KEYFACTOR

The 10-Step Checklist for Tech Leaders in Financial Services

Understand the new NIST standards

Familiarize yourself with the new NIST-approved post-quantum cryptographic algorithms and understand their impact on your bank's security infrastructure, compliance requirements, and risk management strategies.

Evaluate your cryptographic landscape

Assess where and how cryptography is used across your systems – from internal applications to customer-facing services. Identify any legacy systems that may present migration challenges, especially as quantum threats loom closer.

Build your transition roadmap

Create a phased migration strategy aligned with your institution's risk appetite, audit cycles, and tech refresh timelines. Ensure key areas like payments, identity systems, and secure communications are included with clear milestones and resource allocations.

Align business and security stakeholders

Engage senior leadership and compliance teams early to frame the transition as vital for operational resilience, fraud prevention, and long-term data protection. This focus helps maintain customer trust and regulatory compliance.

Test and benchmark algorithms

Establish a controlled environment to test post-quantum algorithms. Use results to validate security controls, refine performance expectations, and meet audit requirements.

Upgrade cryptographic libraries and systems

Ensure all cryptographic libraries across your environment, including third-party tools and cloud platforms, support the new standards. Apply integrity checks to prevent tampering and ensure seamless compatibility.

Map and log affected assets

Maintain an up-to-date cryptographic asset inventory, tracking where current algorithms are used and where replacements are needed. Implement logging policies to support traceability and forensic investigations, ensuring regulatory readiness.

Assess third-party and supply chain readiness

Evaluate the quantum-readiness of your third-party vendors, fintech partners, and service providers. Include quantum preparedness in your third-party risk assessments and penetration testing protocols to avoid vulnerabilities in the supply chain.

Educate teams and build awareness

Provide role-specific training for IT, security, and compliance teams on implementing new algorithms. Run internal awareness campaigns to address quantum risk, secure data handling, and the broader business impact of cryptographic agility.

Monitor progress and refine your strategy

Track your progress across departments and use KPIs tied to compliance, risk reduction, and performance to keep efforts aligned with future goals. Adjust the strategy as necessary based on emerging threats or evolving regulatory guidance.

Simplify Your Transition to New NIST-Approved Cryptographic Standards

With the finalization of NIST's post-quantum cryptographic algorithms in late 2024, financial institutions can now take clear steps to strengthen defenses against future quantum threats. But what does this mean for your institution's security? How can you ensure compliance and a secure, efficient transition?

This 10-step checklist is tailored for banking and financial services leaders to help **drive strategy**, **reduce risk**, and **stay ahead of compliance demands**.

Mitigate Quantum Risk and Strengthen Security

Step into PQC Lab – a secure, no-risk sandbox designed for financial services.

Safely test NIST-approved post-quantum algorithms, assess system vulnerabilities, and refine your transition strategy without the added burden of setting up infrastructure. Stay ahead of quantum threats and ensure compliance with ease.

Enter the PQC Lab ↗