digicert®

Cross the Quantum Divide

The Ultimate Guide to Post-Quantum Cryptography

GUIDE

1. Executive Overview

Standing at the Divide

The emergence of quantum computing has brought us to a critical juncture. Every major advance in computing has forced organizations to rethink how they secure information, and past cryptographic migrations show transitions take years, not months—planning must start early.

This moment is the quantum divide. On one side sit classical algorithms that rely on factoring large prime numbers and today's trust chains; on the other are NIST-standardized post-quantum cryptography (PQC) algorithms now being adopted across governments and enterprises.

The Compliance Clock Is Ticking

- **CNSA 2.0:** Mandates the adoption of PQC across U.S. National Security Systems by 2030, with interim miltones already in effect.
- **EU CRA and DORA:** Security and operational resilience obligations that align with PQC readiness in the latter half of the decade.
- **U.S. Executive actions:** Requires federal agencies to inventory all cryptographic systems and prioritize those vulnerable to quantum threats.
- **Translation:** The need to be quantum secure is closer than it looks. At enterprise scale, cryptographic transitions take a decade—regulators and agencies already expect preparation to be underway.

Quantum computers capable of breaking today's encryption—known as cryptographically relevant quantum computers (CRQCs)—do not yet exist, but the research curve is steep. Gartner predicts that by 2029, current algorithms will be ineffective. Industry experts warn that when a CRQC arrives, the migration window could be compressed to as little as three years—far shorter than past cryptographic transitions.

Crossing the quantum divide isn't just an abstract risk. It's a call to safeguard operations, compliance, and long-term resilience. Encryption underpins everything—securing communications, authenticating devices, protecting long-lived documents, and maintaining trust in the software supply chain. Without a transition strategy, organizations risk outages, regulatory non-compliance, and the loss of customer confidence.

The good news is that the other side of the divide is visible. NIST has finalized the first wave of post-quantum standards (ML-KEM for encryption, ML-DSA for signatures, SLH-DSA for long-lived use cases), and industry bodies such as the NSA with CNSA 2.0 are publishing migration roadmaps. Industry leaders are already using PQC in production, proving that it can be integrated into existing infrastructures.

This guide is designed to help you chart your path across the divide. Throughout, you'll find practitioner tools—CBOM templates, pilot worksheets, a governance RACI, and a vendor briefing checklist—to move from awareness to execution.

The guide includes:

- ✓ A clear explanation of the quantum threat and its impact on today's cryptography.
- ✓ Timelines and milestones from standards bodies, regulators, and governments.
- ✓ A practical playbook for building a PQC migration strategy, from inventory to pilots to enterprise-wide execution.
- ✓ Common migration challenges—from certificate chaining to harware compatibility—and how to address them.
- ✓ A look at how DigiCert can support your journey with cryptographic agility, lifecycle automation, and developer tools.
- ✓ Opportunities to test and learn in controlled environments and even participate in tabletop workshops that bring PQC planning to life.

Crossing the quantum divide will require planning, investment, and coordination across your organization. But it's not a leap into the unknown. With the right approach, the migration becomes a deliberate path that positions you not only to withstand the quantum era, but to thrive in it. DigiCert is here to help you make that crossing.

2. The Quantum Divide Explained

To understand why PQC is necessary, it helps to first understand the divide itself: the gap between the cryptographic protections we rely on today and the vulnerabilities introduced by advances in quantum computing.

Quantum Computing in Simple Terms

Quantum computers use qubits that can exist in multiple states simultaneously, enabling certain problems to be solved in parallel. For many industries, this holds enormous promise—accelerating drug discovery, optimizing logistics, and advancing materials science. But for cybersecurity, the same power presents a profound challenge.

The enterprise takeaway: Once a cryptographically relevant quantum computer (CRQC) exists, the public-key algorithms we rely on today—RSA and ECC—will no longer hold. This doesn't mean the end of public-key cryptography altogether. New post-quantum standards such as ML-KEM (for encryption) and ML-DSA (for signatures) are also public-key algorithms, but they're built on mathematical problems (like lattices) that quantum computers cannot efficiently solve. In other words: We're transitioning away from RSA and ECC, not away from public key cryptography itself.

Why Current Cryptography Breaks

The backbone of today's digital trust is asymmetric (or public key) cryptography. Protocols like RSA and ECC are secure because factoring large prime numbers or solving discrete logarithms is computationally infeasible for classical computers.

Quantum algorithms change that equation.

The most critical is Shor's algorithm, which collapses the hardness assumptions behind RSA and ECC, rendering them insecure once a CRQC exists. Symmetric cryptography is also affected, though less dramatically: Grover's algorithm reduces the effective strength of symmetric keys, requiring longer key sizes to maintain security. However, Grover's algorithm can't be parallelized and is far more difficult to run successfully, even on a CRQC.

The Result: The cryptography that secures communications, authenticates identities, and protects sensitive data today will be vulnerable in a post-quantum world.

Why this matters to operations

- **Long-lived assets:** Medical and industrial devices and digitally signed contracts must remain verifiable for decades.
- **Harvest-now, decrypt-later:** Data exfiltrated today can be decrypted once quantum computing becomes broadly accessible.
- **Trust chain fragility:** Compromises internal public key infrastructures can halt operations while processes are upgraded and trust heirarchies are rearchitected.
- **Pervasive impact:** Digital signatures, secure identities, and encrypted communications are fundamental to internet security, which means cryptography is in everything. All existing asymmetric implementations are vulnerable and must be replaced.

Where Cryptography Lives

It's easy to think of cryptography as just a layer in web browsers or VPNs, but its reach is far deeper and broader. Asymmetric cryptrography and digital certificates underpin:

Network Security (TLS/PKI): Digital certificates and asymmetric algorithms secure TLS connections, VPNs, and encrypted messaging. A CRQC would break the foundation of secure internet communications.

Software Trust (Code Signing): Application code signing, update verification, and supply chain integrity all rely on public key algorithms. With software often used for years, quantum-safe signing is critical for long-term trust.

Device Security (IoT & Embedded): Device identities, firmware updates, and secure boot processes depend on cryptographic signatures. Without PQC, CRQCs could enable unauthorized firmware or compromised devices to enter critical environments.

Data Protection (Encryption & Email): Encrypted storage, digital signatures, and secure email (S/MIME) rely on public-key cryptography. PQC upgrades will be required for both message confidentiality and signature validation.

Documents & Records (Long-Term Verifiability): Legal, healthcare, and government records must remain verifiable for decades. Long-term digital signatures will require re-signing with quantum-safe methods to avoid invalidation.

Because cryptography is woven through so many layers of modern digital infrastructure, transitioning to PQC is not as simple as swapping one algorithm for another. It is a systemic change, with ripple effects across applications, devices, and supply chains.

The Nature of the Divide

What makes the quantum divide unique is not just the looming technical threat, but the mismatch between how long migrations take and how short the warning window may be. When a cryptographically relevant quantum computer becomes operational, the window for securing vulnerable systems may be as little as three years.

The divide isn't hypothetical. It's measurable, documented in standards, and one that every organization must cross.

3. The Bridge Timeline: How Long Is the Divide?

When planning a major transition, one of the most important questions is: How much time do we have? For post-quantum cryptography, the answer is complex. On one hand, CRQCs don't yet exist. On the other, standards are already in place and regulators are setting deadlines. The width of the divide isn't the number of years until a CRQC exists (Q-Day), it's how long your organization needs to prepare—and for most, that spans multiple budget cycles.

The Standards Milestones

The first major milestone was the NIST PQC competition, which began in 2016. After years of global collaboration and review, NIST finalized its first set of post-quantum algorithms in 2024:

- **ML-KEM (formerly Kyber):** Key encapsulation for secure communications.
- **ML-DSA (formerly Dilithium):** Digital signatures for authentication.
- **SLH-DSA (formerly SPHINCS+):** Hash-based signatures for long-term use cases.

PQC Standards Insight – Different Paths Across the Atlantic

- U.S. (NIST): ML-KEM + ML-DSA as primary PQC standards.
- Europe (BSI, ANSSI): Broader acceptance, including unstructured lattices and composites.
- Impact: Multinationals may need region-specific algorithm support.

DigiCert's Role:

DigiCert is active in both ecosystems, giving customers early visibility into evolving requirements.

Additional algorithms, including Falcon, expand the options for specific performance profiles. With these standards in place, the building blocks for PQC migration are no longer theoretical—they're real, vetted, and available.

Government and Regulatory Deadlines

Governments are moving quickly to set expectations:

- **CNSA 2.0 (National Security Agency, U.S.)** requires quantum-resistant algorithms for national security systems by 2030, with interim requirements already in effect for some use cases.
- **The European Union's CRA (Cyber Resilience Act)** and **DORA (Digital Operational Resilience Act)** include provisions that align with PQC-readiness in the second half of the decade.
- **Executive Orders in the U.S.** have directed federal agencies to inventory cryptographic assets and prepare migration plans.

These policies drive home two critical realities: Migration isn't optional, and early preparation is expected, particularly for regulated industries.

The Compression of the Window

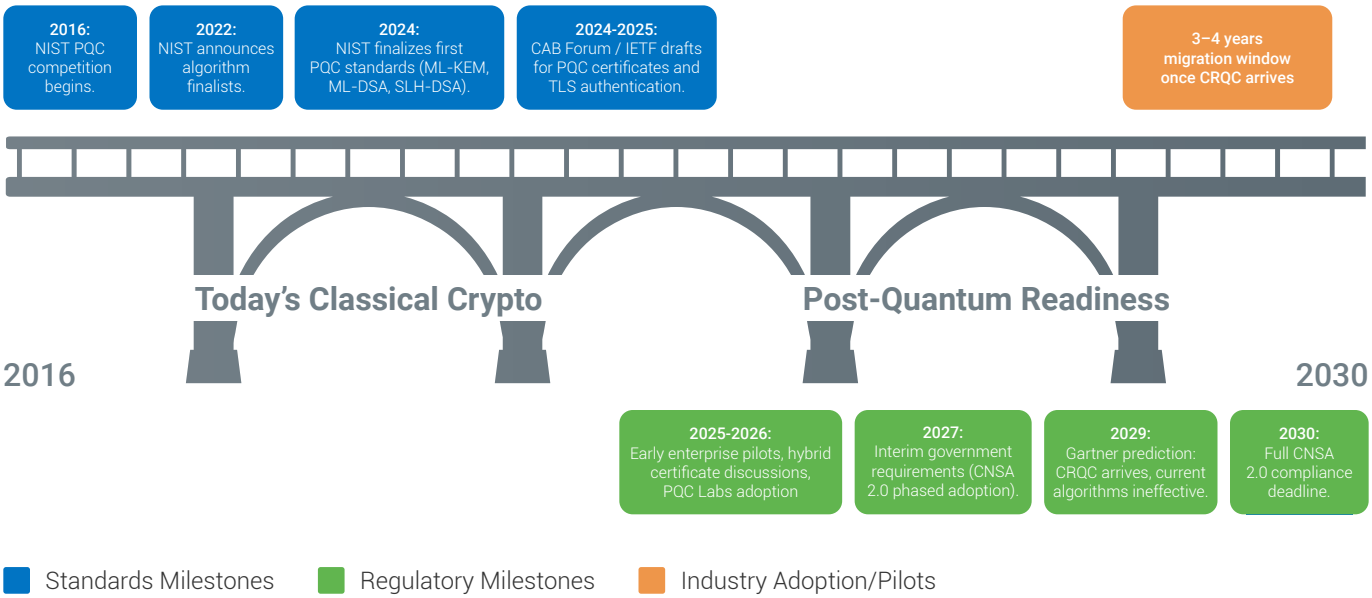
Experts project that once a CRQC is achieved, the window for migration will shrink dramatically. Gartner predicts that current algorithms will be ineffective by 2029. NIST, NSA, and industry groups advise that organizations should budget no more than three to four years to complete their transition once quantum computers reach maturity.

To put this in perspective:

- It took nearly a decage to ransition from SHA-1, an outdated algorithm, to the stronger SHA-2.
- Despite industry consensus, the adoption of TLS 1.2, the standard for secure communications, required many years.
- PQC will touch far more systems, including those with deeply embedded cryptography (IoT, industrial controls, medical devices).

If history is a guide, migrations are always slower and more complicated than expected. Which means the real timeline is not defined by when quantum computers arrive, but by how long organizations need to adapt.

Bridge to Post-Quantum Readiness



Crossing at the Right Time

The "bridge" across the quantum divide is already under construction. Standards exist. Policies are in motion. Pilots are happening today. Organizations that begin discovery and testing now will be positioned to cross steadily and confidently. Those who delay will face compressed timelines that drive up cost and complexity.

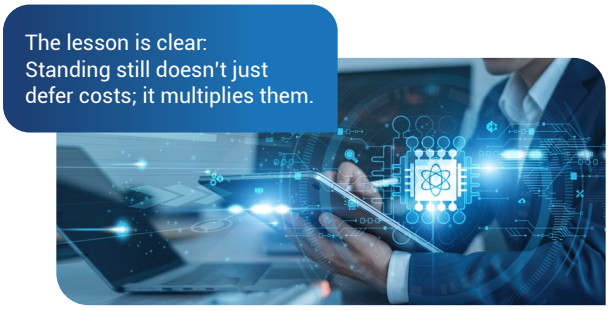
4. Why Standing Still Is Not an Option

Organizations often face competing priorities when it comes to security investments. With quantum computers not yet at scale, it may be tempting to push post-quantum cryptography preparation to the back of the queue. But waiting invites **compliance exposure, vendor bottlenecks**, and **business disruption**. By the time a CRQC is demonstrated, procurement queues, hardware lead times, and scarce PQC expertise will drive costs up and flexibility down.

The Hidden Cost of Delay

Migrations are rarely smooth when left until the last minute. Past cryptographic migrations show that delays drive up cost and complexity once vulnerabilities become undeniable. PQC presents an even bigger challenge because:

- Cryptography is deeply embedded across applications, devices, and supply chains.
- Migration will involve not just software updates, but coordination with vendors, hardware providers, and regulators.
- The compressed window for change once a cryptographically relevant quantum computer arrives may be as little as three years—far less than past transitions.



Compliance and Regulatory Pressure

Regulators are not waiting. Governments are already publishing timelines that assume enterprises are preparing today. As outlined earlier (see Government and Regulatory Deadlines), mandates like CNSA 2.0 in the U.S. and CRA/DORA in Europe are already in motion, and federal executive orders require cryptographic inventories and migration plans.

For regulated industries such as finance, healthcare, and critical infrastructure, compliance requirements will arrive earlier than the arrival of a CRQC. Organizations that wait may find themselves scrambling to meet obligations under intense scrutiny.

Operational Disruption

Delaying also increases the likelihood of operational disruption. Consider the systems that rely on long-lived cryptography: medical devices with 20-year lifespans, industrial control systems designed to operate for decades, or archived legal and healthcare records that must remain verifiable for the long term. Delaying migration raises the risk of operational disruption—especially in systems with long-lived cryptography—leading to outages, verification failures, and costly retrofits.

Strategic Disadvantage

Finally, delay comes with a competitive cost. Enterprises that start their migration early will:

- Gain practical experience with pilot deployments.
- Build credibility with regulators, partners, and customers.
- Avoid being locked into vendor timelines that may not match business needs.

By contrast, those that defer action risk being bottlenecked by supply chain dependencies and competing with others for limited expertise and resources once the deadline arrives.

The Case for Moving Now

Beginning the process today—even with small steps like running a single pilot—reduces long-term costs and builds internal expertise. The decision isn't whether to cross the quantum divide, but whether to start building your bridge now—or wait until time is almost up.

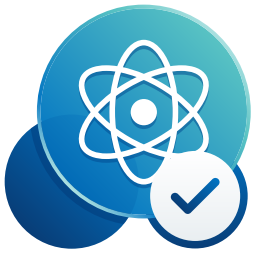
5. Building Your Bridge: The PQC Readiness Playbook

Every successful crossing starts with a blueprint. For PQC, that blueprint is your organizational playbook: the strategy, processes, and artifacts that turn awareness into action.

The Five Steps at a Glance

Building your PQC readiness playbook involves five essential steps:

1. **Create a Cryptographic Bill of Materials (CBOM):**
   Start building visibility into where cryptography lives across your organization.
2. **Pilot a Representative Application:**
   Test PQC in a controlled environment to uncover challenges early.
3. **Define Policies, Governance, and Rollback Plans:**
   Establish clear rules and ownership to guide the migration.
4. **Secure Executive Sponsorship and Budget:**
   Translate technical urgency into business terms and ensure long-term support.
5. **Engage Vendors and Ecosystem Partners:**
   Align your suppliers and partners so your migration isn't held back by external dependencies.



Each of these steps is expanded below with practical guidance, sample templates, and common pitfalls to avoid.

Step 1: Create a Cryptographic Bill of Materials (CBOM)

Why it matters: You can't migrate what you don't know exists. But trying to map your entire environment upfront can lead to analysis paralysis. Instead, start incrementally—build your CBOM one application or system at a time, beginning with those that are most business-critical or long-lived. Each pilot (see Step 2) should help build your CBOM, giving you both inventory and real-world lessons without stalling progress.

How to do it:

- **Start small:** Pick a critical application or system and document its cryptography in detail.
- **Expand outward:** Once you've mapped one application, add supporting systems (APIs, libraries, dependent services) and gradually build coverage.
- **Use a mix of tools:** Automated discovery (vulnerability scanners, certificate lifecycle managers, code analysis tools) is helpful, but manual input from system owners is often needed to fill gaps.
- **Capture the essentials:** Document details like the algorithm (RSA, ECC, AES, SHA), key lengths, certificate expirations, trust anchors, storage type (HSM, token, vault), business owner, vendor dependencies, and criticality.

Pitfalls to avoid:

- **Trying to capture everything at once:** What feels like a shortcut will actually slow progress and create the risk of never finishing.
- **Treating the CBOM as a one-time audit:** Cryptography changes constantly; establish a process for continuous updates.
- **Over-focusing on certificates:** Keys, libraries, and code-signing mechanisms are equally important.

Sample Cryptographic Bill of Materials (CBOM) Template:

Visual/artifact: A sample CBOM template with pre-populated fields and categories.

Field	Description	Example Entry
Asset Name	System, application, or device where crypto is used	Online Banking Portal
Owner	Business/system owner	eBanking Team
Algorithm	Current algorithm in use	RSA
Key Length	Size of the key	2048 bits
Certificate Expiration	Expiry date if applicable	12/01/2026
Trust Anchor / CA	Root or issuing CA	DigiCert Global Root G2
Use Case	Signing, encryption, authentication, key wrapping	TLS handshake
Storage Type	Where key material resides	HSM (on-prem)
Criticality	Business impact if compromised	High (regulatory + customer-facing)
Vendor Dependency	Third-party vendor/software involved	Apache Tomcat
Migration Priority	Rank (High/Med/Low)	High

Guidance for use: Use the CBOM template provided, but start with a single application filled out end-to-end. Treat this as your first "slice" of the inventory, then expand with each pilot.

The Trap:

Trying to inventory every cryptographic asset across your enterprise before doing anything else.

The Fix:

- Pick one critical application.
- Map its cryptography in detail (your first CBOM slice).
- Run it through a PQC pilot.
- Feed lessons learned back into your inventory and governance.

The Benefit:

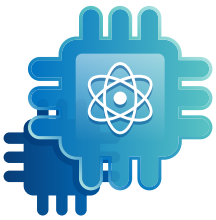
You build momentum, get immediate insights, and avoid the "stall- out" that comes from boiling the ocean.

Key Message:

Your first pilot is also your first CBOM entry. Run it to the ground, then expand outward.

Step 2: Pilot a Representative Application

Why it matters: Pilots aren't just for testing PQC—they're also how you expand your CBOM in manageable chunks. By picking a first application and "running it to the ground," you avoid the trap of endless inventory and instead get immediate, actionable results that inform both your playbook and your migration priorities.



How to do it:

- **Select a representative application:** Choose one that is business-critical, long-lived, or heavily integrated (e.g., a customer-facing service, IoT device, or DevOps platform).
- **Map its cryptographic footprint:** Document all algorithms, keys, and certificates used as part of the pilot—this becomes the first slice of your CBOM.
- **Test real-world scenarios:** Replace vulnerable algorithms with PQC equivalents, experiment with hybrid certificates, and measure impacts (handshake times, key sizes, interoperability).
- **Feed results into planning:** Capture what broke, what needed the most effort, and which skills or vendor dependencies surfaced.

Pitfalls to avoid:

- **Picking an application that's too trivial:** It won't reveal real-world challenges.
- **Failing to document findings:** Pilots are only valuable if lessons are captured and fed back into governance and inventory.
- **Treating the pilot as a standalone exercise:** Its results should shape both the CBOM and the broader migration strategy.

Visual/artifact: A pilot project worksheet with space for objectives, metrics, test results, and lessons learned.

Pilot Project Worksheet:

Objective: Define the scope, risks, and outcomes of a PQC pilot.

Pilot Application/System: (e.g., Customer-facing web app)

Reason for Selection: Representative of larger environment, but safe for testing.

Algorithms Under Test: (e.g., ML-KEM hybrid TLS certs)

Test Environment: (Lab, staging, production subset)

Metrics to Track:

- Handshake time / latency impact
- Key size differences
- Application interoperability
- User experience impact

Challenges Identified: (Document technical issues, vendor gaps, tooling limitations)

Skills Gaps Identified: (Note training needs for staff)

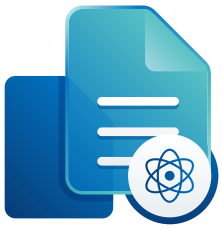
Lessons Learned: (e.g., hybrid certs work in browsers A, B, but not in legacy OS X versions)

Next Steps: (Scale to additional apps, adjust governance policy, engage vendors)

Guidance for use: Use the pilot worksheet to track objectives, metrics, challenges, and lessons learned. Include a section for "CBOM expansion" so the cryptographic inventory grows in lockstep with your pilot projects.

Step 3: Define Policies, Governance, and Rollback Plans

Why it matters: PQC migration isn't just a technical exercise—it touches compliance, procurement, vendor management, and business continuity. Strong governance ensures the transition stays controlled.



How to do it:

- **Policies to define:**
  - **Algorithm adoption policy:** Which PQC algorithms to use, and where.
  - **Key management policy:** How PQC keys will be generated, stored, and rotated.
  - **Exception handling:** When legacy algorithms are permitted (and for how long).
- **Governance structures:**
  - Assign ownership for cryptographic decisions (CISO, PKI team, architecture board).
  - Create a PQC steering committee that includes security, IT, compliance, procurement, and risk management.
  - Align with enterprise change management processes.
- **Rollback strategies:**
  - Plan for hybrid modes where pure PQC causes issues.
  - Define rollback triggers (e.g., latency above threshold, incompatibility with critical vendor systems).
  - Ensure ability to revert without service outages.

Pitfalls to avoid:

- **Writing policies without stakeholder input:** If developers, compliance officers, or vendors aren't consulted, policies won't be followed.
- **Overlooking rollback:** Without safety valves, organizations risk outages.

Visual/artifact: A sample governance RACI chart (who is Responsible, Accountable, Consulted, Informed).

Sample Governance RACI Chart:

Activity	Responsible	Accountable	Consulted	Informed
Cryptographic Inventory (CBOM)	PKI Team	CISO	App Owners, Compliance	CIO
Pilot Projects	Engineering	CTO	PKI, Ops, Vendors	CISO
Policy Development	Risk/Compliance	CISO	Legal, Security, Dev	CIO, Board
Rollback Plans	Ops	CTO	PKI, Vendors	CISO
Vendor Engagement	Procurement	CIO	Security, Risk	CISO, Board
Migration Execution	Engineering + Ops	CTO	Vendors, PKI, Compliance	CIO, Board

Guidance for use: Adapt roles to fit your org structure. The key is clarity—no task should exist without clear ownership.

Step 4: Ensure Executive Sponsorship and Budget

Why it matters: PQC migration is a multi-year, enterprise-wide effort. Without executive buy-in, it will stall.

How to do it:

- **Translate technical risk into business language:**
  - "A three-year migration window vs. a ten-year migration need."
  - "Compliance penalties if unprepared for CNSA 2.0 or CRA."
  - "Operational outages if cryptography in long-lived systems breaks unexpectedly."
- **Budget categories to plan for:**
  - Discovery and inventory (tools, audits).
  - Pilots and test environments.
  - Vendor coordination and procurement updates.
  - Workforce training.
- **Engagement strategy:**
  - Use board-friendly visuals (timelines, bridge metaphor).
  - Share competitor readiness examples—"others are already preparing."
  - Frame PQC as part of business continuity, not just security.

Pitfalls to avoid:

- Asking for "security spend" without showing revenue or continuity impacts.
- Waiting too long—budgets are easier to secure when linked to compliance deadlines.

Visual/artifact: A sample board presentation slide summarizing PQC business impact.

Sample Board Presentation Slide:

Title: *Why Post-Quantum Cryptography Requires Action Now*

The Divide: Current algorithms (RSA, ECC) will be broken by quantum computing.

The Window: Migration may take 8–10 years, but the usable timeline could be as short as 3–4 years once a CRQC arrives.

The Risk: Delaying action increases compliance penalties, operational outages, and cost.

The Opportunity: Starting now builds resilience, strengthens trust, and avoids rushed, expensive retrofits.

Ask: Executive sponsorship and budget for a phased PQC readiness program.

Guidance for use: This single-slide summary arms CISOs to brief boards quickly and in non-technical language.

Step 5: Engage Vendors and Ecosystem Partners

Why it matters: No organization controls every system or dependency in its environment. PQC readiness requires coordination across the supply chain.

How to do it:

- **Map dependencies:** List critical vendors (cloud, hardware, software, PKI providers).
- **Ask the right questions:**
  - Do you support NIST PQC algorithms today?
  - If not, what's your timeline for support?
  - Will you provide hybrid and PQC-only certificate support?
  - How are you handling interoperability testing?
- **Document vendor commitments:** Incorporate responses into your migration timeline.
- **Collaborate:** Participate in standards bodies (IETF, CA/B Forum) and industry alliances.

Pitfalls to avoid:

- Assuming vendors will be ready "in time." Vendor timelines often lag.
- Not aligning vendor roadmaps with your own deadlines.

Visual/artifact: A vendor briefing checklist with sample questions to send suppliers.

Vendor Briefing Checklist:

Questions to Send Vendors:

1. Do you currently support NIST PQC algorithms (ML-KEM, ML-DSA, SLH-DSA)?
2. If not, what's your timeline for adding support?
3. Will you provide hybrid and PQC-only certificate support?
4. Have you tested interoperability with browsers, operating systems, and middleware?
5. How are you addressing PQC in your product roadmap?
6. What migration guidance or documentation do you provide to customers?
7. Who is your internal point of contact for PQC readiness?
8. Will your SLAs or contracts be updated to reflect PQC migration commitments?

Guidance for use: Capture vendor responses in your CBOM/migration plan. Use the checklist to flag suppliers who may delay your readiness.

Putting It Together

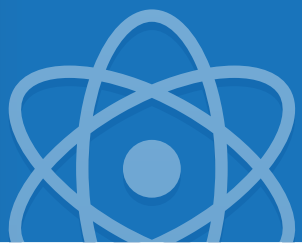
The PQC playbook is more than a plan—it's the foundation for your organization's future digital trust. By investing in discovery, piloting, governance, sponsorship, and ecosystem alignment, you're not just preparing for a technical migration. You're ensuring that your business, your customers, and your partners can confidently cross the quantum divide.

6. Obstacles on the Bridge: Migration Challenges

Even with a strong playbook in hand, no bridge is built without challenges. Post-quantum cryptography (PQC) migration is no different. The complexity lies not in choosing an algorithm, but in making cryptography function across an interconnected web of applications, devices, and vendors. Recognizing common challenges in advance will help your organization prepare strategies to address them before they become roadblocks.

PQC Standards Insight – TLS 1.3 and Quantum-Safe Authentication

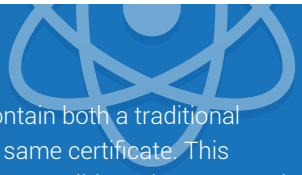
- PQC support will be TLS 1.3+ only.
- TLS 1.2 will not be updated, despite wide use.
- Options for TLS 1.2 users:
  - Accelerate TLS 1.3 migration.
  - Consider bespoke, non-standard extensions (risky).
- **Action:** Begin TLS 1.3 adoption now to align with PQC readiness.



1. Certificate Chaining and Hybrid Certificates

- **The challenge:** Existing systems are tightly bound to classical algorithms like RSA and ECC. Switching abruptly to PQC could break trust chains, cause interoperability failures, or lock out older systems.
- **Why it matters:** Digital certificates anchor most secure connections. If certificate trust chains fail, communication stops.
- Approaches:
  - Experiment with hybrid and PQC-only certificates to identify compatibility gaps.
  - Be clear: These are temporary tools for migration, not permanent solutions. Every system will eventually need to undergo a breaking change to fully adopt PQC.
  - Plan for gradual PQC introduction in test environments before rolling out to production.

PQC Standards Insight – Hybrid vs Composite Certificates



- **Hybrid:** Combing classical and PQC cryptographic in on certificate. Hybrid certificates contain both a traditional cryptographic algorithm (such as RSA or ECC) and a post-quantum algorithm within the same certificate. This approach enables backward compatibility during the transition period, ensuring systems can validate signatures using existing methods while introducing PQC support for future resilience.
- **PQC-Only:** Built entirely on post-quantum cryptography. PQC-only certificates rely exclusively on quantum-resistant algorithms for their public keys and signatures. They represent the end state of the migration, removing dependence on legacy algorithms and delivering full protection against both classical and quantum attacks.
- **Reality check:** Neither hybrid nor composite eliminates the need for breaking changes. They can help with testing and limited transition scenarios, but ultimately every system must adopt pure PQC.
- **DigiCert's view:** The most sustainable long-term direction is pure PQC certificates. Hybrid and composite approaches may provide short-term value, but they're not the destination.

2. Hardware and Firmware Limitations

- **The challenge:** Many systems rely on hardware security modules (HSMs), smart cards, or embedded firmware. These may not yet support PQC key sizes or algorithms.
- **Why it matters:** HSMs secure key storage for critical applications like payments and identity. If hardware lags, migration stalls.
- Approaches:
  - Engage vendors early with the vendor checklist (see Section 5).
  - Ask for firmware upgrade timelines and PQC support roadmaps.
  - Build interim plans for software deployments until full hardware support is available.

3. Application and Protocol Dependencies

- **The challenge:** Cryptography underpins countless security protocols and is embedded deep in libraries (OpenSSL, BouncyCastle, custom code).
- **Why it matters:** A single unsupported dependency can halt migration for an entire business process.
- Approaches:
  - Identify cryptographic dependencies as part of your CBOM.
  - Test PKI interoperability using DigiCert PQC Labs or similar environments.
  - Monitor standards groups (IETF, CAB Forum) to track evolving protocol updates.

PQC Standards Insight – The External Mu Question

- Debate in ML-DSA standards:
- Should signatures apply directly to messages?
- Or to their hashed values?
  - Current NIST design allows both creates API complexity.
  - **Risk:** Cross-protocol security issues if implementations diverge.
  - **Status:** Being resolved at IETF. Enterprises should test carefully.

4. Application and Protocol Dependencies

- **The challenge:** Even if your organization is ready, you depend on vendors and partners. If they lag, your migration will stall.
- **Why it matters:** AEcosystem readiness is as important as internal readiness. Supply chains can amplify or delay success.
- Approaches:
  - Conduct structured vendor briefings using the checklist provided in Section 5.
  - Push for written commitments on PQC support timelines.
  - Incorporate vendor dependencies into your migration plan

5. Performance and Scale

- **The challenge:** PQC algorithms often require larger keys and signatures, which can affect handshake times, storage, and bandwidth.
- **Why it matters:** At enterprise scale, small overheads become noticeable—especially in latency-sensitive applications.
- Approaches:
  - Run performance pilots (see Section 5 worksheets).
  - Document where PQC overheads matter most (IoT, mobile, edge).
  - Explore algorithm options—ML-KEM vs. Falcon vs. SLH-DSA—based on use case needs.

6. Organizational Change Management

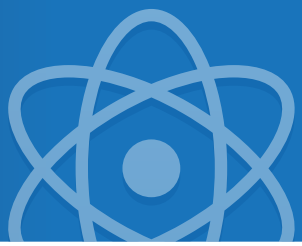
- **The challenge:** Cryptography touches multiple teams—IT, security, compliance, procurement, engineering. Without alignment, migration stalls in silos.
- **Why it matters:** Migration isn't just technical—it's cultural and organizational.
- Approaches:
  - Use governance frameworks (see Section 5 RACI chart).
  - Create a central PQC steering committee.
  - Incorporate training programs so staff understand both the "what" and the "why."

Turning Obstacles into Planning Inputs

Obstacles aren't reasons to delay—they're inputs to your planning. The key is to anticipate them, document where they're likely to appear, and incorporate mitigation strategies into your playbook. Organizations that treat these challenges as part of the journey will cross the quantum divide more smoothly and with fewer costly surprises.

PQC Standards Insight – Revocation in a PQC World

- PQC makes CRLs significantly larger.
- **Proposed solution:** Sharded CRLs split into smaller pieces.
- **Challenge:** Limited software support for sharding today.
- **Opportunity:** DigiCert is actively engaged with industry groups and customers to explore practical approaches to modernizing revocation models.



7. Stress-Testing the Bridge: PQC Labs & Workshops

Bridges aren't built and then trusted on faith. They're stress-tested before people and vehicles begin to cross. The same principle applies to post-quantum cryptography. Once you have a playbook in place, the next step is to test it in controlled environments and through simulated exercises that reveal gaps before they become risks.

Testing in Controlled Environment

Why it matters: Real-world systems are complex, and even small cryptographic changes can ripple across applications and networks. Controlled test environments let you explore PQC integration without endangering production systems.

How organizations can do this:

- Experiment with different certificate formats in lab environments to see how browsers, servers, and devices respond.
- Test hybrid and PQC-only certificates to assess compatibility and handshake performance.
- Evaluate protocol support with PQC libraries such as Open Quantum Safe.
- Use pilot worksheets (from Section 5) to structure tests and capture lessons learned.

What to measure:

- Latency and throughput changes.
- Compatibility with legacy systems.
- Operational impacts on automation workflows.
- Interoperability across vendors.

Scenario-Based Workshops

Why it matters: PQC migration isn't just technical—it involves decisions from CISOs, compliance officers, procurement, and developers. Tabletop exercises expose gaps in governance, decision-making, and cross-team communication.

How organizations can do this:

- Create a scenario: "*What if regulators required you to migrate in six months?*"
- Assign roles (CISO, developer, vendor, regulator) to participants.
- Work through the migration steps under time pressure, making decisions on priorities, exceptions, and resources.
- Debrief: What worked, what broke down, what needs to be codified into your playbook?

Benefits:

- Builds cross-team awareness and alignment.
- Surfaces hidden dependencies (vendor reliance, budget constraints, compliance requirements).
- Produces tangible outputs (draft policies, updated timelines, clarified roles).

Iterating and Improving

Stress-testing isn't a one-time activity. As algorithms mature, standards evolve, and vendors update their roadmaps, organizations should:

- Re-run pilots with updated libraries and protocols.
- Hold periodic workshops to refresh governance and test new scenarios.
- Incorporate lessons into the CBOM and migration plan.

From Planning to Confidence

Testing and workshops transform PQC readiness from theory into practice. By stress-testing your bridge before you need to cross it, you reduce uncertainty, build institutional confidence, and ensure that when the time comes, your organization is ready to move with purpose instead of scrambling under pressure.

DigiCert Perspective – What We're Seeing in PQC Readiness

As DigiCert works closely with standards bodies, vendors, and enterprises, three themes stand out in today's PQC migration landscape:

- **PKILINT Support-** DigiCert's PKILINT tool already validates PQC certificates using NIST algorithms, and can extend to private key checks. This helps enterprises begin conformance testing now, not later.
- **HSM Certification Timelines-** PQC support in hardware security modules is emerging, but validated implementations of ML-DSA and ML-KEM will take time. Early certifications are underway, with wider availability expected in 2025–2026. Hybrid deployments will remain common until then.
- **Industry Working Group Dynamics-** CAB Forum ballots, IETF drafts, and European regulators such as BSI and ANSSI are shaping PQC standards differently across regions. DigiCert's participation helps ensure customers are prepared, wherever they operate.

8. The DigiCert Bridge: How We Help You Cross

Every organization must chart its own path across the quantum divide. But no one needs to build the bridge alone. DigiCert has spent decades helping enterprises, governments, and manufacturers navigate cryptographic transitions—from algorithm changes to certificate migrations to the scaling of PKI into cloud and IoT environments.

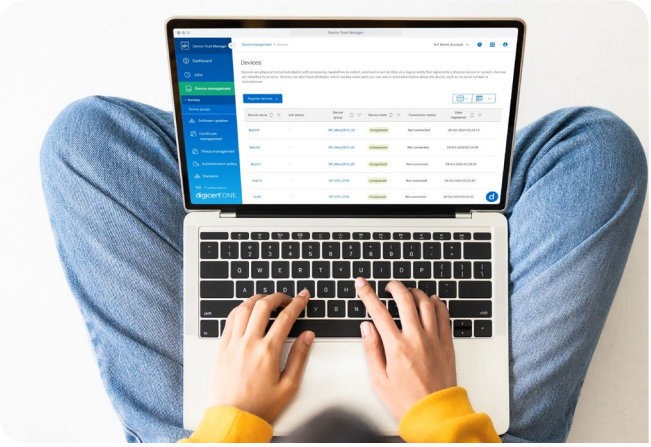
Our role is to provide the platforms, tools, and expertise that make your migration more predictable, automated, and sustainable. Here' is how DigiCert can support each step of your journey.

DigiCert Trust Lifecycle Manager

- What it does: Provides complete visibility into your certificate-based cryptographic assets—the majority of what organizations rely on today—while automating discovery and managing certificate replacement at scale.
- How it helps with PQC:
  - Lets you build and maintain a complete inventory of certificates—a critical foundation for your broader Cryptographic Bill of Materials (CBOM).
  - Automates certificate replacement as you update underlying systems to support PQC.
  - Reduces reliance on manual processes that increase risk during transition.

DigiCert Device Trust Manager

- **What it does:** Manages identity and lifecycle security for IoT and connected devices.
- **How it helps with PQC:**
  - Secures device provisioning and updates as new PQC standards are adopted.
  - Ensures IoT ecosystems remain trusted throughout multi-decade device lifespans.
  - Maintains compliance with emerging PQC requirements across regulated industries.

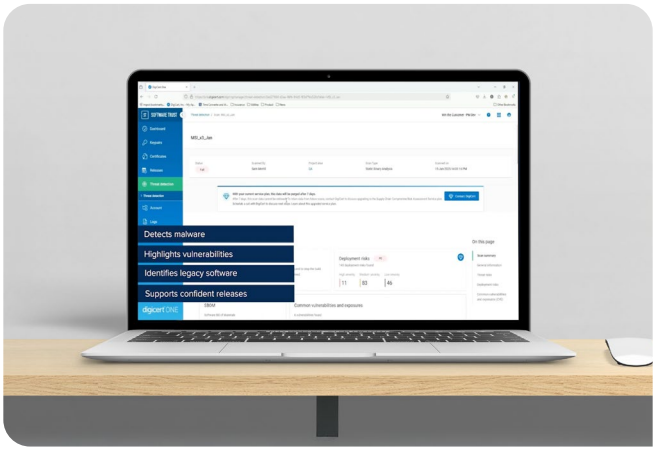


DigiCert TrustCore SDK

- **What it does:** Provides a comprehensive cryptographic library for developers.
- **How it helps with PQC:**
  - Embeds PQC algorithms directly into applications and devices.
  - Allows you to test hybrid and composite certificate support in real-world scenarios.
  - Future-proofs new products with quantum-safe capabilities from day one.

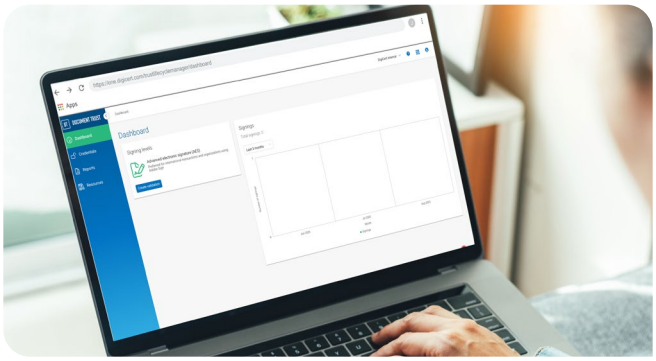
DigiCert Software Trust Manager

- **What it does:** Centralizes management and policy enforcement for code signing keys.
- **How it helps with PQC:**
  - Ensures software signatures remain secure and trusted for long lifespans.
  - Governs the adoption of PQC algorithms for code signing.
  - Supports hybrid signing strategies to maintain compatibility.



DigiCert Document Trust Manager

- **What it does:** Secures digital signatures and documents that must remain verifiable for decades.
- **How it helps with PQC:**
  - Lets you apply PQC-ready signatures to legal, healthcare, and government records.
  - Ensures long-term validity against both classical and quantum threats.



Beyond Technology: Expertise and Community

- DigiCert Labs offers free PQC-enabled certificates for testing.
- DigiCert's Tabletop-in-a-Box simulation exercise helps teams stress-test their PQC readiness by developing a draft playbook, walking through realistic migration scenarios, and then reviewing it with DigiCert experts for recommendations.
- We actively participate in standards bodies (NIST, CA/B Forum, IETF), giving our customers early insight into evolving requirements and ensuring DigiCert products are ready from day one.

A Bridge Built for the Long Haul

Technology alone is not enough. PQC migration requires visibility, governance, and coordination across your enterprise. DigiCert's platform and expertise are designed to help you move methodically and confidently across the quantum divide—and to stay secure once you reach the other side.

9. Resources for the Journey

Crossing the quantum divide isn't a single project—it's a journey that will unfold over years as standards mature, vendors update, and organizations adapt. The most successful migrations will be driven by teams who stay informed, connected, and equipped with the right resources.

Below is a curated set of tools, publications, and programs to help you continue building your post-quantum strategy.

Standards and Government Guidance

- **NIST PQC Project:** The official U.S. effort defining post-quantum cryptographic standards, including algorithm specifications, implementation guidance, and migration resources.
- **CNSA 2.0 (Commercial National Security Algorithm Suite):** NSA guidance on adopting PQC algorithms in U.S. national security systems, with timelines extending to 2030.
- **European Union Cyber Resilience Act (CRA):** Regulation mandating stronger resilience across digital products, aligned with PQC readiness.
- **HIPAA Security Rule (Proposed Update):** HHS has proposed strengthening requirements for encryption (in transit and at rest) and mandating technology asset inventories and network maps. If finalized, these changes would bring HIPAA compliance more in line with PQC readiness expectations.
- **Digital Operational Resilience Act (DORA):** EU regulation that places cryptography readiness in scope for financial services.

Industry and Research Organizations

- **ENISA (European Union Agency for Cybersecurity):** Guidance on quantum-safe migration strategies and best practices for enterprises.
- **Open Quantum Safe Project:** Open-source implementations of PQC algorithms for testing and research.
- **Quantum Computing Reports:** Industry analyses on CRQC progress and expected impact timelines.

DigiCert Resources

- PQC Hub: DigiCert's central resource for post-quantum education, blogs, and tools.
- World Quantum Readiness Day (WQRD): Annual event highlighting milestones, case studies, and readiness frameworks.
- DigiCert Labs PQC Playground: Free PQC-enabled certificates and test environments to evaluate algorithm integration.
- PQC Advisor Program: Strategic consultation for enterprises beginning their PQC migration planning.
- **Webinars and Whitepapers:** Educational sessions and in-depth guides on migration strategies, timelines, and case studies.

Tools and Templates

- **Cryptographic Bill of Materials (CBOM) Template:** Use to build a living inventory of algorithms, keys, and certificates in your environment.
- **Pilot Project Worksheet:** A structured guide to running controlled PQC pilots.
- **Vendor Briefing Checklist:** Key questions to ensure suppliers are aligned with your roadmap.
- **Governance RACI Chart:** A model for clarifying decision-making and accountability.

Next Steps

Resources are only valuable if they're acted upon. As you plan your journey:

1. Stay connected to evolving standards and regulatory updates.
2. Use available tools and templates to begin building your internal playbook.
3. Leverage pilots and labs to gain practical experience.
4. Engage your vendors and partners early, ensuring ecosystem alignment.

Crossing the quantum divide is a shared effort across industry, government, and technology providers. By combining external knowledge, internal planning, and hands-on testing, your organization can move deliberately—and confidently—toward a secure quantum future.

10. Final Call: Start Crossing the Quantum Divide Today

The post-quantum era is no longer a distant horizon. Standards have been set, governments are issuing guidance, and enterprises are already running pilots. The bridge is under construction—now is the time to take your first step.

Throughout this guide, we've explored:

- **Why the quantum divide exists** and how quantum computing will disrupt today's cryptography.
- **How long the bridge is**, with milestones from NIST, CNSA 2.0, and global regulators.
- **Why standing still is costly** in compliance, operations, and competitiveness.
- **How to build your own playbook**, with steps, templates, and governance structures you can use immediately.
- **What challenges to expect** and strategies to overcome them.
- **How to stress-test your readiness** through pilots, labs, and workshops.
- **Where DigiCert can help** with tools, expertise, and community to guide your journey.
- **Which resources are available now** to continue learning and planning.

The message is clear: Crossing the quantum divide is not optional, but it is achievable. Organizations that start today will reduce costs, avoid disruption, and build a foundation of trust that endures well into the quantum era.

Take Your First Step

Every journey begins with a single action. For your organization, that may mean:

- Initiating a cryptographic inventory with the CBOM template.
- Running your first PQC pilot in a lab environment.
- Scheduling a vendor briefing to align your ecosystem.
- Convening a steering committee to define governance and strategy.

Whether you start small or aim big, starting is what matters most.

Moving Forward with Confidence

Crossing the quantum divide will be one of the most significant security transitions of our time. But it doesn't need to be daunting. With preparation, collaboration, and the right guidance, you can build a bridge strong enough to carry your organization into the future of digital trust.

The divide is real, but so is the path forward. Now is the time to take your first step.

About DigiCert

DigiCert is the world's leading provider of digital trust, enabling individuals and businesses to engage online with the confidence that their footprint in the digital world is secure. DigiCert® ONE, the platform for digital trust, provides organizations with centralized visibility and control over a broad range of public and private trust needs, securing websites, enterprise access and communication, software, identity, content and devices. DigiCert pairs its award winning software with its industry leadership in standards, support and operations, and is the digital trust provider of choice for leading companies around the world. For more information, visit digicert.com or follow @digicert.

Want to learn more about Post Quantum Readiness?

Contact sales at 1.855.800.3444 or email sales@digicert.com.