ProteQC® Introduces the ProteQC PQC Lifecycle Framework™, Establishing a Governance-First Approach to Quantum Readiness

Launched on World Quantum Day, the approach addresses the most common PQC migration failure mode: discovery without action

LONDON, UNITED KINGDOM, April 14, 2026 /EINPresswire.com/ -- ProteQC, a cryptographic resilience advisory firm, today introduced the ProteQC PQC Lifecycle Framework™, a governance-first approach to managing an organization's transition to post-quantum cryptography (PQC). The announcement coincides with World Quantum Day, a global recognition of both the promise of quantum computing and the urgency of preparing for its impact on today's cryptographic systems.

With quantum capability advances, organizations face a growing disconnect between awareness and action. While executives increasingly recognize quantum risk as critical, most remain unprepared to operationalize a response. ProteQC's PQC Lifecycle Framework™ addresses this gap by establishing a structured, governance-first model that helps organizations move beyond the Frozen Findings Problem (technically accurate reports that organizations cannot act on) and build an enduring capability for managing quantum risk.

"Organizations are deploying discovery tools before establishing ownership or business context, resulting in what we call the Frozen Findings Problem," said BJ Miller, CEO of ProteQC. "We reframe PQC resilience through a five-stage blueprint — the ProteQC PQC Lifecycle Framework™ — to guide organizations from governance to sustained quantum-safe operations, with business strategy driving execution."

Unlike other frameworks in the PQC Lifecycle Management space, the ProteQC PQC Lifecycle Framework™ begins with two governance and organizational alignment stages before any tools are deployed. It extends through discovery, financial and operational planning, and sustained crypto-agility, with business strategy driving technical execution at every stage. By treating quantum readiness as a lifecycle capability, organizations can move beyond fragmented technical efforts toward a structured, defensible, and repeatable approach to cryptographic change.

“Tool vendors start with discovery. We start with your business,” said Tim D Williams, CTO of ProteQC.

A Five-Stage Blueprint for Quantum Readiness
Developed by ProteQC's founding team based on lessons learned from PQC engagements over the four years preceding ProteQC’s formation, the ProteQC PQC Lifecycle Framework™ defines a five-stage best practice model that enables organizations to build a lasting capability for managing quantum risk:

 Stage 1: Pre-Discovery™ — Establish governance, ownership, risk taxonomy mapping, training and regulatory alignment before any tools are deployed.
 Stage 2: Business Context — Map critical services to cryptographic dependencies and prioritize risks such as long-lived data exposure and Store Now, Decrypt Later.
 Stage 3: Targeted Discovery — Conduct focused scanning to produce a Cryptographic Asset Register aligned to business priorities.
 Stage 4: Migration Planning — Translate findings into a funded, board-level roadmap tied to financial, regulatory, and legal considerations.
 Stage 5: Ongoing Agility — Build crypto-agility as an operational capability, enabling continuous adaptation to future cryptographic change without disruption.

From Awareness to Defensibility
The framework also reflects a broader shift in how quantum risk is being evaluated. Regulatory bodies, financial supervisors, and legal scholars are increasingly treating cryptographic vulnerability as a present-day governance issue, not a future technical concern.

Organizations that adopt a lifecycle approach position themselves to be:

 Audit-ready, with governance established before discovery
 Defensible, with documented, proportionate responses to emerging risk
 Crypto-agile, with systems and processes designed to evolve

In the EU, DORA already requires regulated financial entities to maintain cryptographic management policies as part of their ICT security frameworks — not in 2030, but as of January 2025.

“World Quantum Day is a reminder that this transition isn’t theoretical,” added Miller. “Adversaries are already collecting encrypted data today with the expectation they can decrypt it tomorrow. The question for organizations is no longer if they act, but whether they act in a way that stands up to regulators, auditors, and boards.”

ProteQC was founded to help regulated organizations — financial institutions, healthcare providers, critical infrastructure operators and their extended supply chains — prepare for the transition to post-quantum cryptography while addressing the governance and legal risks

emerging alongside quantum computing. To learn more about the ProteQC PQC Lifecycle Framework™ and how organizations can adopt it, read our accompanying feature article or visit https://proteqc.com

About ProteQC
ProteQC is a vendor-independent cryptographic resilience advisory firm enabling organizations to achieve crypto-agility and mitigate quantum-era risk. The firm delivers training, assessments, strategy development, and ongoing advisory support to financial institutions, healthcare providers, critical infrastructure operators and their extended supply chains.

Ana Perez Quiles
ProteQC
+44 20 3835 5326
email us here
