



Quantum Infinite.

Future Secured!



We enable **ZERO DATA** PQC migration with **FULL DATA SOVEREIGNTY**.

Your data never leaves your environment. Ever.



FUTURE-PROOF your enterprise against quantum threats—**TODAY**.

Eliminate “Harvest Now, Decrypt Later” risk before it’s too late.



NIST-ALIGNED. MANDATE-READY.

Fully aligned with NIST standards and U.S. federal mandates.



ACCELERATE SECURELY. ADAPT ENDLESSLY.

Crypto-agile solutions that evolve as threats and standards evolve.



COMPLETE VISIBILITY. TOTAL CONTROL.

Discover, assess, and remediate crypto risk across your entire ecosystem.



GOOGLE’S 2029 MANDATE IS REAL. THE WINDOW IS CLOSING.

Act now to meet the mandate and stay ahead of quantum disruption.



ZERO DISRUPTION. ZERO COMPROMISE.

NO CHANGES. NO IMPACT. NO RISK.



NO CHANGES TO YOUR
CORE BANKING.



NO CHANGES TO PAYMENT
OPERATIONS.



NO IMPACT TO
YOUR CUSTOMERS.

RECOGNITION & ACCREDITATION



Top 100 Award Winner

Recognized for innovation
and leadership.



Associate Member

Proud member of the
Texas Bankers Association



**FINANCIAL WOMEN
IN TEXAS**

helping women succeed!

Member

Financial Women in Texas
Empowering women.
Driving success.



Trusted Advisor

Texas Bankers ISAO
Trusted partner in strengthening
banking cybersecurity.



Secure your **Quantum** Future with us



LATEST TRENDS 2026

Post-Quantum Cryptography (PQC) Outlook for Banking & Financial Services

1



Government Momentum

Govt procurement and mandates accelerating PQC adoption across regulated sectors.

2



NIST Guidance

NIST's NCCoE publishes practical guidance for discovery, inventories and phased migration.

3



Commercial Alignment

Cloud, HSM, PKI and TLS ecosystems integrating PQC capabilities at scale.

4



Algorithm Diversity

HQC as backup KEM alongside ML-KEM for resilience and crypto agility.

5



Hybrid Cryptography

Hybrid models combining classical + PQC are the preferred migration approach.

6



Identity Systems

NIST drafts enable ML-KEM and ML-DSA in PIV credentials and digital identities.

7



Digital Signature Expansion

New additional PQC digital signature candidates advanced to Round 3 for greater choice.

8



Enterprise Migration

Enterprises executing discovery, pilots and phased migration with crypto-agile architectures.



ZERO DISRUPTION. ZERO COMPROMISE.
NO CHANGES. NO IMPACT. NO RISK.



NO CHANGES TO YOUR
CORE BANKING.



NO CHANGES TO PAYMENT
OPERATIONS.



NO IMPACT TO
YOUR CUSTOMERS.

Secure your **Quantum** Future with us

Risk management in the Quantum Era



We enable **zero data** PQC migration with **full data sovereignty**.
Your data never leaves your environment. Ever.



1. IMMEDIATE P&L IMPACT

Average financial-sector data breach costs **\$6.08M per incident** (IBM, 2024) — before any quantum retro-trust security controls.

Mitigation Outcome

Quantum-safe defenses protect P&L from mass exploitation.



SOURCE:
IBM Cost of a Data Breach Report 2024
Financial services avg. exceeds \$6M



2. SYSTEMIC LOSS AMPLIFICATION

Internet-crime losses exceeded **\$16B** in 2024 (FBI IC3, Apr 23, 2025), showing how rapidly data breach losses amplify.

Mitigation Outcome

PQC safely prevents enterprise and ecosystem loss against threats.



SOURCE:
FBI IC3 Report 2024
Losses exceeded \$12.5B in 2023 and projected to exceed \$16B in 2024



3. REGULATORY ENFORCEMENT RISK

The OCC imposed an **\$80M** civil penalty on Capital One (Aug 6, 2020) for inadequate information-security controls.

Mitigation Outcome

Proactive PQC migration shows credible security to regulators.



SOURCE:
OCC Enforcement Action (Capital One) – Aug 6, 2020
\$80M civil penalty



4. PUBLIC-MARKET COMPLIANCE EXPOSURE

The SEC fined Morgan Stanley **\$35M** (Sep 20, 2022) for safeguarding failures, material penalties, tied to oversight gaps.

Mitigation Outcome

Adopting PQC demonstrates fiduciary security to investors.



SOURCE:
SEC Order (Morgan Stanley) – Sep 20, 2022
\$35M penalty for security failures



5. BRAND & TRUST EROSION

Breaches destroy customer trust, trigger churn, and erode brand value for years.

Mitigation Outcome

Quantum-ready security builds trust, loyalty, and long-term value.



SOURCE:
IBM Cost of a Data Breach Report 2024
Reputational damage is a top long-term cost driver



The time to act is now: Google has accelerated its timeline and issued a global mandate to fully migrate to **Post-Quantum Cryptography by 2029**.

This accelerated deadline reflects the real and immediate quantum risk to our digital world.

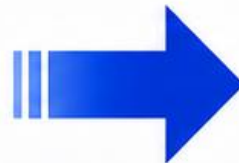
Secure your **Quantum Future** with us

Where Cryptography Lives



WHERE CRYPTOGRAPHY LIVES

-  Internet Banking
-  Mobile Apps
-  Certificates
-  VPNs
-  APIs
-  SWIFT
-  Identity
-  Cloud
-  Third-party Software



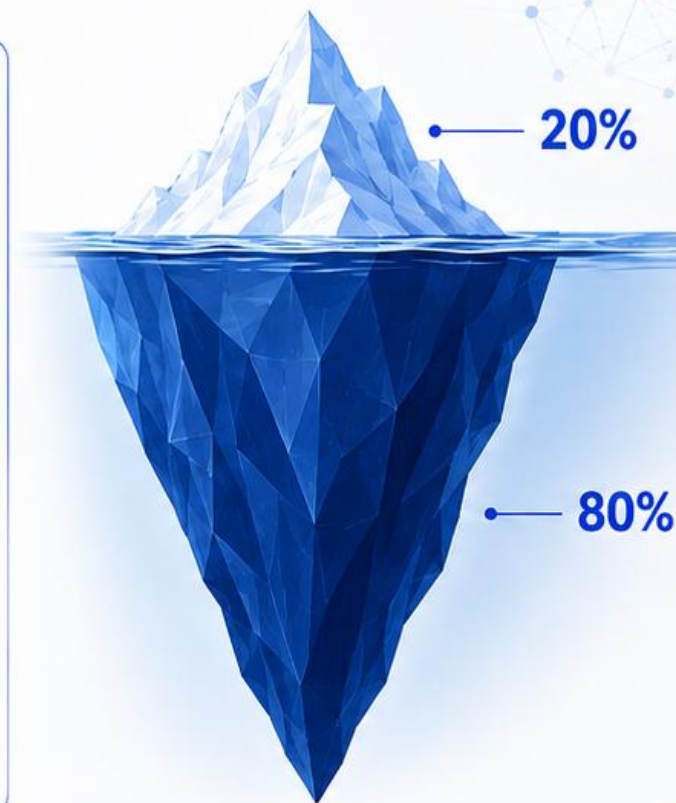
VISIBLE (20%)

- Applications
- Certificates
- VPNs



HIDDEN (80%)

- Embedded libraries
- Legacy systems
- Hard-coded keys
- Unknown dependencies
- Archived data



ZERO DISRUPTION. ZERO COMPROMISE.
NO CHANGES. NO IMPACT. NO RISK.



NO CHANGES TO YOUR
CORE BANKING.



NO CHANGES TO PAYMENT
OPERATIONS.



NO IMPACT TO
YOUR CUSTOMERS.

Secure your **Quantum** Future with us

Urgency to Migrate to Post-Quantum Cryptography



We enable **ZERO DATA PQC** migration with **FULL DATA SOVEREIGNTY**.
Your data never leaves your environment. Ever.



1 Attacks Are Already Underway

"Harvest Now, Decrypt Later" is active.

Sensitive financial data is being captured today.



2 Core Cryptography Will Break

Quantum will break today's **encryption**.

RSA, ECC, and DH will not survive at scale.



3 Security Infrastructure Will Fail

Core trust systems **collapse** together.

TLS, PKI, authentication, and key exchange all fail simultaneously.



4 Assets Are at Risk

Blockchain and crypto face **irreversible exposure**.

Wallets, transactions, and custody are vulnerable.



Discover.

Identify cryptographic risk across your environment.



Analyze.

Assess vulnerabilities and prioritize what matters most.



Transform.

Migrate to NIST-aligned PQC with zero data migration.



The time to act is now: Quantum migration is a mission-critical priority for enterprises and governments.

Industry timelines are accelerating toward **2029**.

Delay is risk. Inaction is exposure.



ZERO DISRUPTION. ZERO COMPROMISE.

NO CHANGES. NO IMPACT. NO RISK.

- ✓ NO CHANGES TO YOUR CORE BANKING.
- ✓ NO CHANGES TO PAYMENT OPERATIONS.
- ✓ NO IMPACT TO YOUR CUSTOMERS.

Secure your **Quantum** Future with us

US GOVERNMENT MANDATES

LATEST DIRECTIVES. CLEAR DEADLINES. ZERO ROOM FOR DELAY.



WHITE HOUSE

June 2026

- ◆ EO 14412: Securing the Nation Against Advanced Cryptographic Attacks.
- ◆ EO 14413: Ushering in the Next Frontier of Quantum Innovation.
- ◆ NSPM-12 reinforces national security implementation.

PQC delay is now a governance risk.



OMB – M-26-15

June 24, 2026

- ◆ Executes federal migration to post-quantum cryptography.
- ◆ Agency plans due within 120 days.
- ◆ Critical systems must reduce quantum risk by 2030.



NIST STANDARDS

2024–2026

- ◆ FIPS 203: ML-KEM (Final)
- ◆ FIPS 204: ML-DSA (Final)
- ◆ FIPS 205: SLH-DSA (Final)
- ◆ Crypto-agility guidance is advancing.



NSA – CNSA 2.0

2022–2025

- ◆ Phased PQC adoption for national security systems.
- ◆ Use CNSA 2.0 approved algorithms and suites.
- ◆ Update cryptography by 2025.



US CONGRESS

2025–2026

- ◆ Quantum readiness legislation continues to advance.
- ◆ Federal funding and procurement are favoring PQC-ready solutions.
- ◆ Oversight pressure on agencies and critical sectors is increasing.



WE ENABLE ZERO DATA PQC MIGRATION WITH FULL DATA SOVEREIGNTY.

Your data never leaves your environment. Ever.



Zero data movement architecture



NIST-aligned Standards-ready



Full visibility, Total control



Built for enterprise-scale migration



THE TIME TO ACT IS NOW

Mandates are accelerating. Timelines are shrinking. The cost of inaction is catastrophic.

Delay is risk. Inaction is exposure.

◆ Secure your Quantum Future with us ◆

PQC MIGRATION TIMELINE

THE WINDOW IS CLOSING

2022



POLICY TRIGGER

Federal mandate initiated

- White House sets PQC migration direction
- Agencies begin crypto inventory

2023



INVENTORY PHASE

Know your exposure

- Full cryptographic discovery required
- RSA, ECC, PKI dependencies identified

2024



STANDARDS FINALIZED

NIST locks the future

- ML-KEM, ML-DSA, SLH-DSA released
- Transition is no longer optional

2025–2027



EXECUTION WINDOW

Act or fall behind

- Deploy quantum-safe algorithms
- Begin phased enterprise-wide migration
- Build crypto-agility at scale

2029



HARD DEADLINE

Quantum risk becomes real

- Google mandates full PQC migration by 2029
- Encryption as we know it becomes vulnerable
- “Harvest Now, Decrypt Later” is already underway



WE ENABLE **ZERO DATA** PQC MIGRATION
WITH **FULL DATA SOVEREIGNTY**.

Your data never leaves your environment. Ever.



Zero data
movement
architecture



NIST-aligned.
Mandate-ready.



Full visibility.
Total control.



Built for
enterprise-scale
migration.



- Legacy cryptography **WILL FAIL** (RSA, ECC, DH)
- Sensitive data is already being harvested
- Migration is a **multi-year transformation**—not a patch
- Delaying = **guaranteed exposure**



THE TIME TO ACT IS NOW

Google has accelerated PQC timelines to **2029** — compressing what was a decade into a few years.

The window is closing. Delay is risk.

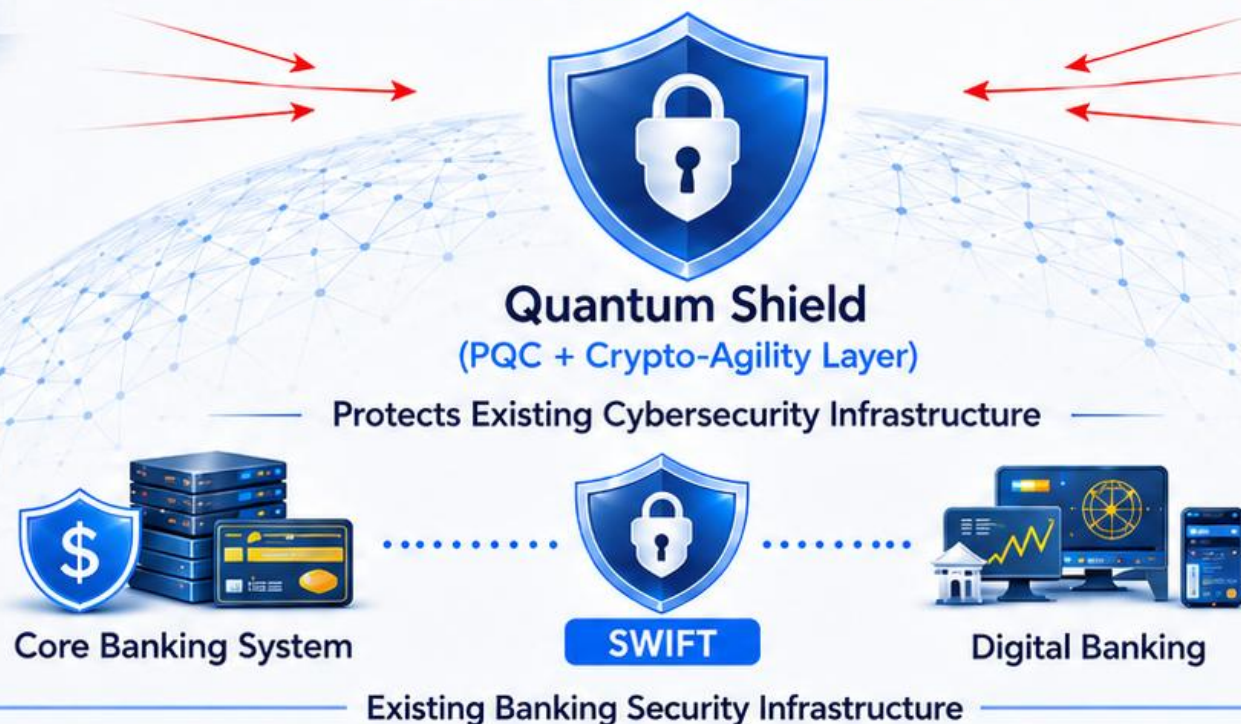
Secure your Quantum Future with us



QUANTUM SHIELD

PROTECTING BANKING SECURITY INFRASTRUCTURE

Post-quantum protection layered over existing banking systems—
no disruption, no replacement.



WHAT THIS MEANS FOR FINANCIAL INSTITUTIONS

- ✓ **No changes** to core banking systems
- ✓ **No disruption** to payment operations
- ✓ **No downtime** or customer impact
- ✓ **Seamless integration** with existing infrastructure



QUANTUM SECURITY IS IMPLEMENTED AS A PROTECTIVE LAYER —
NOT A SYSTEM REPLACEMENT.

Secure your **Quantum** Future with us

QUANTUM DELIVERABLES

ZERO-DATA PQC MIGRATION ACROSS ENTERPRISE SURFACES



WEB SERVER / URL ANALYSIS

EXPOSE. MAP. ELIMINATE RISK.

- ◆ Analyze all exposed web services, endpoints, and URLs.
- ◆ Identify cryptographic usage and risk patterns.
- ◆ Prioritize vulnerabilities with real-world impact.



CODE BASE ANALYSIS

INSPECT. IDENTIFY. REMEDIATE.

- ◆ Deep inspection of application code and dependencies.
- ◆ Detect weak or deprecated cryptographic libraries, algorithms, and implementations.
- ◆ Eliminate hidden risks at the source.



NETWORK ANALYSIS

ASSESS. ALIGN. ASSURE.

- ◆ Assess internal and external network communications.
- ◆ Map cryptographic protocols in use across the network.
- ◆ Identify gaps. Close them. Stay compliant.



DIGITAL CERTIFICATE ANALYSIS

VALIDATE. VERIFY. PROTECT.

- ◆ Evaluate digital certificates, key lengths, algorithms, and trust chains.
- ◆ Assess lifecycle status and expiration risk.
- ◆ Ensure enterprise-wide certificate resilience.



ZERO DATA
MOVEMENT.
ZERO RISK.



COMPLETE
VISIBILITY.
TOTAL CONTROL.



NIST-ALIGNED.
MANDATE-READY.
FUTURE-PROOF.



NO BLIND SPOTS.
NO ASSUMPTIONS.
ONLY ASSURANCE.



BUILT FOR
ENTERPRISE SCALE.
ENGINEERED TO WIN.



QUANTUM RISK IS REAL. ATTACKERS ARE PREPARING.
SEE IT. FIX IT. SECURE IT. BEFORE IT'S TOO LATE.

◆ Secure your Quantum Future with us ◆

QUANTUM RESILIENCE ASSESSMENT REPORTS

CLEAR INSIGHTS. ACTIONABLE RISK INTELLIGENCE. QUANTUM RESILIENT FUTURE.



QUANTUM EXPOSURE ANALYSIS

Post Quantum Risk Summary

QUANTUM RISK IMPACT – URGENT

67% Non-Compliant

67% Non-Compliant – 57%



CRYPTOGRAPHIC ASSETS INVESTIGATED



- 67% User Credentials
- 17% Public CAs (RSA 2048)
- 24% Code / Signatures
- 25% Other

KEY PQC NON-COMPLIANT AREAS

PQC CURVE	AT RISK	HIGH RISK	MED RISK	LOW RISK
PQC Curves – Algorithms	88%	6%	4%	2%
SSL/TLS – RSA 2048	57%	17%	19%	7%
Digital Certificates – RSA 2048	57%	21%	15%	7%



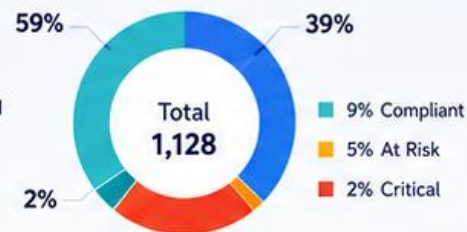
NETWORK CRYPTOGRAPHIC MAPPING

Protocol Distribution Summary

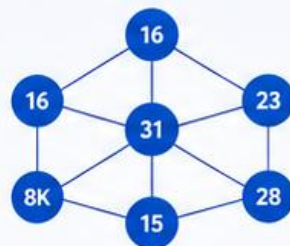
666acy

Weak / Deprecated

- 59% Weak / Deprecated
- 2% Insufficient
- 39% Non-Compliant



LEGACY NODES IDENTIFIED



- SSL, RSA 15 / SHA1 / RC4 | 16
- Digital Certificates RSA 2044 | 31
- Weak Protocols / Legacy Nodes | 28

LEGACY & WEAK PROTOCOLS IDENTIFIED

- SSL, RSA 1266 / RSA 2048
- SSH RSA 1024 / SHA1 | 5315
- SSH RSA 1536 / SHA1 | RC4
- Digital Certificates RSA 2044
- Digital Certificates RSA 2044
- Digital Certificates RSA 2007



DIGITAL CERTIFICATE ANALYSIS

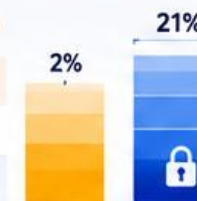
Certificate Health Summary

51% NON-COMPLIANT – 31%

67% Non-Compliant

77% Non-Compliant

77% In 17 Weak Industry



KEY CERTIFICATE ISSUES IDENTIFIED

ISSUE	NON-COMPLIANT	IMPACT
TLC500	51%	PQC Curves
PQC Curves	67%	PQC Curves
PQC Curves Ascendist	21%	PQC Algorithms
Large / Expiry Window	57%	Expiry / Renewal
Duplicate Certificate RSA 2048	37%	Duplicate Certs
PCC Curves Anticam RSA 3557	21%	CA Misconfiguration

* Commonly used weak key cert compliant standards notes

Secure your Quantum Future with us

EXECUTIVE SUMMARY

REPORT SCOPE



This report provides a comprehensive cryptographic security assessment covering classical and post-quantum threat landscapes. The analysis evaluates algorithm strength, protocol configurations, certificate hygiene, and quantum readiness across all scanned assets.

Quantum Safe analysis websites, source code, networks, and system certificates to detect quantum and classical cryptographic vulnerabilities, providing a unified view of security risks and quantum readiness across your digital environment.



CONSOLIDATED SCAN SUMMARY

Scan Type		Coverage
	Code Scanning	348 files, 29 components
	Certificate Scanning	7 certificates
	Network Traffic	79,681 packets captured
	URL / TLS Scanning	8 endpoint(s)



RISK SUMMARY

The analysis reveals 703 critical, 46 high, 1146 medium, and 65 low-risk indicators across 4 scan types.

 Critical	703	Immediate remediation required
 High	46	Address within 30 days
 Medium	1146	Plan remediation
 Low	65	Acceptable / monitor



KEY HIGHLIGHTS



- Code analysis across 9 languages: HTML, JSON, JavaScript, Markdown, Python, SQL, Shell, TypeScript, YAML



- Certificate scan: 7 certificates assessed, 1 expired.



- Network traffic: TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0 detected across 79,681 packets.



- URL / TLS scanning: 8 endpoints analyzed for cipher suite and protocol security.



CONFIDENTIAL — This report contains sensitive security assessment data. Distribution should be limited to authorized personnel only.



PROTECT YOUR DATA



STRENGTHEN SECURITY



STAY QUANTUM-READY



Secure your Quantum Future with us



CONSOLIDATED RISK DISTRIBUTION



REPORT SCOPE

This report provides a comprehensive cryptographic security assessment covering classical and post-quantum threat landscapes. The analysis evaluates algorithm strength, protocol configurations, certificate hygiene, and quantum readiness across all scanned assets.

Quantum Safe analyzes websites, source code, networks, and system certificates to detect quantum and classical cryptographic vulnerabilities, providing a unified view of security risks and quantum readiness across your digital environment.



CONSOLIDATED SCAN SUMMARY

Scan Type	Coverage
</> Code Scanning	398 files, 23 components
🛡️ Certificate Scanning	7 certificates
🌐 Network Traffic	79,681 packets captured
🔑 URL / TLS Scanning	8 endpoint(s)



RISK SUMMARY

The analysis reveals **703 critical**, **46 high**, **1146 medium**, and **65 low-risk** indicators across **4 scan types**.



- 🔴 Critical (703)
- 🟠 High (46)
- 🟡 Medium (1146)
- 🟢 Low (65)

Risk Level	Count	Description
Critical	703	Immediate remediation required
High	46	Address within 30 days
Medium	1146	Plan remediation
Low	65	Acceptable / monitor



KEY HIGHLIGHTS

- ✓ **Code analysis** across 9 languages: HTML, JSON, JavaScript, Markdown, Python, SQL, Shell, TypeScript, YAML
- ✓ **Certificate scan**: 7 certificates assessed, 1 expired
- ✓ **Network traffic**: TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0 detected across **79,681** packets
- ✓ **URL/TLS scanning**: 8 endpoints analyzed for cipher suite and protocol security



THE TIME TO ACT IS NOW: Google has accelerated its timeline and issued a global mandate **to fully migrate to Post-Quantum Cryptography by 2029.**

This accelerated deadline reflects the real and immediate quantum risk to our digital world.



CBOM COMPLETE:
90.6%



CONFIDENTIAL — This report contains sensitive security assessment data. Distribution should be limited to authorized personnel only.



PROTECT YOUR DATA



STRENGTHEN SECURITY



STAY QUANTUM-READY

✦ Secure your Quantum Future with us ✦

KEY PERFORMANCE INDICATORS (KPI)

Cryptographic Security KPI Dashboard



CBOM complete: 90.6%



62.6 / 100

Health Score

WARNING



3.3 / 10

Quantum Readiness

CRITICAL



30.8%

Weak Algorithm Rate

CRITICAL



7.7%

CNSA 2.0 Alignment

CRITICAL

KPI SCORECARD

#	KPI Metric	Value	Status	Target
1	Overall Crypto Health Score	62.6 / 100	Warning	> 70
2	Quantum Readiness Index	3.3 / 10	Critical	> 7.0
3	Weak Algorithm Detection Rate	30.8%	Critical	< 10%
4	CNSA 2.0 Alignment Score	7.7%	Critical	> 70%
5	Certificate Expiry Lead Time	130.7 days	Good	> 90 days
6	Key Lifecycle Compliance Rate	Data unavailable	N/A	> 95%
7	Protocol Compliance (Classical)	99.5%	Good	> 90%
8	Protocol Compliance (Quantum)	39.4%	Warning	> 90%
9	Quantum-Vulnerable Asset Rate	46.2%	Warning	< 20%
10	Hybrid Algorithm Adoption Rate	1.0%	Critical	> 20%
11	Regulatory Compliance Coverage	55.6%	Critical	> 80%
12	CBOM Completeness Score	90.6%	Good	> 80%

EXECUTIVE PRIORITIES

1



Raise quantum readiness

Current score 3.3 / 10

2



Reduce weak algorithms

Detection rate 30.8%

3



Increase hybrid adoption

Current adoption only 1.0%

4



Improve regulatory coverage

Current coverage 55.6%



CONFIDENTIAL — This report contains sensitive security assessment data.
Distribution should be limited to authorized personnel only.



PROTECT YOUR DATA



STRENGTHEN SECURITY



STAY QUANTUM-READY



Secure your Quantum Future with us



NEXT STEPS: EXECUTE YOUR PQC MIGRATION NOW

ALIGNED TO 2029 MANDATES. **NO MARGIN FOR DELAY.**



0-30 DAYS

EXECUTIVE ALIGNMENT

Decide fast. Set direction. Commit.

- ✓ Establish executive ownership and accountability
- ✓ Define quantum risk posture across the enterprise
- ✓ Lock funding, governance, and success metrics



30-90 DAYS

RISK ASSESSMENT & INVENTORY

Expose your vulnerabilities — before they are exploited.

- ✓ Complete cryptographic inventory across all systems
- ✓ Identify quantum-vulnerable algorithms and dependencies
- ✓ Prioritize high-risk assets (HNDL exposure)
- ✓ Define enterprise PQC migration roadmap



90-180 DAYS

PILOT EXECUTION & VALIDATION

Prove readiness. Eliminate uncertainty.

- ✓ Deploy controlled PQC pilots in real environments
- ✓ Validate performance, interoperability, and compliance
- ✓ Identify gaps and remediate immediately
- ✓ Establish deployment playbooks



180+ DAYS

ENTERPRISE DEPLOYMENT

Scale fast. Secure everything. Stay compliant.

- ✓ Roll out PQC across infrastructure, applications, and data layers
- ✓ Integrate into business operations and security frameworks
- ✓ Continuously monitor, optimize, and adapt
- ✓ Achieve full cryptographic resilience



2029 IS NOT A TARGET — IT IS A HARD DEADLINE.

Migration takes years. Delay compounds risk.

DELAY IS RISK. INACTION IS EXPOSURE.



**FUTURE-PROOF
SECURITY**



**ELIMINATE
CRYPTOGRAPHIC RISK**



**MEET REGULATORY
MANDATES**



**PROTECT SENSITIVE
DATA NOW**

Secure your **Quantum** Future with us

LET'S SECURE YOUR QUANTUM FUTURE

CONNECT TODAY. SECURE TOMORROW. LEAD FOREVER.



EMAIL

Christine@Quantum-Infinite.com



ADDRESS

www.Quantum-Infinite.com



**FUTURE-PROOF
SECURITY**



**ELIMINATE
CRYPTOGRAPHIC RISK**



**MEET REGULATORY
MANDATES**



**PROTECT SENSITIVE
DATA NOW**

Begin your **Quantum** Journey with us