LAMAH
INTELLIGENT SOLUTIONS

LAMAH BOARDROOM PAPERS
No. 1 · July 2026

Quantum Resilience

Why Boards Must Govern Time, Not Just Technology

Saleh Sailik
Managing Director, LAMAH Intelligent Solutions

LAMAH
INTELLIGENT SOLUTIONS

LAMAH Boardroom Papers

No. 1 · Quantum Resilience: Why Boards Must Govern Time, Not Just Technology

PUBLISHED July 2026, Doha, Qatar

AUTHOR Saleh Sailik, Managing Director, LAMAH Intelligent Solutions

SERIES The LAMAH Boardroom Papers present original perspectives on emerging governance and resilience challenges facing Boards and executive management in Qatar and the wider Gulf region.

SUGGESTED CITATION Sailik, S. (2026). Quantum Resilience: Why Boards Must Govern Time, Not Just Technology. LAMAH Boardroom Papers, No. 1. LAMAH Intelligent Solutions, Doha.

CONTACT LAMAH Intelligent Solutions | Level 13, Burj Marina Tower, Street 303, Lusail
PO Box 31260, Doha, State of Qatar | Tel +974 4144 7259 | Fax +974 4144 7198
info@lamahsolutions.com | lamahsolutions.com

Executive Summary

Quantum computing is usually discussed as a cybersecurity problem: which algorithms will break, which standards will replace them, and when. This paper argues that the framing is too narrow — and that the narrowness is itself a risk. Quantum risk is an operational resilience and governance problem, distinguished from every other threat an organisation plans for by a single characteristic: the event that creates the exposure may already have occurred, while the business impact may not arrive for years. Encrypted information harvested today can be stored indefinitely and decrypted when the capability arrives — a strategy known as harvest now, decrypt later — which means the exposure window opened before most organisations began paying attention.

This paper introduces **Time Horizon Risk** — the risk that the confidentiality lifetime of information exceeds the effective lifetime of the cryptography protecting it — and argues that it should become a Board-level consideration within enterprise risk management. It shows that European and American regulators are converging on precisely this logic: the European Union now classifies any use case as high-risk where confidentiality must survive ten years or more, with mandatory migration deadlines of 2030 and 2035, while NIST has committed to deprecating today's vulnerable algorithms by 2035. It examines what this convergence means for Qatar and the GCC, where supervisory frameworks draw on both traditions and preparatory signals are already visible, even though no binding regional mandate yet exists.

Finally, the paper proposes the **LAMAH Quantum Resilience Model**: five governance disciplines and five maturity levels through which boards can direct quantum readiness using operational resilience machinery they already own. It closes with seven questions every board should ask.

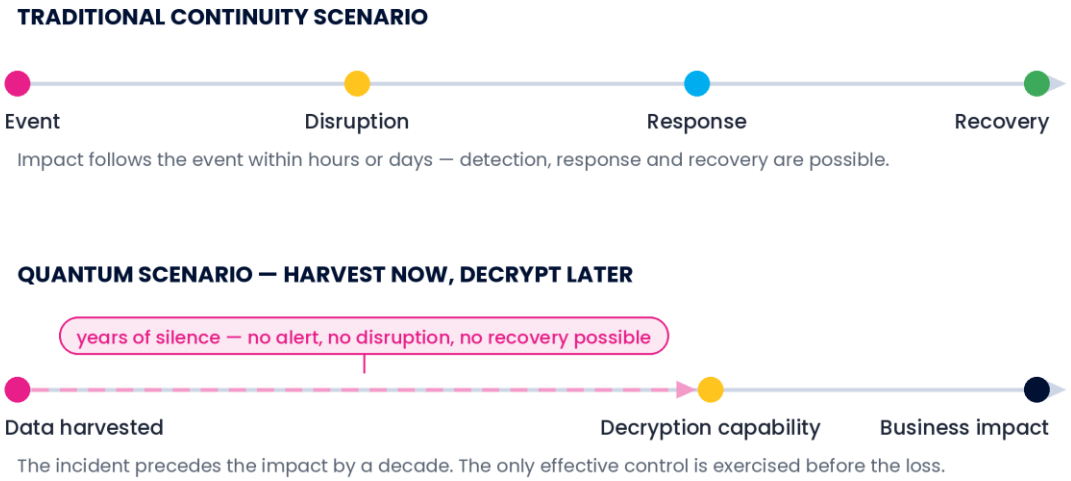
The quantum era has not yet arrived. The exposure window already has.

1 The Incident That May Have Already Happened

Imagine presenting the following scenario to your board. Last year, an attacker copied a large volume of encrypted information from your organisation — customer files, transaction records, board papers, due diligence documentation. They made no ransom demand, disrupted no systems and altered no records. Because the information remained encrypted, no regulatory notification was triggered, and the incident was closed as low-impact. For the next decade, nothing happens. Customers transact normally, audits find no material weakness, and the event fades from institutional memory. Then advances in quantum computing render the encryption protecting those records obsolete, and information that appeared secure throughout the intervening years becomes readable.

When, exactly, did the operational resilience failure occur? Not on the day the data became readable — by then, nothing could have been done. The failure occurred on the day the information was harvested, which was the organisation's last opportunity to prevent the outcome. Every continuity and resilience framework in use today, from ISO 22301 to the operational resilience regimes now embedded in financial regulation, assumes the opposite sequence: an event occurs, disruption follows, the organisation responds and recovers. Quantum risk reverses it. The initiating event may already be behind us; only the impact is still ahead.

EXHIBIT 1 The reversed sequence: quantum risk breaks the event-to-recovery logic of traditional continuity planning.



> ***Quantum computing is the first major business continuity threat whose impact occurs years after the incident itself.***

That inversion has an uncomfortable corollary: there is no recovery from retroactive decryption. Backup sites, crisis communications and disaster recovery plans are all instruments for restoring a disrupted present. None of them can restore the confidentiality of information that was copied years earlier. The only effective control is the one exercised before the loss — which is why quantum risk belongs to resilience and governance, disciplines concerned with acting ahead of disruption, rather than to incident response.

2 Why the Cybersecurity Framing Is Incomplete

The quantum conversation is currently owned by two communities: cryptographers, who frame it as an algorithm replacement problem, and security vendors, who frame it as a procurement decision. Both framings quietly assign the issue to the technology function, where it competes for budget with more immediate priorities

and predictably loses. Yet technology is only the mechanism through which the risk materialises. The question that should concern boards has little to do with quantum physics: **what happens if information that must remain confidential for decades is being collected today by adversaries who intend to read it tomorrow?** That is a governance question.

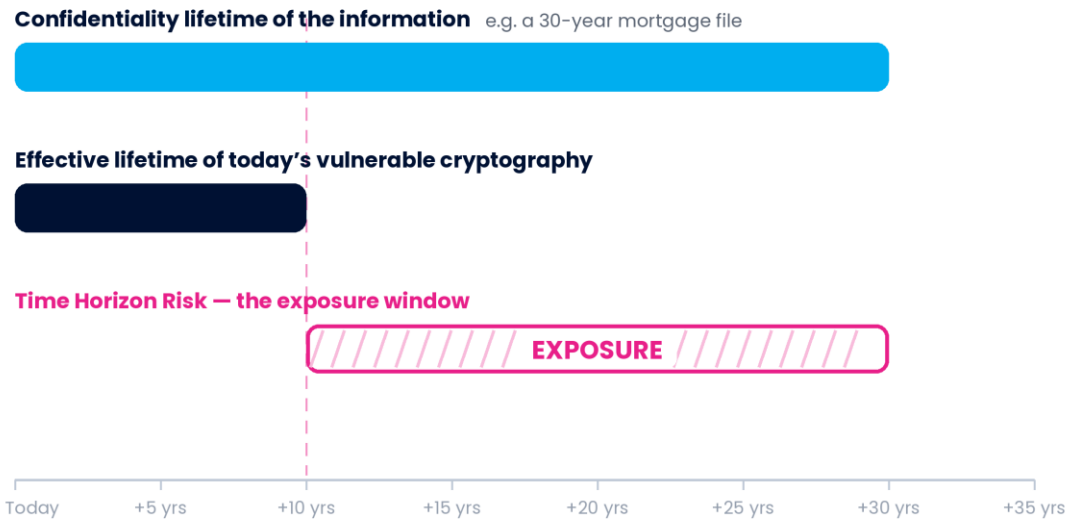
It is also no longer a speculative one. The Bank for International Settlements has identified quantum decryption as among the most significant cybersecurity threats facing the financial system, with the potential to expose transactions and much of the financial data stored today.[1] The scale of unpreparedness is equally documented: a joint study by Moody's and Corinium Intelligence found that 86 percent of organisations are not ready for post-quantum cybersecurity, even though 84 percent anticipate needing it within two to five years.[2] The gap between recognised threat and organisational response is precisely the space in which governance is supposed to operate.

3 Time Horizon Risk

Conventional risk assessment evaluates two dimensions — likelihood and impact — over a defined horizon, typically the coming year. Quantum risk introduces a third dimension that most enterprise risk frameworks have never had to consider explicitly: the lifetime of the information itself. The controlling question is no longer only how sensitive is this data, but for how long must it remain trustworthy — and whether the cryptography protecting it will remain effective across that entire period.

This paper names that exposure **Time Horizon Risk: the risk that the required confidentiality period of information exceeds the effective lifespan of the cryptographic controls protecting it.** Unlike conventional cyber risk, it grows silently. Nothing appears to happen, no control fails visibly, and yet each year of inaction moves the organisation closer to the point at which future computational capability outlives today's protection.

EXHIBIT 2 Time Horizon Risk: exposure arises where the confidentiality lifetime of information extends beyond the effective lifetime of the cryptography protecting it.



The concept has a rigorous ancestor. In what is now known as Mosca's theorem, the cryptographer Michele Mosca formalised the timing problem as a simple inequality: if the number of years information must remain secure, plus the number of years migration to quantum-resistant cryptography will take, exceeds the number of years until a cryptographically relevant quantum computer exists, the organisation is already too late.[3] Time Horizon Risk is the governance translation of that inequality. Its practical power lies in what it does not require: a board does not need to predict the arrival date of quantum computing — a number nobody knows — to act rationally. It needs to know two things that are entirely knowable facts about its own organisation: how long its information must stay confidential, and how long its migration will take. When those two numbers are large, uncertainty about the third is an argument for starting, not for waiting.

Three illustrations

Consider a retail bank. A thirty-year mortgage originated this year carries a confidentiality obligation — customer identification records, income documentation, property files — that runs to the 2050s. If that portfolio's records were harvested in encrypted form today and became readable in the mid-2030s, the bank would face notifying customers of a breach that occurred more than a decade earlier, with

twenty years of the obligation still to run. No incident response plan in existence addresses that scenario, because none was written for an incident whose detection postdates the compromise by ten years.

Consider an energy company. Engineering designs for national infrastructure — grid topologies, control system architectures, pipeline specifications — describe physical assets with forty-year operating lives. Exposure of those designs is not a data privacy incident; it is a national security and physical safety exposure that lasts as long as the asset stands. For critical infrastructure operators, Time Horizon Risk is measured not in retention schedules but in the service life of steel and concrete.

Consider a telecommunications operator. A carrier does not merely hold its own secrets; it transports an economy's worth of everyone else's. Encrypted traffic crossing an operator's backbone — and, in the case of satellite services, broadcast across footprints spanning entire regions — can be intercepted passively and stored at scale: harvesting a downlink requires an antenna, not an intrusion. The infrastructure compounds the exposure. Satellites and network platforms designed years before deployment operate for one to two decades, and while keys and software can often be updated from the ground, cryptography embedded in hardware makes retrofit capability limited and uneven — crypto-agility must be designed in, not bolted on. For telecommunications operators, Time Horizon Risk is measured not by the lifespan of cryptographic algorithms, but by the lifespan of the infrastructure that depends on them.

> ***Operational resilience has traditionally asked organisations to survive disruption. Quantum resilience requires them to survive time itself.***

4 The Dependency Nobody Maps

Modern operational resilience methodology rests on dependency mapping: identify the organisation's important business services, then map the people, processes, technology, facilities, data and third parties each service requires. Regulators across jurisdictions have made this mapping mandatory for financial institutions, and mature firms now maintain sophisticated inventories of data centres, cloud providers, telecommunications links, payment infrastructure and key personnel.

Almost no one maps cryptography. Yet encryption, digital signatures and public key infrastructure sit beneath virtually every service in those inventories: customer onboarding depends on digital certificates; payments depend on public-key exchange; remote access, software updates, electronic contracts, cloud storage and identity management all rest on cryptographic trust. It is shared critical infrastructure in the fullest sense — and it is absent from dependency maps, scenario libraries and board risk reports almost everywhere.

The omission matters because cryptographic compromise fails differently from every other dependency. When a data centre fails, services stop and dashboards turn red. When cryptographic trust fails, nothing stops. Applications remain available, customers experience no interruption, and every important business service continues operating comfortably within its impact tolerances — while the confidentiality and authenticity on which those services depend has already been irreversibly undermined. Availability metrics are silent on the question that matters. Operational continuity and information trust are not the same thing, and quantum computing is the risk that exposes the difference.

5 The Migration Itself Is an Operational Risk

Quantum computing in fact presents two resilience challenges, and the second receives far less attention than the first. Beyond protecting information against future decryption, organisations must eventually replace public-key cryptography

that has been embedded in enterprise technology for more than thirty years — across thousands of applications, certificates, interfaces, hardware security modules, operational technologies and vendor products, many of which were never designed to have their algorithms changed.

This creates a paradox that boards should sit with: the programme intended to strengthen resilience may itself become one of the largest sources of operational risk the organisation undertakes. A poorly sequenced migration can break interoperability between systems, interrupt customer services and stall on vendor dependencies outside the organisation's control. The task is therefore not algorithm selection — that work has been done by the standards bodies — but enterprise transformation: prioritisation, sequencing, testing, independent assurance and executive oversight. In other words, it demands exactly the governance disciplines that operational resilience programmes already exercise.

A NOTE ON QUANTUM KEY DISTRIBUTION

Post-quantum cryptography is not the only quantum-safe technology boards will hear about. **Quantum key distribution (QKD)** uses the physics of light, rather than mathematics, to establish encryption keys over dedicated optical links, with any interception detectable by design. The technology is real and maturing: commercial deployments now run over live carrier fibre networks,[4] and the Gulf is investing — Abu Dhabi's Technology Innovation Institute has built a quantum optical ground station and is working with Honeywell to test satellite-to-ground QKD links.[5]

The two technologies answer different questions. PQC is software: it runs on existing systems, protects information wherever it moves and rests, and provides the signatures and authentication on which digital trust depends — which is why every regulatory timeline cited in this paper mandates it. QKD is infrastructure: powerful but point-to-point, dependent on specialised hardware, and unable to authenticate by itself — it relies on classical or post-quantum cryptography underneath. National security agencies, including the NSA and the UK's NCSC,

accordingly position QKD as a complement for selected high-value links — a natural consideration for telecommunications operators, governments and financial market infrastructure — rather than a substitute for migration.[6]

For boards, the conclusion is convenient: QKD changes nothing about the sequence. Inventory, information longevity and crypto-agility come first; QKD is a later infrastructure decision for a narrow set of connections.

6 Regulatory Convergence: Three Traditions, One Destination

Organisations sometimes defer emerging risks with a familiar sentence: we will wait until the regulator tells us what to do. For quantum risk the logic fails on its own terms, because regulation cannot reverse the passage of time — it can compel future protection, but it cannot restore the confidentiality of information harvested in the years spent waiting. Regulatory developments should therefore be read as confirmation of direction rather than as the trigger for action. Read that way, the direction is now unambiguous, because the three regulatory traditions that shape Gulf supervisory practice are converging on the same conclusion.

The European track

In June 2025 the EU's NIS Cooperation Group published its Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, following the European Commission's Recommendation of April 2024.[7] Its most consequential provision is a classification rule with immediate bite: a use case is high-risk if a compromise of confidentiality ten or more years from now would still cause significant damage — a methodology drawn from the Dutch PQC Migration Handbook.[8] Member States must initiate national transition plans by the end of 2026; high-risk use cases must be migrated by the end of 2030; all remaining cases by 2035. Under this logic, long-lived data is high-risk today — the ten-year clock and

the harvest-now-decrypt-later clock are the same clock. For the financial sector the obligation is already live: the technical standards under the Digital Operational Resilience Act require entities to monitor cryptanalytic developments and address cryptographic threats, explicitly including those arising from advances in quantum computing.[9] Gulf firms with European parents, subsidiaries or counterparties will feel this contractually long before any local rule is written.

The American track

NIST finalised the first post-quantum cryptographic standards — FIPS 203, 204 and 205 — in August 2024,[10] and has set a formal sunset: under NIST IR 8547, today's quantum-vulnerable algorithms are to be deprecated after 2030 and removed from standards by 2035, with higher-risk systems expected to move earlier.[11] Just as significantly, the joint quantum-readiness guidance issued by CISA, the NSA and NIST frames the task in organisational rather than mathematical terms — establish a cryptographic inventory, prioritise by data sensitivity and longevity, engage the supply chain.[12] That is resilience methodology in federal clothing.

The financial stability track

The Bank for International Settlements has moved the issue onto the central banking agenda through its Innovation Hub's Project Leap, which began quantum-proofing experiments for the financial system and framed post-quantum migration as a financial-stability imperative, with further phases designed to bring additional central banks into scope.[13] Central banks calibrate supervisory agendas to BIS thinking; when the BIS names a threat to the financial system, supervisory expectations follow.

What this means for Qatar and the GCC

No GCC regulator has yet issued a binding post-quantum mandate, and this paper will not pretend otherwise. But the preparatory signals are visible at all three layers of the region's regulatory architecture. At the central-bank layer, Qatar Central Bank, SAMA and the Central Bank of the UAE draw directly on the BIS agenda described

above. At the national cybersecurity layer, agencies across the region — Saudi Arabia's National Cybersecurity Authority, the UAE's cybersecurity authorities and Qatar's national CERT — have signalled the incorporation of quantum-safe cryptography into national control frameworks, and regulated entities are beginning to be directed toward cryptographic asset inventories as a foundational readiness step. At the financial-centre layer, the QFCRA, DFSA and FSRA have each embedded operational resilience regimes requiring firms to map critical services and their dependencies — the QFCRA's regime takes effect in October 2026 — and that mapping methodology is precisely the vehicle through which quantum readiness should be delivered.

Both source traditions on which GCC frameworks have historically been built — NIST-derived national controls and European-style financial regulation — now point at the same requirement. The direction of regional supervision is therefore not in serious doubt; only its timing is. And for groups operating across several Gulf jurisdictions, that timing will almost certainly be uneven: requirements will arrive from multiple supervisors, on different schedules, in different vocabularies. **Firms that build readiness once, on a sound resilience foundation, will answer every regulator from the same evidence base. Firms that wait will respond several times, reactively, at greater cost.**

7 The Cost of Waiting

Resilience arguments persuade risk professionals; financial arguments persuade everyone else. The economics of quantum readiness are driven by an asymmetry: the earliest steps are the cheapest, and the cost of the later steps is a function of how late they begin. An orderly migration planned over eight years is absorbed within normal technology refresh cycles. A compressed migration executed under regulatory deadline — competing with every other late adopter for the same scarce cryptographic specialists and vendor attention — carries emergency pricing throughout.

The liability picture is shifting in parallel. Once recognised standards and published government timelines exist — and since 2024 they do — the legal question following a future disclosure event changes from whether the organisation could have known to why it did not act on what was knowable. Boards should expect historical harvesting incidents, once they become readable, to generate litigation and regulatory penalty exposure judged against today's published expectations, not yesterday's ignorance. Beyond liability sit the quieter costs: customer attrition when decade-old records surface; quantum readiness questions entering acquisition due diligence and, over time, insurance underwriting; and the valuation discount that attaches to any firm whose data liabilities are unquantified. Against all of this, the entry-level controls — data classification with a time dimension, a cryptographic inventory — are among the least expensive exercises in the entire GRC repertoire.

The clock is not the quantum computer's.

It is your data's.

8 The LAMAH Quantum Resilience Model

Quantum readiness should not become another standalone programme competing for attention. It should be governed through five interconnected disciplines that extend machinery most well-governed organisations already operate.

Information Longevity. Determine how long each category of critical information must remain confidential, authentic and trustworthy. This adds a time dimension to existing data classification and establishes the organisation's true quantum exposure — anything clearing the ten-year threshold is, by the EU's own definition, high-risk now.

Cryptographic Visibility. Inventory where vulnerable public-key cryptography exists across applications, infrastructure, cloud services, operational technology and third-party platforms. Organisations cannot manage what they cannot see, and every regulatory framework surveyed above treats this inventory as the non-negotiable first step.

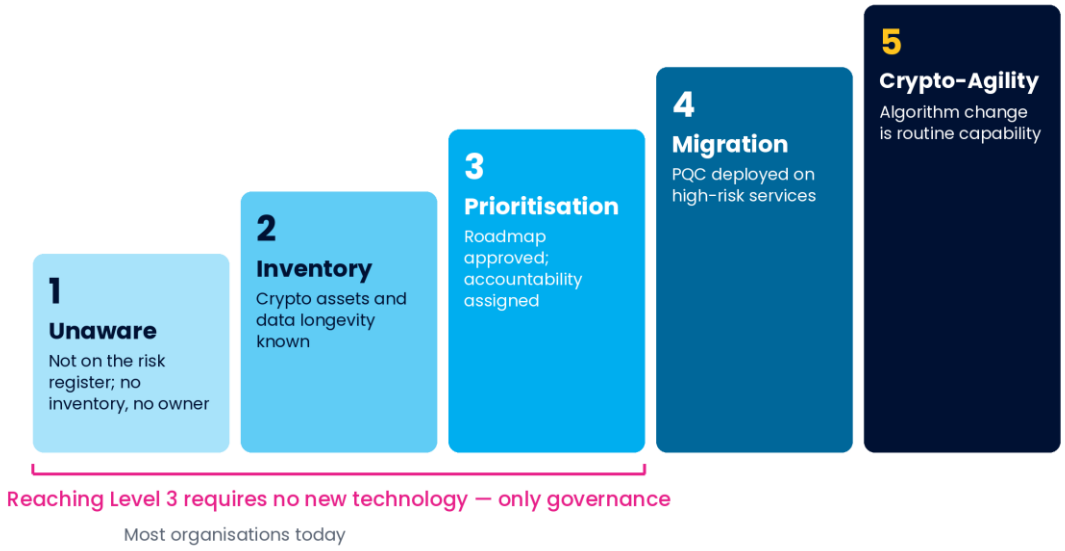
Critical Service Dependency. Extend operational resilience dependency maps to include the cryptographic trust supporting each important business service — recognising cryptography as a critical dependency in exactly the way cloud providers and telecommunications networks are already recognised.

Migration Governance. Treat the transition to post-quantum cryptography as an enterprise transformation programme: prioritised by Time Horizon Risk, sequenced to protect the longest-lived and highest-impact data first, and governed with executive sponsorship, testing and independent assurance.

Continuous Adaptation. Standards, vendor capabilities and supervisory expectations will keep evolving for a decade. Readiness is therefore a continuous governance capability — crypto-agility as an organisational property — rather than a one-time project with an end date.

The model carries an assessment dimension. Five maturity levels locate where an organisation stands and what the next step is — and they make one point boards should find liberating: reaching Level 3 requires no new technology at all, only governance.

EXHIBIT 3 Five maturity levels, from Unaware to Crypto-Agility. Most organisations today sit between Levels 1 and 2.



Level	Stage	Characteristics
Level 1	**Unaware**	Quantum risk absent from risk registers and board reporting; no cryptographic inventory; no owner.
Level 2	**Inventory**	Cryptographic assets catalogued; data classified by confidentiality lifetime; Time Horizon Risk assessed and reported.
Level 3	**Prioritisation**	Exposure ranked by information longevity and service criticality; executive accountability assigned; board-approved migration roadmap in place.
Level 4	**Migration**	Post-quantum cryptography deployed on the highest-risk services; suppliers contractually engaged on migration roadmaps; progress independently assured.

Level 5	**Crypto-Agility**	Algorithm change is a routine, tested organisational capability; readiness monitored continuously as standards and threats evolve.

The distance from Level 1 to Level 3 — the point at which an organisation can demonstrate governed readiness to any supervisor, counterparty or acquirer — is measured in months of governance work, not years of technology spend.

9 Seven Questions Every Board Should Ask

Board oversight of quantum readiness need not begin with technical standards. It should begin with the following questions — which deliberately avoid algorithms, because boards govern outcomes and management determines implementation.

1. Which information held by our organisation must remain confidential beyond the expected lifetime of today's cryptographic standards?
2. Where does vulnerable public-key cryptography underpin our critical business services?
3. Which third parties control our most important cryptography, and what are their post-quantum migration roadmaps?
4. Who within executive management is accountable for quantum readiness?
5. Is Time Horizon Risk reflected in our enterprise risk and operational resilience reporting?
6. What would an orderly migration cost over the coming years — and what would an emergency migration cost under a regulatory deadline?
7. If our primary regulator requested evidence of our quantum readiness tomorrow, what could we show today?

10 Conclusion: A New Chapter in Operational Resilience

Each generation of business leaders faces a development that changes accepted thinking: globalisation transformed supply-chain risk, the financial crisis transformed enterprise risk management, the pandemic transformed operational resilience. Quantum computing is a credible candidate for the next inflection point — not because cryptographic collapse is imminent, and not because every organisation faces the same urgency, but because it quietly withdraws an assumption on which digital trust has rested for decades: that today's cryptography will remain effective for as long as tomorrow's information requires protection.

Once that assumption is questioned, resilience must evolve. The objective is no longer only to recover from disruption; it is to ensure that today's decisions continue protecting tomorrow's organisation. Boards that begin now — classifying information by longevity, making cryptography visible, engaging suppliers and governing migration deliberately — will have time on their side, and will meet every future supervisory expectation from a single evidence base. Those that wait for certainty may find that certainty arrives years after the opportunity to act.

The relevant question, in the end, is not when cryptographically relevant quantum computers will arrive. It is which of our information assets must still be protected when they do. For most organisations that information already exists — and for some of it, so may the copies. **The clock is not the quantum computer's. It is your data's.**

References

1. Bank for International Settlements, Innovation Hub, Project Leap: Quantum-Proofing the Financial System (2023).
2. Moody's / Corinium Intelligence, post-quantum readiness survey (2024).
3. Mosca, M., "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?", IEEE Security & Privacy, vol. 16, no. 5 (2018).
4. Quantum Corridor and Toshiba, first cross-state QKD demonstration over a live commercial carrier fibre network in the United States (December 2025).

5. Technology Innovation Institute (Abu Dhabi), Abu Dhabi Quantum Optical Ground Station (2024); TII–Honeywell collaboration on satellite QKD (November 2025).

6. NSA, Quantum Key Distribution (QKD) and Quantum Cryptography guidance; UK National Cyber Security Centre, Quantum Security Technologies white paper.

7. NIS Cooperation Group, Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (June 2025); European Commission Recommendation C(2024) 2393 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography (11 April 2024).

8. AIVD, TNO and CWI, The PQC Migration Handbook, §2.4 (risk classification methodology).

9. Commission Delegated Regulation (EU) 2024/1774 supplementing DORA with regulatory technical standards on ICT risk management, Arts. 6–7.

10. NIST, FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), finalised August 2024.

11. NIST IR 8547, Transition to Post-Quantum Cryptography Standards (initial public draft, November 2024).

12. CISA, NSA and NIST, Quantum-Readiness: Migration to Post-Quantum Cryptography (joint factsheet, August 2023).

13. BIS Innovation Hub, Project Leap, Phase 1 report (2023).

About the author. Saleh Sailik is the Managing Director of LAMAH Intelligent Solutions, where he leads the firm's work at the intersection of business strategy, enterprise technology and risk. With nearly two decades of experience, he advises Boards and executive teams on navigating complex technological, regulatory and organisational change—helping them translate emerging risks into practical governance, strategic decisions and executable transformation programmes across Qatar and the GCC.

About LAMAH Intelligent Solutions. LAMAH Intelligent Solutions is a Qatar-based management consulting and enterprise IT firm. LAMAH operates across three lines of business—Consulting, Outsourcing, and Managed Services—and serves three core domains: Digital Transformation, IT GRC, and Corporate Integrated Risk Management. We advise on what to change and deliver how to do it—seamlessly combining business consulting with enterprise technology execution.

About this series. The LAMAH Boardroom Papers present original perspectives on emerging governance and resilience challenges facing Boards and executive management in Qatar and the wider Gulf region. To discuss a quantum readiness assessment or a Board briefing for your organisation, contact the LAMAH advisory team.

Turning Complexity into Clarity
Risk into Opportunity
Strategy into Execution

LAMAH
INTELLIGENT SOLUTIONS

Digital Transformation | Risk & Resilience | Technology Execution

INNOVATE. TRANSFORM. LEAD.

Level 13, Burj Marina Tower, Street 303, Lusail
PO Box 31260, Doha, State of Qatar
+974 4144 7259 | info@lamahsolutions.com | lamahsolutions.com