Pilot Projects and Case Studies

By Tooba Qasim

Learning Before You Commit

By the time organisations reach the implementation phase of post-quantum cryptography, the conversation changes. The questions are no longer “Should we prepare?” or “Which algorithms are approved?” Instead, they become much more practical:

Where do we start without breaking anything?

How do we learn safely before making irreversible changes?

What does post-quantum cryptography actually look like in our environment?

This is where pilot projects become essential.

A pilot is not a half-finished deployment. It is a controlled learning exercise designed to surface real-world issues early when they are still manageable.

Why Pilots Matter More Than Whitepapers

Post-quantum cryptography looks straightforward on paper. Algorithms are standardised, libraries exist and protocols are being updated. But real systems are messy. They include legacy components, third-party dependencies, unexpected performance constraints and operational assumptions that were never documented.

Pilots allow organisations to test these realities in a safe environment.

They answer questions that planning alone cannot:

- How much additional latency does hybrid TLS introduce in our network?
- Which applications fail when certificate sizes increase?
- Which vendors are actually ready and which only say they are?

Research consistently shows that performance and interoperability issues often emerge only during hands-on testing. For example, multiple academic studies evaluating hybrid post-quantum TLS deployments found that handshake sizes and latency varied significantly depending on algorithm combinations and system configurations, effects that are difficult

to predict without empirical testing. This is exactly the kind of insight pilots are meant to uncover.

What a Good PQC Pilot Looks Like

Effective pilot projects are deliberately narrow.

Rather than attempting to "make everything quantum-safe," organisations typically select one or two representative use cases. Common starting points include internal TLS connections between services, non-customer-facing APIs, development or staging environments or isolated VPN tunnels.

The goal is not to demonstrate perfection. The goal is to learn.

A well-designed pilot focuses on:

- a limited scope that reflects real production conditions,
- hybrid cryptography rather than PQC-only configurations,
- clear success criteria that include performance, stability, and operational impact.

Many organisations also deliberately include at least one legacy component in the pilot, precisely because legacy friction is one of the hardest problems to solve later.

What Organisations Learn from Early Pilots

Across industries, pilot projects tend to surface similar lessons.

One common discovery is that cryptography is far more distributed than expected. Teams often find PQC-relevant cryptographic operations buried inside load balancers, identity brokers, embedded devices, or third-party libraries that were not visible during initial planning.

Another frequent insight is that performance impact is rarely uniform. Some systems show negligible overhead, while others experience noticeable increases in handshake time or memory usage. Research papers benchmarking NIST post-quantum finalists consistently show that algorithm choice, implementation quality and environment matter as much as the algorithm itself.

Pilots also reveal organisational issues. Teams discover gaps in logging, monitoring and incident response processes when new cryptographic behaviours appear. These are not cryptographic failures they are operational blind spots that pilots are meant to expose.

What Research Tells Us About Pilots

Academic and industry research reinforces the importance of pilots as a risk-reduction mechanism.

Studies analysing hybrid TLS deployments in realistic network environments have shown that some PQC algorithm combinations increase packet sizes enough to trigger fragmentation or compatibility issues in certain middleboxes. Other papers highlight how VPN and SSH implementations behave differently under post-quantum key exchange, even when based on the same algorithms.

This research does not argue against PQC. Instead, it supports a phased, test-driven approach.

The key message from the literature is consistent: **post-quantum cryptography is safe in theory but success in practice depends on careful integration, measurement and iteration**.

That is precisely what pilots enable.

Anonymised Examples from Early Adopters

While most organisations do not publicly disclose their PQC pilots, anonymised patterns are emerging.

In financial services, pilots often start with internal service-to-service communication, allowing teams to test hybrid TLS without customer impact. In cloud-native environments, teams frequently pilot PQC within Kubernetes ingress layers or API gateways, where cryptographic changes can be controlled centrally.

In industrial environments, pilots tend to focus on management networks rather than operational control paths, reflecting the higher risk tolerance required for production systems.

Across all sectors, the most successful pilots share one trait: they treat PQC as a system-level change, not a cryptographic experiment.

Pilots as Organisational Learning Tools

One of the most underappreciated benefits of pilot projects is cultural rather than technical.

Pilots create shared understanding across security teams, architects, developers, operations and procurement. They turn abstract requirements into concrete experience. Teams stop asking “What is PQC?” and start asking “How does this behave in our environment?”

This shift is critical. Organisations that skip pilots often find themselves forced into reactive deployments later under time pressure and regulatory scrutiny. Organisations that pilot early gain confidence, data, and internal alignment.

From Pilot to Scaled Deployment

A successful pilot does not end with a rollout decision. It ends with documentation.

The outputs of a pilot should include performance measurements, failure modes, vendor readiness assessments, operational impacts and clear recommendations for broader deployment. These outputs feed directly into deployment strategies and operational readiness planning.

In this sense, pilots are not optional experiments. They are **the bridge between preparation and production**.

Why This Stage Should Not Be Skipped

Post-quantum migration is not a single switch to flip. It is a journey that unfolds over years. Pilot projects are how organisations take the first real step carefully, deliberately and with evidence rather than assumptions.

Research, standards and guidance all point in the same direction: organisations that learn early will move faster and more safely later.

Pilots are where that learning begins.