Amberteq | QUANTUM READINESS

WHITE PAPER · 2026

Quantum Readiness: A Governance and Resilience Framework for Regulated Enterprises

How security, risk, and technology leaders can assess cryptographic exposure, prioritize post-quantum transition risks, and build a phased roadmap before committing to specific technologies or vendors.

POST-QUANTUM CRYPTOGRAPHY | CRYPTOGRAPHIC RISK ASSESSMENT | NIST PQC STANDARDS | DORA · NIS2 | VENDOR-NEUTRAL ADVISORY | PHASED TRANSITION PLANNING

© 2026 Amberteq Inc. · amberteq.com/quantum-ready-advisory

Confidential · For authorized recipients only

CONTENTS

Table of Contents

EXECUTIVE SUMMARY

Start with visibility, not replacement

Post-quantum transition is not a cryptographic upgrade. For regulated enterprises and data-sensitive organizations, it is a multi-year governance, resilience, and risk management program. The organizations that will navigate it most effectively are those that begin with structured assessment — not those that rush into premature technology replacement.

> "*Quantum readiness is a cyber resilience and governance issue, not only a cryptography topic. The first step is understanding which data, systems, vendors, certificates, protocols, and trust relationships create long-term exposure.*"

This white paper describes the business case for quantum readiness assessment, who should act and when, what an effective assessment covers, and how Amberteq's phased advisory approach helps organizations prepare without unnecessary disruption or vendor lock-in.

The core problem: Organizations cannot plan a post-quantum transition until they know where cryptographic risk sits, which data has a long confidentiality horizon, and which dependencies will slow down change.

The practical urgency: The urgency is not immediate cryptographic failure. It is that visibility, governance, vendor alignment, and transition planning take years to build — and that window is narrowing.

Key takeaways

Assessment before migration. Large-scale cryptographic replacement without prior assessment leads to inefficient spend, vendor lock-in, and disruption to critical services. Discovery and sequencing must come first.

Governance is the foundation. Ownership, procurement criteria, crypto agility principles, and cross-function alignment are prerequisites for successful transition — not afterthoughts.

Vendor-neutral advisory reduces risk. The post-quantum market is still maturing. Advisory that is independent of specific product vendors protects organizations from premature commitment.

Regulatory preparedness is already expected. NIST has finalized initial standards. The EU has issued a coordinated transition roadmap. DORA and NIS2 reinforce digital resilience expectations across regulated sectors.

SECTION 1

Why Quantum Readiness Matters Now

1.1 The harvest-now, decrypt-later threat

The most immediate and concrete quantum-related risk does not require fully capable quantum computers to exist today. It requires only that adversaries can capture and store encrypted communications, records, and data flows now — and decrypt them later, once quantum computing capability becomes sufficient.

This approach, known as "harvest now, decrypt later," has practical implications for any organization that:

· Transmits sensitive data over VPNs, TLS connections, or secure file transfer channels
· Maintains long-retention archives of regulated records, clinical data, legal documents, or financial transactions
· Relies on digital signatures for contracts, workflows, regulatory filings, or software integrity
· Operates trusted machine-to-machine relationships protected by asymmetric cryptography
· Holds data that must remain confidential for 10, 20, or 30+ years beyond today

For these organizations, the relevant question is not "will quantum computers break everything tomorrow?" It is: "how long must our sensitive data remain confidential, and does our current cryptographic protection cover that horizon?"

1.2 Transition timelines are longer than expected

Post-quantum migration is not a software update. It is a multi-year modernization and governance effort that involves cryptographic discovery across complex estates, vendor and third-party alignment, architecture decisions, certificate and PKI lifecycle management, and gradual replacement of embedded and legacy systems.

Organizations that start assessment early gain a significant advantage: they can sequence changes deliberately, avoid emergency decisions, maintain vendor negotiating leverage, and build governance structures before regulators require them.

Governance programs of this complexity typically take years to build. Organizations that wait for external pressure to create urgency will have significantly less control over timing, scope, cost, and vendor decisions.

1.3 Regulatory and standards context

The external environment is providing increasing direction — without yet mandating universal, immediate migration.

NIST Post-Quantum Cryptography Standards (August 2024)

NIST finalized the first three post-quantum cryptography standards: ML-KEM (formerly CRYSTALS-Kyber), ML-DSA (formerly CRYSTALS-Dilithium), and SLH-DSA (formerly SPHINCS+). These provide the technical baseline for transition planning and procurement requirements.

EU Post-Quantum Transition Roadmap (2024–2025)

The European Commission has recommended a coordinated approach to post-quantum transition planning. A high-level roadmap for EU member states was published in 2025, setting expectations for structured preparedness across critical sectors.

DORA — Digital Operational Resilience Act (applicable January 2025)

DORA strengthens digital operational resilience requirements for EU financial entities. It reinforces expectations for ICT risk management, third-party oversight, and the management of vulnerabilities — including cryptographic dependencies — as part of a broader operational resilience framework.

NIS2 Directive

NIS2 establishes a unified cybersecurity governance framework for 18 critical sectors across the EU. It broadens the scope of entities subject to requirements and strengthens obligations for security governance, incident reporting, and supply chain risk management.

Note: This section reflects publicly available information about standards and regulatory frameworks as of 2026. Organizations should verify specific compliance obligations applicable to their jurisdiction and sector with their legal and compliance teams. Amberteq does not guarantee specific regulatory compliance outcomes.

SECTION 2

Who Should Act

2.1 Primary: regulated enterprises

Quantum readiness assessment is most directly relevant for enterprises operating in regulated sectors where long-term confidentiality, digital trust, and operational resilience are strategic obligations — not optional considerations.

- **Finance and Banking**

  Transaction systems, customer data, long-term financial records, interbank trust chains, DORA operational resilience requirements, and extensive third-party ICT dependency. The combination of long data retention requirements, complex vendor ecosystems, and DORA obligations makes this sector among the most immediately relevant.

- **Healthcare and Life Sciences**

  Clinical records with decades-long retention requirements, privacy regulations, medical device communications, laboratory system integrations, and identity and signing workflows. Patient data captured today may require confidentiality protection well beyond current infrastructure lifecycles.

- **Government and Public Sector**

  Citizen records, critical government services, national security-adjacent data, inter-agency trust chains, long-term archive requirements, and legacy modernization programs. Data classification requirements may extend confidentiality obligations across decades.

- **Critical Infrastructure**

  Operational technology, SCADA and ICS systems, long-life hardware, embedded cryptographic libraries, safety-critical communications, and infrastructure that cannot be easily taken offline for updates. Legacy constraints make early planning especially important.

- **Telecommunications**

  Secure communications infrastructure, roaming trust chains, certificate dependencies, network key management, and the cryptographic fabric underpinning connected service delivery for millions of users and devices.

2.2 Secondary: data-sensitive SMBs

Quantum readiness is not limited to large regulated enterprises. Smaller organizations may have significant exposure if they:

Hold long-life sensitive data | Operate in trusted supply chains | Support regulated clients | Manage clinical / legal / financial records | Depend on PKI or digital signatures | Process citizen or strategic data

For SMBs, the assessment scope is typically narrower than for large enterprises, but the fundamental questions — what data requires long-term protection, what cryptographic dependencies exist, and what third-party constraints apply — remain equally important.

SECTION 3

What a Readiness Assessment Covers

An effective quantum readiness assessment connects business exposure, technical discovery, governance analysis, third-party dependency mapping, and transition planning. The goal is a decision-ready view of where action should begin — not a description of cryptographic theory.

3.1 Six assessment areas

Assessment area	What we examine	Output
Business criticality	Critical services, regulated obligations, data classes by confidentiality horizon, business processes dependent on cryptographic controls	Business exposure view, service priority list
Cryptographic discovery	Certificates, protocols, PKI infrastructure, cryptographic libraries, secure channels, TLS configurations, identity systems, signing workflows	Cryptographic dependency map, exposure inventory
Data confidentiality horizon	How long sensitive data must remain protected, retention requirements, archive classifications, regulatory obligations by data type	Priority data classes, harvest-now-decrypt-later exposure view
Third-party exposure	Vendor and managed service cryptographic readiness, platform constraints, supply chain dependencies, legacy system integration points	Vendor readiness assessment, third-party constraint map
Governance and crypto agility	Ownership and accountability structures, procurement criteria, security policies, architecture principles, cross-function alignment	Governance gap analysis, crypto agility framework
Risk prioritization	Business impact by domain, exposure severity by system and data class, transition difficulty, dependency concentration	Priority risk list, sequenced action plan

3.2 Key risks the assessment addresses

- **Unknown cryptographic exposure**
  Certificates, embedded libraries, and cryptographic protocols distributed across the estate without consolidated visibility or ownership.
- **Long-life data without protection horizon planning**
  Data with multi-decade confidentiality requirements protected only by cryptography that may not outlast its sensitivity window.
- **Third-party and vendor lock-in risk**
  Platforms, managed services, and legacy systems whose transition readiness will determine the organization's migration timeline.
- **Board and regulator exposure**
  Inability to provide a defensible answer to leadership, audit committees, or regulators about quantum-related risk and preparedness.
- **Premature technology commitment**
  Early product selection before standards fully stabilize and before organizational exposure is understood — creating costly constraints.
- **Governance and ownership gaps**
  No designated owner, no procurement criteria, no cross-function alignment — leaving the organization unable to execute transition when needed.

SECTION 4

The Phased Advisory Approach

Post-quantum readiness should be sequenced deliberately. The objective is not immediate large-scale replacement. It is to reduce uncertainty, establish ownership, identify high-priority exposure, and prepare a transition path that can be explained to leadership, auditors, vendors, and regulators.

1

Align — Frame the risk, define ownership

Establish executive sponsorship. Define scope in terms of business context, not cryptographic theory. Identify stakeholder responsibilities across security, risk, architecture, compliance, legal, privacy, and procurement. Set decision criteria for prioritization.

`Stakeholder map` `Scope definition` `Decision criteria`

2

Discover — Map the cryptographic estate

Identify cryptographic dependencies across business-critical services, data classes, secure channels, certificate and PKI infrastructure, signing workflows, identity systems, and third-party platforms. Establish a baseline inventory of exposure and gap areas.

`Exposure map` `Dependency inventory` `Initial gap list`

3

Prioritize — Focus on what matters most

Evaluate exposure against business impact, data confidentiality horizons, transition difficulty, and third-party constraints. Identify where action should begin, where quick wins exist, and what can be responsibly deferred.

`Priority risk list` `Quick wins` `Vendor constraint view`

4

Plan — Design the transition roadmap

Develop a phased transition roadmap with governance principles, crypto agility criteria, architecture decisions, and executive-ready framing. Prepare the documentation needed for board briefings, audit responses, and regulatory inquiry.

`Phased roadmap` `Governance plan` `Executive briefing`

5

Execute and Oversee — Support implementation

Provide advisory and implementation support for priority actions. Assist with vendor and platform alignment, architecture decisions, and deployment of initial changes. Offer managed oversight options including periodic reassessment and readiness scoring updates.

`Implementation support` `Managed oversight` `Readiness metrics`

SECTION 5

Optional Software-Enabled Layer

For organizations that need a reusable, updatable view of their cryptographic estate, the advisory process can be supported by a software-enabled layer. This is not a replacement for advisory judgment — it is a tool that consolidates relevant systems, dependencies, service interactions, and readiness indicators into a structured view for executive reporting and ongoing reassessment.

Unified system inventory

A single consolidated view of systems, services, assets, and dependencies relevant to cryptographic exposure — across the organization and its operational domains. Designed to serve as the foundation for assessment and ongoing monitoring.

Readiness scoring

Organization-level and domain-level readiness scores for prioritization and executive reporting. Scoring is designed to highlight where readiness is weakest, support decision-making, and enable periodic reassessment as the environment evolves.

Interaction analysis

Visibility into how applications, communication channels, identities, and data flows connect across the estate — surfacing cryptographic dependencies that span organizational units, vendors, and legacy systems.

Actionable reporting

Support for executive reporting, board briefings, architecture review, and phased transition planning — with structured evidence that can be shared with leadership, auditors, and regulators.

> The software layer is an optional component. Many organizations benefit significantly from advisory-led assessment and roadmap development without requiring a software platform. Relevance depends on organizational complexity, the size of the cryptographic estate, and the need for ongoing monitoring versus a point-in-time assessment.

SECTION 6

Deliverables

The engagement is structured around decision-ready outputs that help organizations move from uncertainty to prioritized action. Each deliverable is designed to serve a specific stakeholder need and to remain useful as the transition program evolves.

EXECUTIVE

Executive Briefing

Board-ready summary of quantum-related exposure, ownership, key priorities, and recommended next steps. Non-technical framing for leadership, audit committees, and regulators.

DISCOVERY

Exposure Summary

Consolidated view of where cryptographic risk sits — organized by service, data class, and organizational domain. Identifies known gaps and highest-priority areas for action.

TECHNICAL

Dependency Map

Structured view of cryptographic dependencies across certificates, PKI, protocols, cryptographic libraries, secure channels, signing workflows, and machine-to-machine trust.

PLANNING

Phased Transition Roadmap

Prioritized, sequenced roadmap showing what to address first, where quick wins exist, where vendor alignment is needed, and what can be responsibly deferred.

GOVERNANCE

Governance Recommendations

Ownership model, crypto agility principles, procurement criteria updates, and cross-function alignment guidance for the transition program.

SCORING

Readiness Scoring Model

Domain-level and organization-level readiness scores for prioritization and executive reporting. Available as part of the optional software-enabled layer. Designed to support periodic reassessment.

SECTION 7

Why Vendor-Neutral Advisory Matters

The post-quantum cryptography market is still maturing. Standards have been finalized, but product implementations are at varying stages of maturity, interoperability testing is ongoing, and the full landscape of enterprise PQC tooling continues to evolve.

In this environment, organizations that make early, narrow product commitments risk constraining their options before they understand their own exposure — and before the market has settled enough to make durable choices.

> "*Vendor-neutral advisory helps organizations understand exposure and make sequenced decisions before committing to specific products or platforms. Early commitment — before standards stabilize and products are tested in production — can create constraints that are difficult and costly to reverse.*"

Comparison: advisory-led vs. generic IT delivery

Dimension	Generic IT vendor	Amberteq Quantum Readiness
Starting point	Starts with implementation scope and delivery capacity	Starts with assessment, exposure mapping, and prioritization
Vendor position	May recommend specific products early in the process	Vendor-neutral throughout; avoids premature lock-in
Security framing	Treats quantum readiness as a technical delivery task	Connects security, risk, architecture, compliance, and procurement
Planning output	Generic modernization or migration plan	Phased quantum readiness roadmap with governance model
Board readiness	Technical report for security team	Executive briefing and board-ready risk framing
Long-term alignment	Focus on project completion	Ongoing oversight, reassessment, and managed options

SECTION 8

Engagement Models

Amberteq Quantum Readiness offers structured engagement options designed to match organizational scale, complexity, and readiness maturity. Engagements can begin at any point and expand as priorities become clearer.

Engagement type	Scope and output	Best suited for
Readiness Workshop	Executive and technical alignment session. Covers: what to protect, where risks sit, what questions board and regulators will ask, and what the practical first steps are.	Organizations at the earliest stage of awareness — building internal understanding and executive alignment before committing to a full assessment.
Focused Assessment	Structured review of business-critical services, data classes, cryptographic dependencies, third-party exposure, governance, and crypto agility. Full deliverable set including exposure summary and dependency map.	Organizations ready to move from awareness to evidence — needing a structured view of where exposure sits and what to prioritize.
Roadmap Design	Based on assessment findings: phased transition roadmap, governance recommendations, executive briefing materials, vendor neutrality principles, and prioritized action list.	Organizations that have completed an initial assessment and need a defensible, board-ready transition plan.
Implementation Support	Advisory support during execution of priority actions. Includes vendor alignment assistance, architecture guidance, and support for organizational change management around transition.	Organizations that have a roadmap and need expert support through early execution phases, particularly where vendor negotiations or architectural decisions are involved.
Managed Oversight	Periodic reassessment, readiness scoring updates, regulatory preparedness review, and ongoing advisory as the environment and standards evolve.	Organizations that need continuous governance of quantum readiness as a program rather than a one-time project.

All engagements are scoped to organizational context. The right starting point depends on current readiness maturity, internal capacity, sector-specific obligations, and the complexity of the cryptographic estate. A readiness discussion is the best first step for determining which engagement model is most appropriate.

ABOUT

About Amberteq

Amberteq is a technology advisory and delivery company working with regulated enterprises and data-sensitive organizations to address complex system modernization, resilience, and risk challenges.

Amberteq Quantum Readiness is a vendor-neutral advisory and assessment service designed for organizations in finance, healthcare, public sector, critical infrastructure, telecom, and data-sensitive SMBs that need to prepare for post-quantum cryptographic transition responsibly — without unnecessary disruption or premature vendor lock-in.

Markets served:
European Union · United Kingdom · United States

Contact:
quantum@amberteq.com
amberteq.com/quantum-ready-advisory

Disclaimer: This white paper is intended for informational purposes. The content reflects publicly available information about post-quantum cryptography standards, regulatory frameworks, and industry practices as of 2026. It does not constitute legal, compliance, or technical advice. Organizations should assess their specific obligations and circumstances with qualified legal, compliance, and technical advisors. Amberteq does not guarantee specific outcomes, regulatory compliance, or the elimination of cryptographic risk through engagement with its services. The assessment models and deliverables described represent typical scope and may vary based on organizational context, engagement type, and agreed scope.

© 2026 Amberteq Inc. All rights reserved. · amberteq.com