CYBERINSIGHTS | PRACTICAL SECURITY

PQC readiness without false confidence: build a crypto-agility evidence plan

A practical evidence aid. Not certification or an automated assessment.

1 DISCOVER

Inventory cryptographic use across network, application, identity, software signing, storage and recovery paths. Mark unknowns.

2 CLASSIFY

Separate key establishment from signatures and symmetric encryption. Record the exact implementation and purpose.

3 PRIORITIZE

Consider confidentiality lifetime, signature assurance needs, exposure and replacement lead time. Do not invent a Q-Day date.

4 CONFIRM SUPPORT

Check supported protocol profiles, libraries, hardware and partner dependencies. Algorithm standardization is not product validation.

5 PILOT

Use an authorized isolated service with representative clients. Preserve current security and define rollback.

6 VERIFY

Record actual mechanism, authentication, interoperability, performance, failure behaviour and a complete transaction.

7 REVIEW

Track blockers and unknown critical services separately. Recheck suppliers and protocol guidance before rollout.

Evidence: scope / owner / expected result / observation / gaps / reviewer / recheck

Sources: NIST: Approved post-quantum cryptography FIPS; NIST NCCoE: Migration to post-quantum cryptography; NIST CSWP 39upd1: Crypto agility; NIST SP 800-52 Rev. 2: TLS implementation guidelines. Full links and limitations are in the companion guide. Examples are hypothetical; no customer environment was tested.