

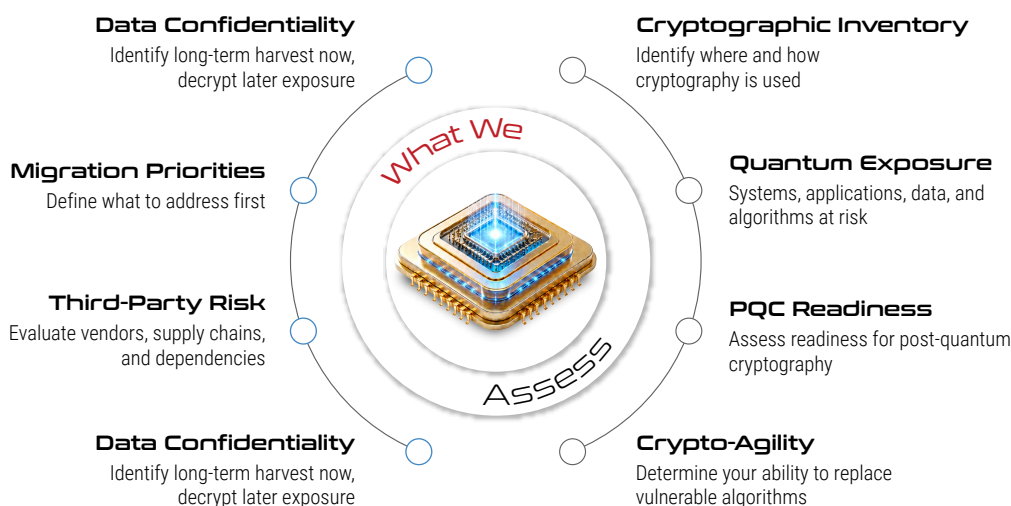
Is Your Encryption Ready for the Quantum Era?

Today's public-key cryptography protects your VPNs, TLS sessions, applications, and sensitive data. Quantum computing will eventually threaten these protections—and adversaries may already be harvesting encrypted data for future decryption.



NIST has finalized post-quantum standards, and the transition clock is running.

The ecfirst Quantum Cyber Risk Readiness Assessment helps you understand your current exposure, identify cryptographic weaknesses, and establish a prioritized path toward quantum resilience.



What You Receive?

Quantum Readiness Report

Current-state maturity and risk rating



Cryptographic Risk Register

Prioritized quantum-related risks and exposures



PQC Migration Roadmap

Sequenced actions to improve quantum resilience



Executive Summary

Leadership-ready findings and recommendations



Why It Matters?

- ✓ Establish a defensible quantum-readiness baseline
- ✓ Uncover cryptographic risk hidden in legacy and third-party systems
- ✓ Protect data requiring confidentiality beyond today's encryption lifecycle
- ✓ Turn quantum risk into a prioritized, actionable program
- ✓ Prepare before customers, regulators, or auditors ask

Who Should Use This Assessment?

CISOs • CIOs • CTOs • Security Architects • Cryptography Owners • Risk, Privacy & Compliance Leaders

Dashboard

TRACERSM
ASSET RISK MANAGEMENT

My Modules

File Dashboard

Data Collection Forms

- Compliance DCF
 - Quantum PQC Self Assessment
 - Dashboard
 - Self Assessment

Quantum PQC Cyber Risk Self Assessment

Overall Status

60%

Download Report

Data Collection Form Status

Governance & Ownership

75%

Details

Encryption & Cryptographic Inventory

55%

Details

Sensitive Data & Harvest-Now-Decrypt-Later Exposure

80%

Details

Infrastructure & Network Crypto-Agility

45%

Details

Technical Migration & Crypto-Agility

70%

Details

Vendors & Supply Chain

50%

Details

Awareness, Policy & Training

90%

Details

Input

Self Assessment

Reference

Client Uploaded Files

Quantum Cyber Risk

Export

Governance & Ownership

0%

Governance & Ownership

5

Encryption & Cryptographic Inventory

5

Sensitive Data & Harvest-Now-Decrypt-Later Exposure

4

Infrastructure & Network Crypto-Agility

3

Technical Migration & Crypto-Agility

4

Vendors & Supply Chain

2

Awareness, Policy & Training

2

Governance & Ownership

Do you have a documented quantum-readiness or post-quantum cryptography (PQC) migration roadmap?

WHY THIS MATTERS

Independent surveys put 91% of security professionals with no formal PQC roadmap. A roadmap is the clearest single signal of readiness, and the first thing an auditor, regulator, or enterprise customer will ask to see.

Response

Yes Partial No Not Sure N/A

Status

1 2 3 4 5 6 7

8 9 10 11 12 13 14

15 16 17 18 19 20 21

22 23 24 25

25 Total Questions

Current Question

Not Answered

Answered Question(s)

Incomplete Question(s)

1

25

0

0

 Peter.Harvey@ecfirst.com



 www.ecfirst.com

© ecfirst. All Rights Reserved. 2026