Quintessence Labs

PQC READINESS ASSESSMENT: A RISK-BASED BLUEPRINT FOR YOUR PQC TRANSITION

The Cryptographic Cliff

The transition to post-quantum cryptography is one of the most significant cybersecurity transformations organizations have faced in decades. As standards mature and regulatory expectations increase, organizations need visibility into where cryptography is used, which systems are vulnerable, and how to prioritize migration efforts.

Generally, the greatest challenge is not the implementation of a particular new algorithm. It is the process of identification and streamlined remediation of cryptographic assets across the organization.

Harvest Now, Decrypt Later (HNDL) Risk

Sensitive data intercepted today may remain vulnerable long after it is collected. Adversaries can capture encrypted information now and retain it until quantum computers are capable of breaking today's public-key cryptography.

Organizations responsible for protecting financial information, government data, or long-life confidential information must assess whether their data remains secure throughout its required lifetime.

The Compliance Mandate

With NIST's PQC standards finalized and global regulatory pressure mounting, migration is no longer a future initiative—it is a mandatory requirement for compliance and business continuity.

PQC Readiness Assessment

The PQC Readiness Assessment package is a technology-led service that kick-starts enterprise efforts to streamline your post-quantum cryptography initiatives. While it starts with cryptographic discovery, the focus is not on producing massively inflated CBOMs, rather focuses on actionable remediation plans that can be automated immediately.

> ***Aggressive new regulatory mandates, driven by recent advances in cryptographic research, now require organizations to not only prove full visibility over their encryption assets, but also provide a path of remediation. The risk of operating with blind spots in your cryptographic posture is not a future problem—it is happening right now.***

Why Organizations Need a PQC Readiness Assessment

Most organizations cannot answer fundamental questions about their cryptographic posture:

- Where is cryptography being used across the enterprise?
- Which systems rely on vulnerable algorithms such as RSA and ECC?
- Which assets present the greatest business and compliance risk?
- How complex will migration be?
- Where should investment be prioritized first?

Without this visibility, organizations risk inefficient migrations, increased compliance exposure, and unnecessary operational disruption.

A Risk-Based Approach

Successful PQC migration begins with understanding risk. Most organizations struggle with “Shadow Cryptography”, unknown keys and algorithms hidden within existing systems. Rather than attempting to replace cryptography everywhere at once, QuintessenceLabs helps organizations identify and prioritize the systems, applications, data stores, and cryptographic assets that present the greatest exposure.

Using automated discovery, cryptographic inventory, and risk analysis, we provide a clear understanding of:

- Where vulnerable cryptography exists
- Which assets are most exposed to HNDL risk
- Which systems are most critical to business operations
- Where migration efforts will deliver the greatest risk reduction

The result is a practical, prioritized roadmap that aligns security investment with business objectives.

QuintessenceLabs’ risk-based approach focuses on visibility before action.

1 Comprehensive Cryptographic Discovery & Automated Inventory

Using qSentry we create a detailed Cryptographic Bill of Materials (CBOM) that provides visibility into cryptographic assets and dependencies across the enterprise:

The assessment includes:

- **Algorithm Identification:** Detecting RSA, ECC, and legacy protocols.
- **Asset Mapping:** Locating keys across cloud, on-prem, IoT, and Hardware Security Modules (HSMs).
- **Dependency Mapping:** Understanding how your applications rely on specific cryptographic functions.

2 Risk-Based Prioritization

We don’t treat all data equally. We assess your assets based on:

- **Data Longevity:** How long must this data remain secret? (Critical for HNDL protection).
- **Business Criticality:** How vital is this system to your revenue and operations?
- **Migration Complexity:** How easily can the current algorithm be swapped?

YOUR PATH TO QUANTUM RESILIENCE

PHASE 1 Workshops: Discovery & Inventory

- Full cryptographic discovery.
- Risk scoring and gap analysis.
- Identification of “High-Risk/High-Value” assets.

PHASE 2 Workshops: Risk Assessment & Strategy

- Development of a prioritized migration roadmap.
- Selection of NIST-standardized PQC algorithms.
- Design of a Crypto-Agility framework to ensure future-proof transitions.

PHASE 3 Workshops: Roadmap & Remediation

- Phased rollout of PQC protocols.
- Interoperability and performance testing.
- Final validation and security hardening.

KEY DELIVERABLES

Audit Ready Assessment Report: A prioritized vulnerability mapping and threat exposure

Cryptographic Bill-of-Materials (CBOM): Visibility into cryptographic applications, algorithms and dependencies

Remediation Plan: An actionable roadmap to showcase tangible progress to governance bodies

Crypto-Agility Strategy: Recommendations to support future cryptographic transitions with minimal operational disruptions

Powered by qSentry Platform

The assessment leverages qSentry, QuintessenceLabs' cryptographic discovery and crypto-agility management platform.

qSentry provides automated discovery, CBOM generation, risk evaluation, and policy-based remediation, enabling organizations to continuously assess cryptographic posture and prioritize migration activities based on business risk.

Rather than treating PQC migration as a one-time project, qSentry helps establish an ongoing crypto-agility framework capable of adapting to future cryptographic requirements.



WHY PARTNER WITH QUINTESSENCELABS?

- **Minimize Disruption:** Our phased approach ensures security upgrades don't break your existing production workflows.
- **Optimize Investment:** Stop guessing. Use our risk-based data to allocate your budget where it provides the highest security ROI.
- **Achieve Crypto-Agility:** Don't just fix today's problem; Build a framework that allows you to swap algorithms effortlessly as new threats emerge.
- **Ensure Compliance:** Stay ahead of NIST, and industry-specific mandates with a documented, audit-ready migration path.

Be quantum ready today.

Contact QuintessenceLabs to schedule a PQC Readiness Assessment consultation and take the first step toward long-term quantum resilience.

info@quintessencelabs.com | www.quintessencelabs.com

Quintessence Labs

About QuintessenceLabs

QuintessenceLabs' portfolio of modular products addresses the most difficult security challenges, helping implement robust security strategies to protect data today and in the future.

For more information on QuintessenceLabs' data protection solutions, please visit **www.quintessencelabs.com** or email **info@quintessencelabs.com**.

Global Headquarters
Unit 11, 18 Brindabella Circuit
Brindabella Business Park
Canberra Airport ACT 2609
+61 2 6260 4922

US Headquarters
175 Bernal Road Suite 220
San Jose CA 95119
+1 650 870 9920

Document ID: 7472-01