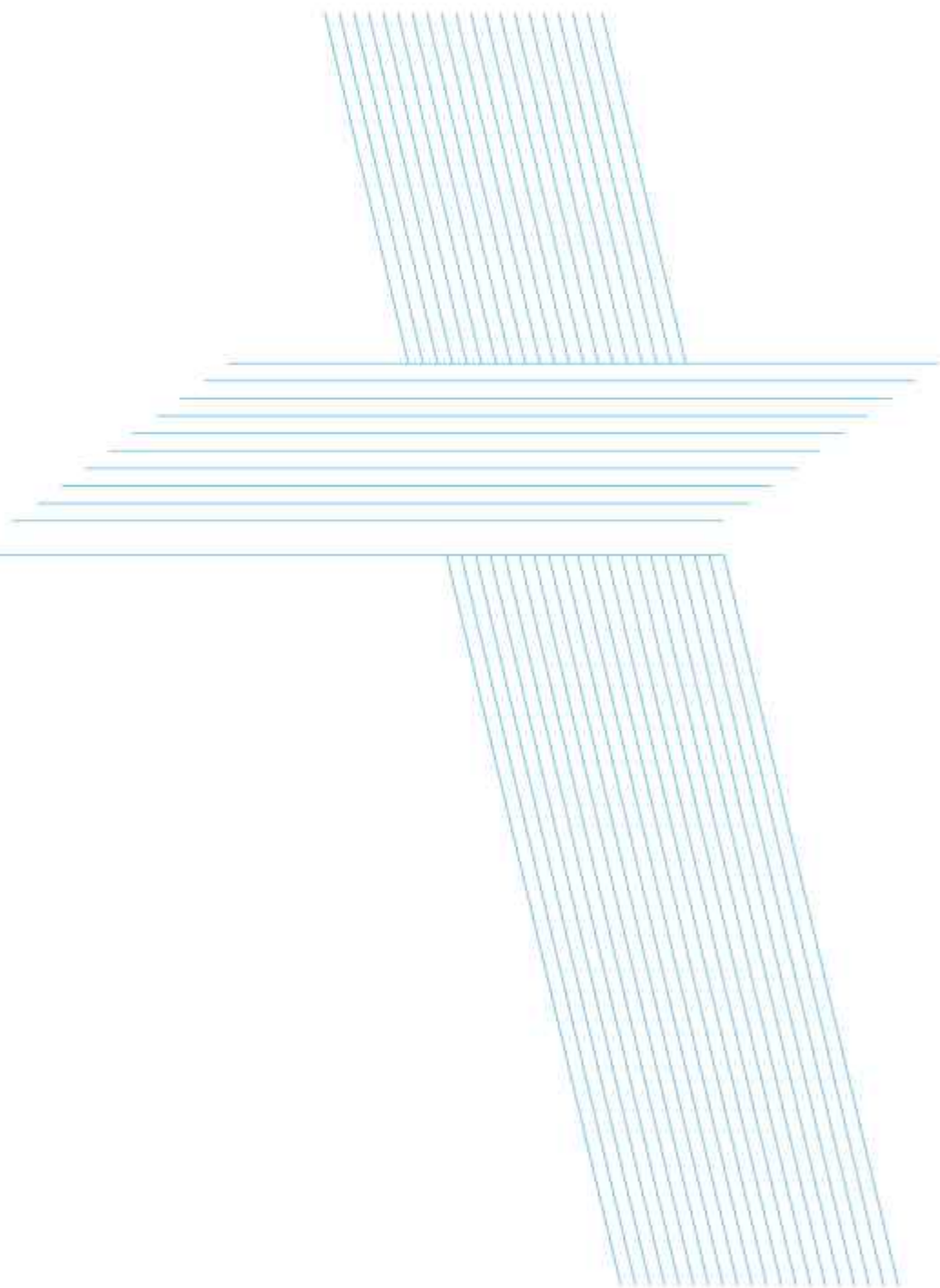
Achieve full compliance with international quantum-safe standards and requirements



Maintain technological leadership in quantum-safe implementation and best practices



Ensure sustainable quantum-safe cybersecurity posture for critical national infrastructure



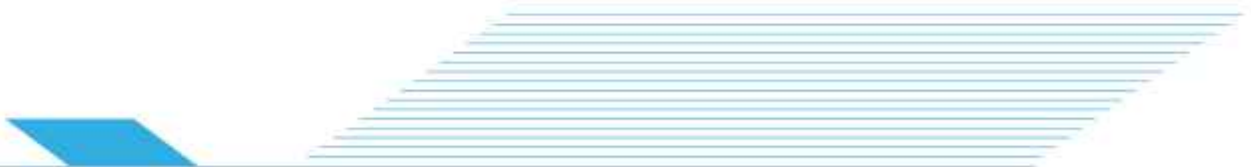
Conclusion

The emergence of quantum computing represents a paradigm shift in cybersecurity, posing an unprecedented challenge to traditional cryptographic systems that safeguard sensitive data and digital transactions. With quantum computers expected to break widely used encryption protocols, organizations must act now to future-proof their security infrastructure. Failing to prepare for this shift could leave critical assets vulnerable to quantum-enabled cyberattacks.

The guiding principles for migration can be summarised as follows: establish an organizational governance structure that institutionalizes quantum risk; raise awareness of quantum risk across all levels of the organization; prioritize quantum risk alongside existing cybersecurity threats; make strategic decisions that support future technology adoption; and foster collaboration across the broader ecosystem.

A successful quantum-safe migration requires a structured and proactive approach, beginning with comprehensive risk assessments, cryptographic inventory audits and stakeholder engagement. Organizations must adopt hybrid cryptographic models, balancing traditional and quantum-resistant algorithms to ensure a smooth transition while maintaining interoperability with existing systems. Rigorous testing and validation of PQC implementations will be essential to ensure performance, security and compliance with evolving regulatory frameworks. Moreover, businesses must commit to continuous monitoring, adapting security frameworks and staying aligned with global PQC standards, to remain resilient against future quantum threats.

The quantum revolution is inevitable, but organizations that act decisively and strategically will not only protect their data from quantum risks but also lead the way in shaping a quantum-resilient future.



References

1. NIST's Post-Quantum Cryptography Standardization Project:
<https://csrc.nist.gov/projects/post-quantum-cryptography>
2. NIST's Finalized Post-Quantum Encryption Standards:
<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>
3. NIST's Announcement of Quantum-Resistant Cryptographic Algorithms:
<https://www.nist.gov/programs-projects/post-quantum-cryptography>
4. RSA: Perspective on Quantum Computing and Encryption:
<https://www.rsa.com/resources/blog/zero-trust/setting-the-record-straight-on-quantum-computing-and-rsa-encryption/>
5. ENISA: Post-Quantum Cryptography: Current state and quantum mitigation
<https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation>
6. NCSC UK: Next steps in preparing for post-quantum cryptography
<https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography>
7. Inputs from Synergy Quantum India Pvt Ltd
8. Inputs from QClairvoyance Quantum Labs Pvt Ltd
9. Mitre: Quantum Computing: Quantifying the current state of the art to assess cybersecurity threats
10. World Economic Forum: Quantum Readiness Toolkit: Building a Quantum-Secure Economy
11. FS-ISAC: Future State Technical Paper
12. Strategy for Migrating to Automated Post-Quantum Cryptography Discovery and Inventory Tools:
<https://www.cisa.gov/resources-tools/resources/strategy-migrating-automated-post-quantum-cryptography-discovery-and-inventory-tools>

Acronyms used

Acronym	Full Form
PQC	Post-Quantum Cryptography
QBOM	Quantum Bill of Materials
NIST	National Institute of Standards and Technology
FIPS	Federal Information Processing Standards
ISO	International Organization for Standardization
TLS/SSL	Transport Layer Security/Secure Sockets Layer
SSH	Secure Shell
IPsec	Internet Protocol Security
SCADA	Supervisory Control and Data Acquisition
HSM	Hardware Security Module
CI/CD	Continuous Integration / Continuous Deployment
IAM	Identity and Access Management
SSO	Single Sign-On
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
CBOM	Cryptographic Bill of Materials
QKD	Quantum Key Distribution
TPM	Trusted Platform Module
CA	Certificate Authority
IoT	Internet of Things
HQC	Hamming Quasi-Cyclic
ML - KEM	Module Lattice – Key Encapsulation Mechanism
QPU	Quantum Processing Unit
SaaS	Software as a Service
ML – DSA	Module Lattice – Digital Signature Algorithm
RSA	Rivest–Shamir–Adleman
DSA	Digital Signature Algorithm
DH	Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie–Hellman

SISA

SISA is a Leader in Cybersecurity Solutions for the Digital Payment Industry. As a Global Payment Forensic Investigator of the PCI Security Standards Council, we leverage forensics insights into preventive, detective, and corrective security solutions, protecting 1,000+ organizations across 40+ countries from evolving cyberthreats. Our suite of solutions from AI-driven compliance, advanced security testing, agentic detection/ response and learner focused-training has been honoured with prestigious awards, including from Financial Express, DSCI-NASSCOM and The Economic Times. With commitment to innovation, and pioneering advancements in Quantum Security, Hardware Security, and Cybersecurity for AI, SISA is shaping the future of cybersecurity. In the quantum space, we offer Quantum Risk Assessments, QBOMs (Quantum Bill of Materials), and strategic Quantum Briefing Sessions—helping organizations prepare for the next wave of cyber threats through deep forensics intelligence.

For more information about our solutions and how they can revolutionize cybersecurity for digital payments, visit www.sisainfosec.com.

CERT-In

CERT-In is the national agency for responding to computer security incidents as and when they occur. In the Information Technology Amendment Act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents.
- Emergency measures for handling cyber security incidents.
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed Refer www.cert-in.org.in for more details