Continuous Monitoring and Audit

By Tooba Qasim

Keeping Quantum-Safe Systems Secure Over Time

One of the most dangerous assumptions in cybersecurity is the idea that a successful deployment marks the end of the journey.

In reality, deployment is only a checkpoint. This is especially true for post-quantum cryptography. While reaching implementation is a major milestone, quantum-safe security is not something an organisation can "install and forget." It is a capability that must be monitored, reviewed and adjusted over time as standards evolve, vulnerabilities emerge and operational environments change.

The sustainability phase exists for one reason: **long-term resilience**.

Why Post-Quantum Security Is Not Static

Traditional cryptographic systems have benefited from decades of stability. Algorithms such as RSA and elliptic curve cryptography were deployed, optimised, hardened and audited over many years. Changes were infrequent and usually reactive.

Post-quantum cryptography enters a very different environment.

The algorithms are newer. Implementations are younger. Operational experience is still being accumulated. Standards bodies continue to refine guidance, and research continues to test assumptions. This means that even after a successful rollout, organisations must remain attentive.

Quantum-safe security is less like installing a firewall and more like maintaining a safety-critical system. The absence of visible problems today does not guarantee safety tomorrow.

Monitoring What Is Actually Running

One of the first sustainability challenges is visibility.

After deployment, organisations often assume that systems continue to run exactly as designed. In practice, configurations drift, patches introduce changes and fallback

mechanisms behave in unexpected ways. Over time, it becomes harder to answer simple but critical questions:

Are post-quantum algorithms still enabled everywhere they should be?

Are hybrid configurations still functioning as intended?

Have any systems silently reverted to classical cryptography due to performance or compatibility issues?

Continuous monitoring helps answer these questions before they become incidents.

This includes monitoring cryptographic configurations in TLS connections, VPNs, identity systems, certificate chains and internal services. It also includes validating that cryptographic libraries, hardware security modules and firmware continue to support the intended algorithms and parameters.

In a quantum-safe context, **absence of alerts does not equal assurance**.

Auditing Beyond Compliance Checkboxes

Audit plays a different role in the sustainability phase.

Early audits often focus on readiness: whether inventories exist, plans are documented and migrations are underway. Post-deployment audits must instead focus on **assurance over time**.

This means reviewing not only whether post-quantum algorithms are present but whether they are being used correctly, consistently and safely. It also means revisiting design assumptions made during deployment and testing whether they still hold under real operational conditions.

For example, an audit may examine whether hybrid cryptographic approaches are still providing the intended protection, whether key sizes and parameters remain aligned with current guidance, or whether changes in system load have altered performance characteristics in ways that affect security.

Effective audits in this phase are iterative, not one-off.

Tracking Standards, Guidance and Vulnerabilities

Another reason continuous review matters is that the post-quantum landscape itself is still evolving.

Standards bodies continue to publish updates, clarifications and new recommendations. Additional algorithms may be standardised to improve diversity or address specific use cases. At the same time, researchers continue to analyse post-quantum schemes for weaknesses, implementation risks and side-channel exposure.

None of this implies that current standards are unsafe. It does mean that organisations must stay informed.

Sustainable quantum-safe programmes include mechanisms for tracking updates from standards organisations, national cyber authorities and the research community. This information must feed into risk assessments, architecture reviews, and change management processes in a structured way.

Without this feedback loop, organisations risk freezing their security posture at a moment in time that may no longer be optimal.

Operational Lessons Emerge After Go-Live

Some of the most important insights only appear after systems are live.

Performance issues, operational edge cases and integration challenges often surface under real workloads. In post-quantum deployments, this can include increased latency, higher memory usage, or unexpected interactions with legacy systems and security tooling.

Operational monitoring allows teams to detect these issues early and respond without compromising security. It also helps prevent the gradual erosion of quantum-safe protections through ad-hoc workarounds or undocumented configuration changes.

From a sustainability perspective, **operational reality must continuously inform governance decisions**.

Third-Party and Supply-Chain Assurance

Quantum-safe security does not exist in isolation.

Cloud providers, software vendors, identity platforms and managed service providers all form part of an organisation’s cryptographic environment. Even if internal systems are well maintained, external dependencies may change in ways that affect overall risk.

Continuous audit therefore extends beyond internal systems. It includes reviewing vendor updates, contract clauses, service-level agreements and cryptographic roadmaps. It also

involves validating that third-party changes do not undermine hybrid strategies or introduce unintended downgrade paths.

Sustainability depends as much on ecosystem awareness as it does on internal controls.

Embedding Review into Business Rhythm

The most resilient organisations do not treat post-quantum monitoring as a special project. They embed it into existing governance rhythms.

This might include regular reviews as part of enterprise risk management cycles, security architecture boards, internal audit schedules, or technology refresh programmes. Over time, post-quantum considerations become just another dimension of digital risk which important, but not disruptive.

This is the real goal of the sustainability phase: **normalisation**.

Quantum-safe security should eventually feel routine, not exceptional.

Why This Phase Makes the Difference

Many organisations will succeed in deploying post-quantum cryptography. Fewer will succeed in maintaining it effectively over time.

The difference lies in mindset.

Continuous monitoring and audit recognise that security is a moving target, especially in a domain shaped by active research and long-term technological change. By committing to ongoing review, organisations protect not only their systems but the investment they have already made in becoming quantum-safe.

In the end, sustainability is not about predicting the future perfectly. It is about building systems and governance that can adapt as the future unfolds.

That is what turns quantum-safe deployment into quantum-safe resilience.