OPSWAT.

A Cybersecurity Guide to Quantum Readiness

What drives quantum migration, what governments require, and a practical checklist to get started.

OPSWAT.

Table of Contents

01 The Need for a Quantum-Ready Security Architecture

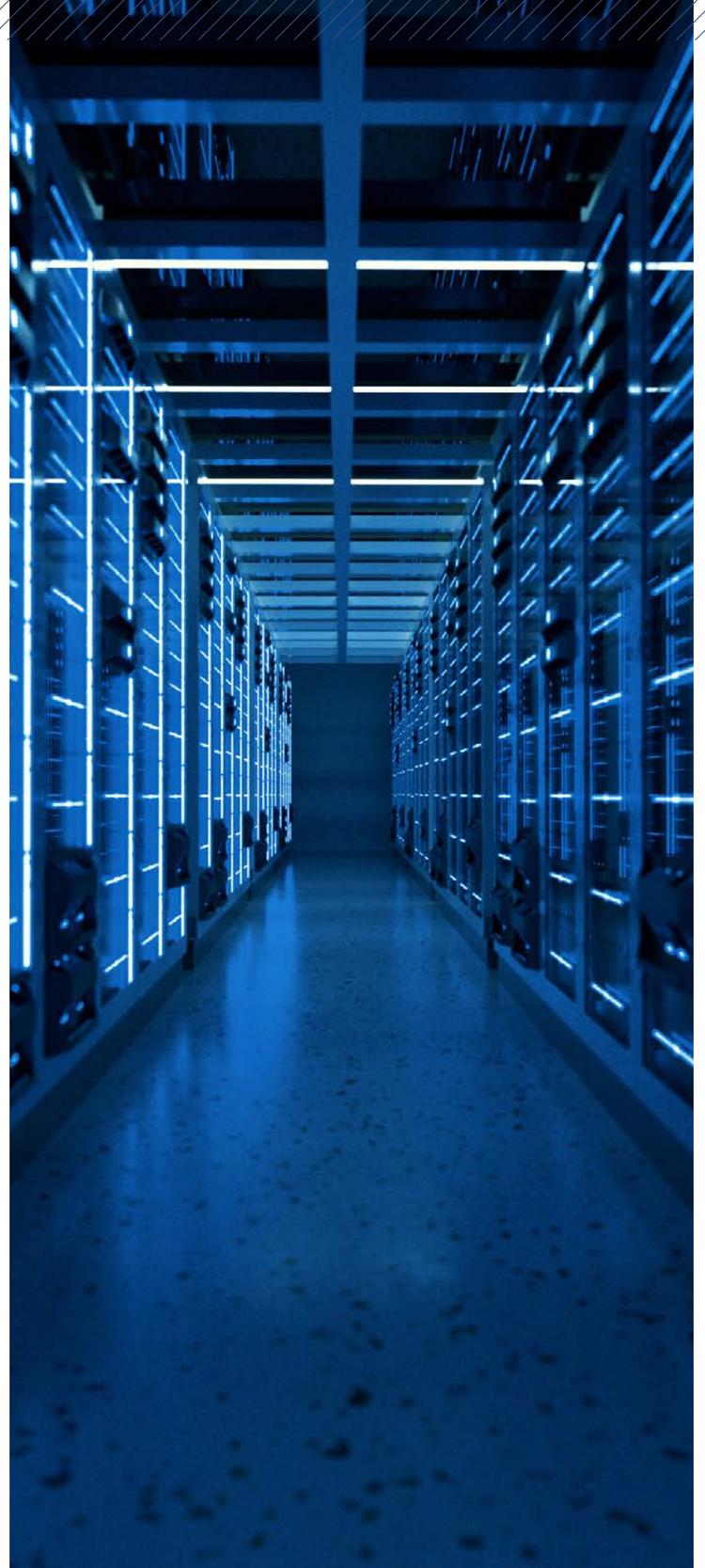
02 Why Prepare Early for the Quantum Era

03 Key Challenges

04 Government Requirements and Regulatory Frameworks

05 Quantum Readiness Checklist

06 Next Steps Toward Quantum Readiness



01

The Need for a Quantum-Ready Security Architecture

While quantum computers capable of breaking today's public-key cryptography remain beyond current capabilities, preparation for quantum readiness cannot wait. Migration across critical infrastructure takes years, and governments have already begun setting concrete deadlines, adding more urgency to the transition to quantum-resistant security.

A practical quantum-safe architecture layers three complementary technologies that wrap around the switches, HSMs (Hardware Security Modules), and control systems an organization already owns, so there is no rip-and-replace:

- PQC (Post-Quantum Cryptography) for scalable algorithms and authentication
- QKD (Quantum Key Distribution) for keys whose interception is physically detectable
- Data diodes for hardware-enforced one-way transfer that keeps key infrastructure unreachable from untrusted networks

02

Why Prepare Early for the Quantum Era

Harvest Now, Decrypt Later (HNDL)

Adversaries can record encrypted traffic today and decrypt it once sufficiently capable quantum computers exist. Data that must stay confidential for 10 to 20 years is already exposed. NIST names HNDL as a main reason the transition is urgent.

Long Migration Lead Times

Cryptography is embedded in applications, devices, certificates, HSMs, and supplier products. Inventory, testing, and staged rollout take years, not quarters.

Authenticity as Well as Confidentiality

Quantum-vulnerable signatures put software updates, certificates, and trust anchors at risk. Strong post-quantum authentication such as ML-DSA counters on-path (person-in-the-middle) attacks.

Defense in Depth

No single layer should carry the risk. PQC provides scalable algorithms and authentication. QKD provides keys whose interception is physically detectable. Hardware-enforced one-way transfer keeps key systems unreachable from untrusted networks.

03

Key Challenges

Visibility

Most organizations cannot list where cryptography is used, including third-party services and embedded devices.

Rip-and-Replace Risk

Operational technology, HSM estates, and certified systems cannot be swapped out. Migration must layer onto existing infrastructure.

Supply Chain Dependencies

Much of the exposure lies in vendor products and partner interfaces that you do not control.

Protecting the Key Path

Key management systems and delivery middleware become high-value targets and must be isolated from the untrusted side.

Operations and Audit

Teams must plan key consumption, buffering, time synchronization, degraded modes, and certification reviews for new key sources.

Moving Guidance

Standards and mandates continue to evolve, so designs must be crypto-agile.



04

Government Requirements and Regulatory Frameworks

The table summarizes published timelines relevant to critical infrastructure operators. Confirm applicability to your sector and jurisdiction with your compliance team.

Framework	Requirements highlights	Key dates
NIST FIPS 203, 204, 205	Standardize post-quantum key establishment (ML-KEM) and digital signatures (ML-DSA, SLH-DSA). These are the algorithms to migrate to.	Published August 2024
NIST IR 8547 (final)	Sets the transition plan away from quantum-vulnerable algorithms and supports hybrid approaches. It also covers the cryptographic supply chain.	Final report published October 27, 2026
US NSM-10 and Executive Order 14412	NSM-10 sets 2035 as the primary federal migration target. EO 14412 accelerates it for federal high-value assets and high-impact systems.	2030 key establishment 2031 (digital signatures) 2035 overall
NSA CNSA 2.0 (National Security Systems)	Requires quantum-resistant algorithms in national security systems and affects contractors that supply them. Verify exact milestones in the NSA CNSA 2.0 FAQ.	New acquisitions from January 1, 2027 (secondary sources; verify)
EU Coordinated Implementation Roadmap	Member States start migration, with high-risk and critical sectors first, such as energy, finance, defense, and health.	National plans by end of 2026 High-risk systems by 2030 Remainder by 2035
UK NCSC migration timelines	Three phases: discover and plan, execute priority upgrades, then complete migration.	2028 plan 2028–2031 priority upgrades 2031–2035 completion
NIS2 and DORA (EU)	Do not name quantum threats directly, but require state-of-the-art cryptographic controls, risk management, and resilience. Treat cryptographic inventory and crypto-agility as practical evidence.	In force (check national transposition)
IEC 62443 (industrial security)	Sector design constraint for operational technology. Plan to map quantum-safe designs to its zones and conduits. Confirm any quantum-specific requirements with your assessor.	Per sector and assessor

Dates for NIST, NSM-10, and EO 14412 are from NIST's October 2026 announcement. EU and UK dates are from the European Commission and NCSC publications as reported by secondary sources. CNSA 2.0 dates are from secondary sources and should be verified with the NSA. NIS2, DORA, and IEC 62443 are summarized at a high level; they are not quantum-specific mandates.

OPSWAT.

05

Quantum Readiness Checklist

01 Discover
Know what you protect

- [ ] **Name an Owner**
  Assign one accountable executive for quantum migration, with budget authority.
- [ ] **Build a Cryptographic Inventory (CBOM)**
  List every use of cryptography: applications, certificates, VPNs, code signing, HSMs (Hardware Security Modules), and third-party services.
- [ ] **Classify Data by Shelf Life**
  Data that must stay confidential for 10 years or more is already exposed to HNDL (Harvest Now, Decrypt Later). It sets your migration order.
- [ ] **Map Supplier Dependencies**
  Ask vendors for written post-quantum roadmaps for embedded devices and partner interfaces.

02 Design
Build quantum-safe layers around what you already own

- [ ] **Adopt NIST-Standardized Algorithms**
  Use ML-KEM (FIPS 203) for key establishment and ML-DSA (FIPS 204) or SLH-DSA (FIPS 205) for signatures.
- [ ] **Layer PQC with QKD Where Keys Must be Strongest**
  PQC provides scalable algorithms and authentication. QKD (Quantum Key Distribution) delivers keys whose interception is physically detectable. IonQ supplies the QKD layer.
- [ ] **Protect the Key Path with Hardware-Enforced One-Way Transfer**
  Place MetaDefender™ NetWall Optical Diode paths between key management systems and the secure zone, so key infrastructure is unreachable from the untrusted side.
- [ ] **Feed Quantum-Generated Keys into Existing HSMs**
  Use standard interfaces (ETSI GS QKD 014, PKCS#11) so no HSM is replaced.
- [ ] **Design for Crypto-Agility**
  Centralize trust stores, shorten certificate lifetimes, and remove hard-coded algorithm choices.

03 Prove and Govern
Pilot, then scale link by link

- [ ] **Pilot One High-Value Link**
  Run hybrid key exchange on one production path. Measure latency, throughput, and failure modes, and rehearse degraded-mode and rollback drills.
- [ ] **Update Procurement Language**
  Require post-quantum support in every new contract that runs past 2030.
- [ ] **Align to Government Timelines and Report to the Board**
  Map your plan to the published mandates, such as NIST FIPS 203/204/205 and CNSA 2.0, and track one readiness metric, including the percentage of cryptography migrated.

06

Next Steps Toward Quantum Readiness

Quantum computing is progressing from experimental prototypes to practical systems, making preparation for quantum-era security an ongoing effort. Hosting a workshop on countrywide deployment of QKD/PQC Cross-Domain Solutions is a good start. A dedicated workshop can help assess the existing network topology and deployment constraints, establish a current-state assessment, define a target architecture, and develop a sequenced migration plan.

Become Quantum-Ready with OPSWAT

Scan the QR code or visit us at:
opswat.com/get-started
sales@opswat.com

OPSWAT.
Protecting the World's Critical Infrastructure

©2026 OPSWAT Inc. All rights reserved. OPSWAT, Metascan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc. Rev. November 13, 2026 4:46 PM