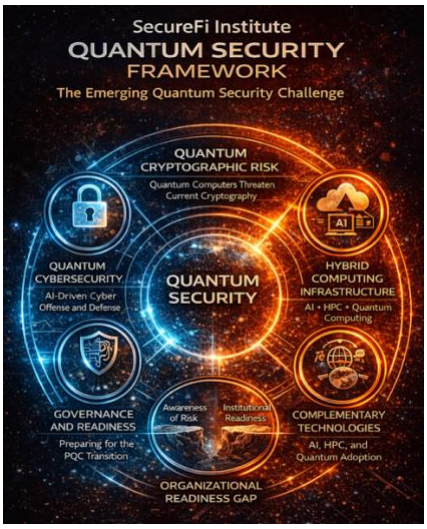
SecureFi Institute Research Series

The Quantum Security Framework - Emerging Technology and Infrastructure Security

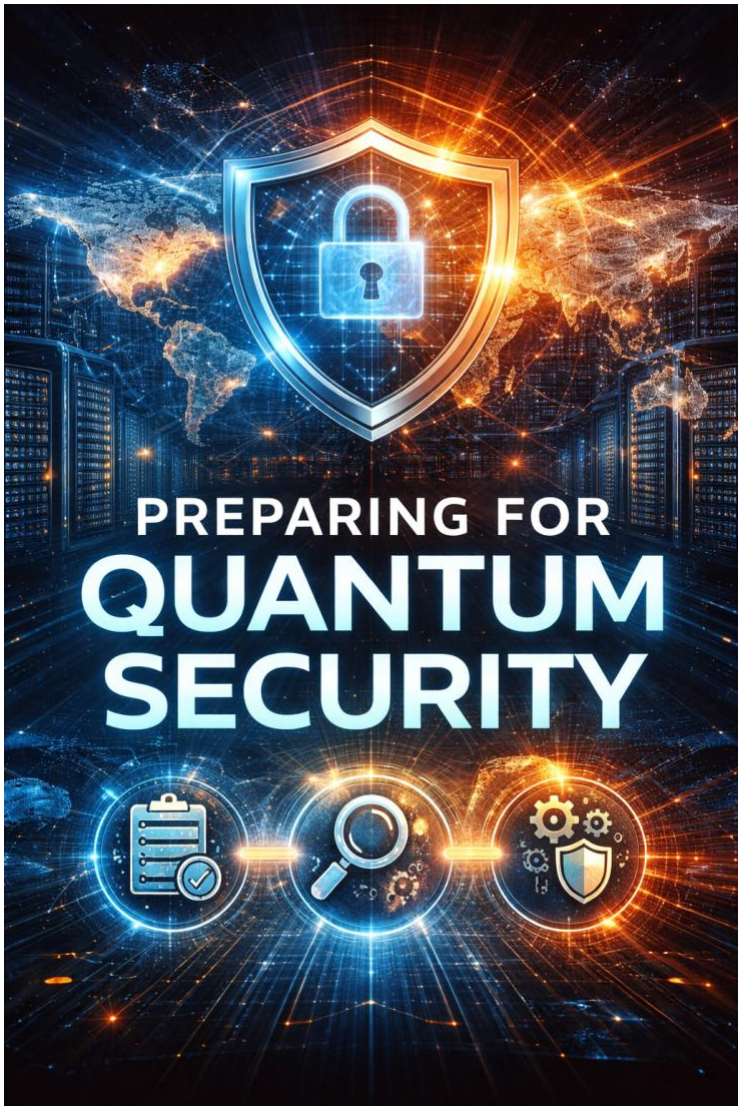


Preparing Organizations for Quantum Security

Date: March 2026
SecureFi Institute

Preparing Organizations for Quantum Security

SecureFi Institute Research Brief



Executive Summary

The transition to quantum-resistant cryptography represents one of the most significant security infrastructure changes organizations will face in the coming decade.

The possibility that encrypted data collected today may be decrypted in the future by quantum computers has heightened the urgency for organizations to begin planning for cryptographic transition.

While large scale quantum computers capable of breaking widely used cryptographic systems may still be years away, the preparation required to transition critical systems will take considerable time.

Modern digital infrastructure depends heavily on public key cryptography, including RSA and elliptic curve cryptography, which are widely used to secure communications, authenticate systems, and protect sensitive data. Quantum computing introduces the possibility that these cryptographic systems may eventually become vulnerable.

Preparing for this transition requires more than simply replacing cryptographic algorithms. Organizations must understand where cryptography is used across their infrastructure, assess long-term risk exposure, and develop migration strategies that integrate with existing technology lifecycles.

The transition to post quantum cryptography will require coordinated planning across infrastructure teams, cybersecurity organizations, enterprise architecture, and procurement processes. Organizations that begin planning early will be better positioned to manage this transition in a controlled and secure manner.

The Coming Cryptographic Transition

Public key cryptography forms the foundation of modern digital security. Protocols that rely on RSA and elliptic curve cryptography are embedded throughout digital infrastructure, including secure communications, identity systems, financial transactions, and software authentication.

Quantum computing introduces a potential disruption to this foundation. Algorithms such as Shor’s algorithm demonstrate that sufficiently advanced quantum computers could break many of the cryptographic systems currently used to secure digital communications.

Although the timeline for large scale cryptographically relevant quantum computers remains uncertain, the infrastructure protected by current cryptographic systems often has long operational lifecycles. Systems deployed today may remain in operation for decades.

This creates a challenge for organizations responsible for protecting long lived infrastructure and sensitive information. Preparing for quantum-resistant cryptography must begin well before quantum computers capable of breaking existing systems become operational.

Inventory of Cryptographic Systems

One of the most difficult challenges in preparing for post quantum cryptography is identifying where cryptography is used within an organization’s technology environment.

Cryptographic functions are embedded in many different systems and applications, often across infrastructure that has evolved over many years.

Examples include:

• Secure web communications and TLS certificates
• Identity and authentication systems
• Virtual private networks and remote access platforms
• Software and firmware signing systems
• Cloud infrastructure services
• Embedded systems and industrial control environments

Many organizations do not have a complete inventory of these cryptographic dependencies. Without visibility into where cryptography is used, it becomes difficult to assess risk or plan for migration.

Developing a comprehensive inventory of cryptographic systems is therefore a critical first step in preparing for quantum security.

Risk Assessment

Once cryptographic dependencies are identified, organizations must assess which systems present the greatest long-term security risk.

Several factors influence the urgency of migration planning:

• Sensitivity of the data being protected
• Expected operational lifespan of systems
• Exposure to potential data collection or interception
• Dependency on long-term confidentiality

Certain types of information, such as government records, healthcare data, or intellectual property, may require protection for many years. If adversaries collect encrypted data today and store it for future decryption, organizations could face significant long-term security risks.

This risk model is often described as *"harvest now, decrypt later",* where encrypted data captured today may be decrypted once quantum computing capabilities become available.

Understanding which systems face this type of long-term exposure helps organizations prioritize their transition planning.

Migration Strategy

Transitioning to post quantum cryptography will likely occur gradually over many years.

Most organizations will not replace all cryptographic systems at once. Instead, migration strategies will typically involve phased deployment of new algorithms and hybrid cryptographic environments.

A practical migration strategy often includes several stages:

- Discovery and cryptographic inventory
- Risk analysis and prioritization
- Evaluation of quantum algorithms
- Testing and interoperability validation
- Gradual deployment across infrastructure

During the transition period, many systems may operate using both classical and quantum-resistant cryptographic methods. These hybrid approaches allow organizations to maintain compatibility while gradually strengthening their cryptographic posture.

Organizations should also monitor emerging cryptographic standards and guidance to ensure that migration strategies align with evolving post-quantum cryptographic frameworks.

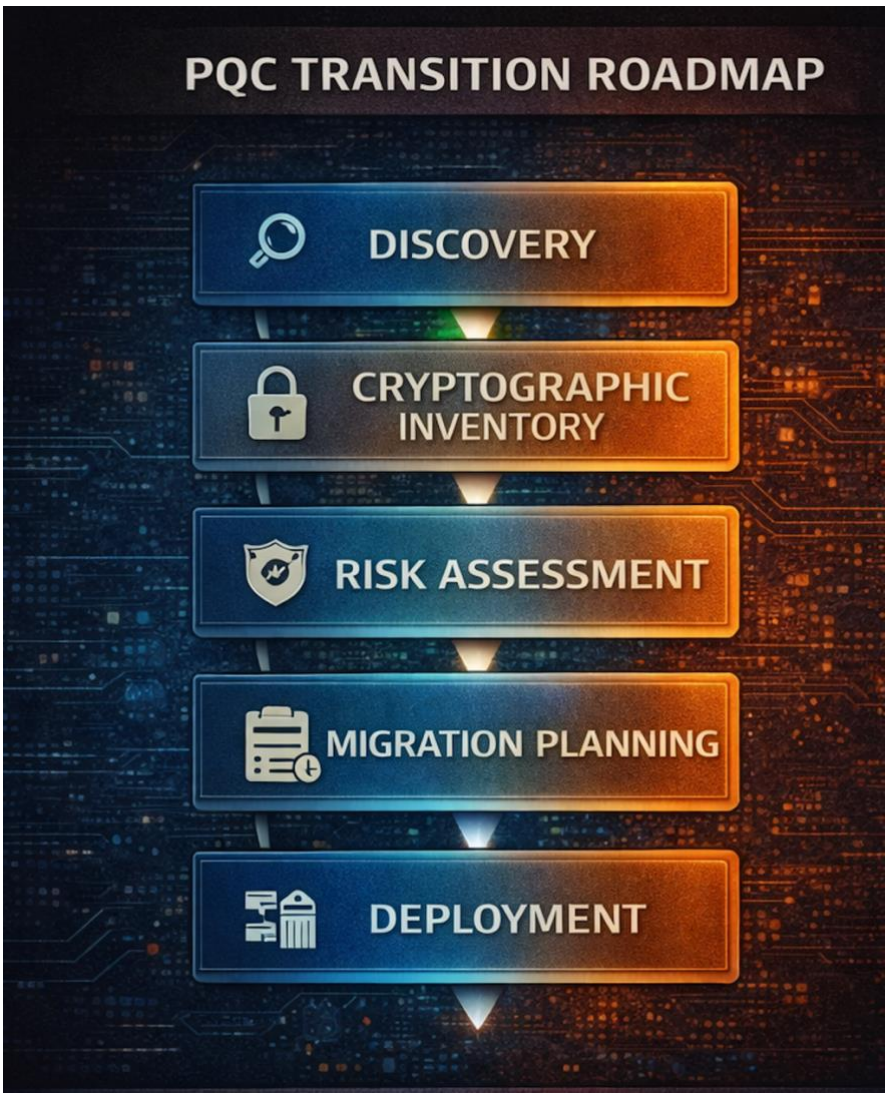


Figure 1. Post-Quantum Cryptography Transition Roadmap

Organizations preparing for quantum security will typically follow a multi-stage transition process. Initial discovery and cryptographic inventory enable visibility into where cryptographic systems are used across infrastructure. Risk assessment and migration planning then guide phased deployment of quantum-resistant cryptographic algorithms.

Institutional Readiness

Preparing for quantum security requires coordinated planning across technology infrastructure, cybersecurity governance, and organizational decision making. Quantum security is not only a technical challenge but also an organizational one.

Cryptographic systems are embedded across many areas of modern digital infrastructure, which means the transition will require coordination across multiple teams.

Key stakeholders may include:

- Cybersecurity leadership
- Infrastructure and network teams
- Enterprise architecture organizations
- Software development teams
- Procurement and vendor management

Procurement processes will also play an important role. Organizations will increasingly need to ensure that technology vendors support post quantum cryptographic standards and migration pathways.

Institutional awareness and coordination will be essential to ensure that cryptographic transitions occur smoothly and without unintended disruptions to critical systems.

Figure 2. Organizational Readiness Model for Quantum Security

Transitioning to quantum cryptography requires coordination across leadership, governance, procurement, infrastructure, and cybersecurity teams. Organizational readiness ensures that cryptographic migration strategies align with infrastructure lifecycles, vendor support, and institutional risk management.

Leadership Challenge

The transition to quantum-resistant cryptography presents a leadership challenge for organizations responsible for long-term infrastructure security.

Leaders must balance uncertainty regarding the timeline of quantum computing with the reality that infrastructure changes can take many years to implement.

Waiting until quantum computers capable of breaking existing cryptographic systems are widely available would likely leave organizations insufficient time to transition critical infrastructure.

Instead, leadership awareness and early planning are essential for managing this transition responsibly.

Looking Ahead

The migration to quantum-resistant cryptography will likely be one of the most complex cybersecurity transitions organizations face in the coming decade.

Unlike many technology upgrades, cryptographic systems are deeply embedded across digital infrastructure and often integrated into systems that have long operational lifespans.

Organizations that begin building awareness, developing cryptographic inventories, and evaluating migration strategies today will be better prepared to adapt as quantum computing capabilities continue to evolve.

Preparing for quantum security is ultimately a matter of long-term institutional readiness and strategic technology governance.

Key Takeaways

- Transitioning to quantum-resistant cryptography will require long-term planning and coordination.
- Organizations must develop an inventory of where cryptography is used across their infrastructure.
- Risk assessments should prioritize systems that protect long lived or highly sensitive data.
- Migration strategies will likely involve phased deployments and hybrid cryptographic environments.
- Institutional readiness and leadership awareness are essential for managing the transition to quantum security.

About SecureFi Institute

SecureFi Institute focuses on leadership awareness and governance readiness across emerging computing technologies, including artificial intelligence, cybersecurity, high performance computing, and quantum systems.

The Institute works to help government and institutional leaders understand the security and strategic implications of these technologies before they become deeply embedded in critical infrastructure.

SecureFi Institute Research Brief No. 005

Preparing Organizations for Quantum Security

March 2026

Figures and Analytical Models

All figures, diagrams, and analytical models presented in this research brief were developed by SecureFi Institute as part of its research on emerging computing architectures and cybersecurity implications.

Research Disclaimer

This research brief is provided for informational and educational purposes and reflects analysis from SecureFi Institute on emerging computing technologies and cybersecurity trends. The views expressed are intended to support awareness and discussion of technology and infrastructure challenges and do not represent official policy positions.