

SEPTEMBER 2026

The State of Post-Quantum Readiness in Key GCC Markets

A survey of how enterprises across key GCC markets are preparing to replace quantum-vulnerable cryptography.

Supported by



Contents

INTRODUCTION

Forewords	05
About This Report	07
Executive Summary	08
Five Key Findings	09

SECTIONS

01	The Quantum Threat	10
	What PQC is • What quantum breaks • Harvest now, decrypt later • Why migration starts now	
02	Where the World Stands	16
	NIST standards • National mandates • Enterprise adoption • The UAE framework • The GCC landscape	
03	Survey Findings and Analysis	21
	Nine findings, from threat perception to what each audience should do next	
04	Strategic Insights	31
	Six recommended actions, in the order to take them	

CLOSING AND REFERENCES

Conclusion	34
The Organizations Behind This Report	35
Glossary	37
References	38



H.E. Dr. Mohamed Al Kuwaiti
Head of Cyber Security for the UAE
Government; Chairman, UAE Cyber
Security Council

*“Cybersecurity is now part of
the foundation on which
nations operate.”*

Building national resilience for the quantum era

In the UAE, we treat cybersecurity as national infrastructure. It protects the networks, services, and institutions our nation depends on. This approach has strengthened the UAE’s digital resilience and prepared us for the next challenge.

Quantum-safe cryptography is now part of that challenge. It affects every critical sector, including finance, energy, healthcare, and government. No organization can address it alone. Systems are connected, supply chains are shared, and weaknesses can spread across sectors. The country needs a coordinated response.

The UAE Cyber Security Council is leading this work through the National Post-Quantum Migration Program. The program gives critical sectors a clear path forward. The National Cryptography Center supports that effort as the national authority for cryptographic standards. It sets the requirements organizations will follow and provides a common reference for approved algorithms, cryptographic discovery, risk assessment, and migration planning.

Organizations that align early will be better placed to plan their work, control costs, and avoid having to repeat it later. Nationally developed cryptographic libraries can also support this effort. When they meet national requirements, they provide a trusted foundation and help keep the cryptography protecting national systems under national control.

This report shows how enterprises across selected GCC markets are preparing for quantum-related cryptographic risk. It highlights the work already underway, and also gives leaders a way to compare their own readiness with that of their peers.

The findings point to a clear starting point. Organizations need to identify where vulnerable cryptography is used, determine which systems and data require priority, and assign clear responsibility for the work ahead.

I thank QuantumGate and the organizations that supported this research for their contribution to national cyber resilience. The UAE Cyber Security Council and the National Cryptography Center will continue to work with government and industry to support a secure, coordinated move to quantum-safe cryptography.

The quantum era is here

For more than a decade, the risk quantum computing poses to cryptography belonged mainly to research discussions. That is no longer the case. In 2024, NIST finalized the first three post-quantum cryptography standards, and migration guidance now points to the retirement of today's public-key algorithms by 2035. Organizations have standards they can use and a deadline they cannot ignore.

Long-lived data brings that date forward. Encrypted information can be collected today and stored until a capable quantum computer exists. No one can say exactly when that will be, but we already know how long health records, government information, financial data, and critical infrastructure data must remain confidential. For organizations holding data of that kind, the exposure exists now, and the confidentiality period is the timeline to plan against.

The work itself takes years. Public-key cryptography sits deep inside networks, applications, identity systems, certificates, devices, and third-party services. Replacing it is more than a routine software update. It is a program that has to be planned, sequenced, and funded across several budget cycles, which is why the starting date matters as much as the deadline.

The UAE began building this capability early. The Technology Innovation Institute launched the country's first post-quantum cryptography library and has contributed to NIST's wider standardization work, including HQC and additional digital signature candidates. That research now supports a national program connecting technical standards, cryptographic discovery, and deployment across critical sectors, and it reflects a decision to shape the quantum-safe future through the country's own research, standards, and technologies.

QuantumGate carries that work into enterprise environments. We help organizations locate vulnerable cryptography across complex systems and build migration plans based on evidence. This reflects a principle that has guided our work at TII: research must leave the laboratory and solve real problems.

The survey in this report shows where the immediate challenge lies. Many organizations have allocated budgets and begun planning. Far fewer have begun a cryptographic inventory or set a clear migration path, and that inventory is what everything after it depends on.

There is no shortcut. Organizations need a verified inventory, a roadmap built on data sensitivity and business risk, clear ownership, and systems that can absorb future algorithm changes without another major rebuild.

The standards are in place. The next task is to put them to work.



Dr. Najwa Aaraj

Chief Executive Officer, QuantumGate
and Technology Innovation Institute

*“The standards are in place.
The next task is to put them to
work.”*

Method, sample, and scope

This report is published by QuantumGate and the UAE Cyber Security Council, with support from the National Cryptography Center and Technology Innovation Institute. It examines how ready enterprises across selected GCC markets are to protect long-lived data against the shrinking window in which today’s encryption remains reliable, as quantum computing advances.

EVIDENCE BASE 01

A survey of 125 senior leaders

Respondents hold C-suite roles (CTO, CIO, CISO, CRO), VP and Director of IT positions, digital transformation leadership, and heads of cybersecurity and compliance, across financial services, energy, healthcare, telecommunications, technology, government, and travel. Two thirds work in organizations of 1,000 employees or more. Cybersecurity decision makers or members of the decision-making team account for 94% of the sample, and a third are the sole decision maker for cybersecurity.

Respondents were screened for familiarity with post-quantum cryptography, and almost all describe themselves as very or somewhat familiar with it. Findings should therefore be read as the position of senior security leaders already engaged with this question, rather than of the market as a whole.

The survey was designed and fielded by an independent third-party research partner using its own respondent panel. Respondents were anonymous, were not QuantumGate customers or contacts, and QuantumGate had no role in selecting them. Respondents are based in the United Arab Emirates, Saudi Arabia, and Qatar; findings are reported at regional level and are not broken down by country.

EVIDENCE BASE 02

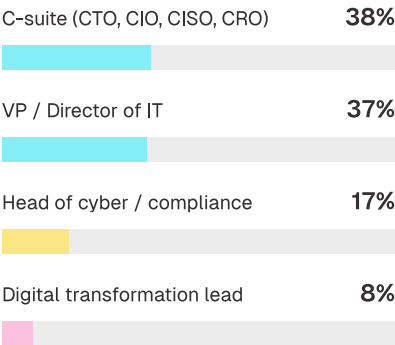
A review of the global landscape

A review of the global quantum-security landscape drawing on the finalized NIST standards¹ and the migration roadmaps of national agencies including the U.S. National Security Agency², the UK National Cyber Security Centre³⁻⁴, and the EU’s ENISA⁵, to set the regional findings in international context.

All findings are self-reported and reflect how respondents assess their own organizations. They are not an audit and may differ from what regulators or external assessments would observe. Figures are presented as the survey recorded them and are rounded to the nearest whole percentage, so some exhibits do not sum to 100. All percentages refer to the full sample of 125 respondents unless stated otherwise.

EXHIBIT 1

Who was surveyed



n = 125. Every respondent is involved in, or informs, cybersecurity decisions.

WHAT THIS REPORT COVERS

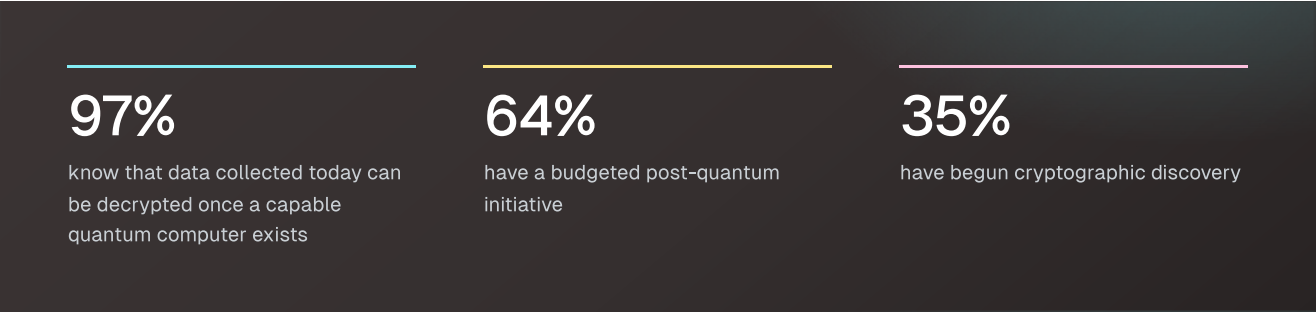
- Awareness of the threat
- Migration planning
- Cryptographic visibility
- Barriers to adoption
- Demand for sovereign or local control

NOTE ON ATTRIBUTION

The findings, analysis, and recommendations set out in this report are those of QuantumGate. They do not represent the views or the position of any individual named in this report, or of the organizations those individuals represent. No statement in this report may be attributed to any named individual, and no named individual may be quoted on its content. Requests relating to this report, including requests for comment, clarification, or use of any material in it, should be directed to the relevant organization.

Cryptographic discovery is the next step

Senior technology and security leaders across selected GCC markets are funding post-quantum migration and planning for it. Fewer have begun the cryptographic inventory that the rest of the work depends on.

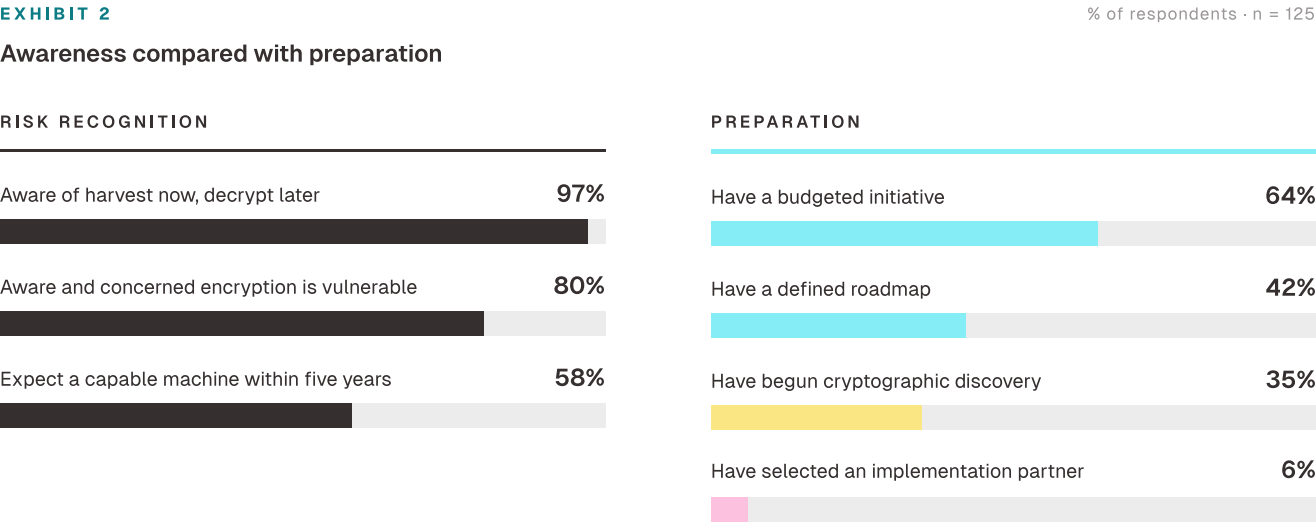


The deadlines are firmer than the technology. NIST’s draft transition guidance points to today’s public-key algorithms being retired by 2035, major platform providers are moving ahead of that date, and 58% of respondents expect a capable machine within five years.

Funding is largely in place, with 64% carrying a budgeted initiative and 42% working to a defined roadmap. Only 34% rate themselves well or very well prepared. Respondents name cost, the complexity of the transition, and the lack of ready-to-deploy solutions as the main barriers.

Nearly all respondents, 98%, require cryptographic solutions that are nationally governed, locally controlled, or both. Buyers in these markets treat this as a standard procurement condition.

For most organizations the first move is the same. A verified cryptographic inventory is what lets a migration be sized, sequenced, and budgeted, and it is the least expensive step in the program.



Each figure comes from a separate survey question. Respondents did not pass through these stages in sequence.
Source: QuantumGate Post-Quantum Readiness Survey, 2026 (n=125).

Five key findings

Five findings from the survey, in the order they matter to a migration program.

1	Awareness is ahead of execution Two-thirds say they can see all their cryptographic keys, certificates and algorithms. Of those 83 organizations, 41% have conducted or begun a discovery exercise. The rest are describing familiarity with their estate, and self-reported readiness therefore overstates the verified position.	66% vs 41% CLAIM FULL VISIBILITY VS. HAVE RUN DISCOVERY
2	The timeline has shortened 58% expect a cryptographically relevant quantum computer within five years, and harvest now, decrypt later brings that exposure forward for data that must stay confidential into the 2030s.	58% EXPECT A CAPABLE MACHINE WITHIN FIVE YEARS
3	Cost and complexity lead the barriers The barriers named most often are practical. Cost of implementation leads at 49%, while lack of executive sponsorship was named least often of the barriers tested, at 17%.	49% vs 17% COST VS. LACK OF EXECUTIVE SPONSORSHIP
4	Delivery decisions are still open Most organizations have yet to define how migration will be delivered — internally, through a partner, or as a hybrid. Choices made over the next two years will shape programs for years afterwards.	58% vs 6% EVALUATING OPTIONS VS. IDENTIFIED A PREFERRED PARTNER
5	Sovereign and local control are widely required 98% require cryptographic solutions that are nationally governed, locally controlled, or both — making national or local control a standing procurement requirement across these markets.	98% REQUIRE SOVEREIGN OR LOCAL CONTROL

Source: QuantumGate Post-Quantum Readiness Survey, 2026 (n=125).

01

The Quantum Threat

Why encrypted data can be exposed before a capable quantum computer arrives.

1.1	What post-quantum cryptography is	1.4	Harvest now, decrypt later
1.2	What quantum breaks, and what it does not	1.5	Why migration has to start now
1.3	When a capable machine might arrive		

1.1

What post-quantum cryptography is, and why it exists

Cryptography protects information, proves it has not been altered, and verifies identities. Banking, communications, government services and almost every online transaction depend on it.

Modern cryptography rests on two principal families. The first is symmetric cryptography, where AES and the hash functions used to check integrity depend on computations that are impractical to reverse. The second is public-key cryptography, where RSA and ECC depend on mathematical problems that are quick to compute in one direction and, as far as anyone knows, impractical to reverse without the matching private key.

Public-key cryptography therefore rests on an assumption about what an attacker can compute. It is not a physical guarantee. The assumption has held for decades because no known classical algorithm can solve those problems at the key sizes in use, and it holds only as long as that stays true.

Post-quantum cryptography (PQC) is a set of algorithms built on different mathematical problems, chosen because no efficient quantum attack on them is known.¹ They run on ordinary computers. Defending against quantum computing does not require owning one.

Timing is what separates this from most security work. A software flaw can be patched once it is found. Encryption cannot be applied retroactively, so replacing an algorithm later does nothing for data captured while the old one was still in use. For information that must stay confidential for years, the algorithm has to be right at the moment the data is sent or stored.

Authentication behaves differently. A signature already verified cannot be forged after the fact, so the deadline there is the arrival of a capable machine rather than any earlier date. The reason to start early is that certificates, code-signing keys and roots of trust take years to replace.

This is also why the transition runs as a multi-year program. The algorithms have already been chosen and standardized. What remains is building them into products, testing them, and rolling them out across estates that were never designed to have their cryptography swapped. Section 1.5 sets out the order of work, and the arithmetic that decides how much time an organization actually has.

You cannot go back and encrypt data an adversary already holds.

WHERE CRYPTOGRAPHY SITS

- Applications
- Devices and endpoints
- Networks and protocols
- Cloud services
- Identity systems
- Certificates and keys
- Stored data, backups and archives
- Third-party systems

Every layer holds cryptographic assets, which is why an inventory is the first task rather than a later one.

1.2

What quantum computing breaks, and what it does not

Symmetric cryptography survives. Public-key cryptography has to be replaced.

Most digital systems rely on public-key cryptography, mainly RSA and ECC. They are relied on today because no known classical algorithm can solve the mathematical problems behind them fast enough to make an attack practical. Those problems are integer factorization and the discrete logarithm problem.

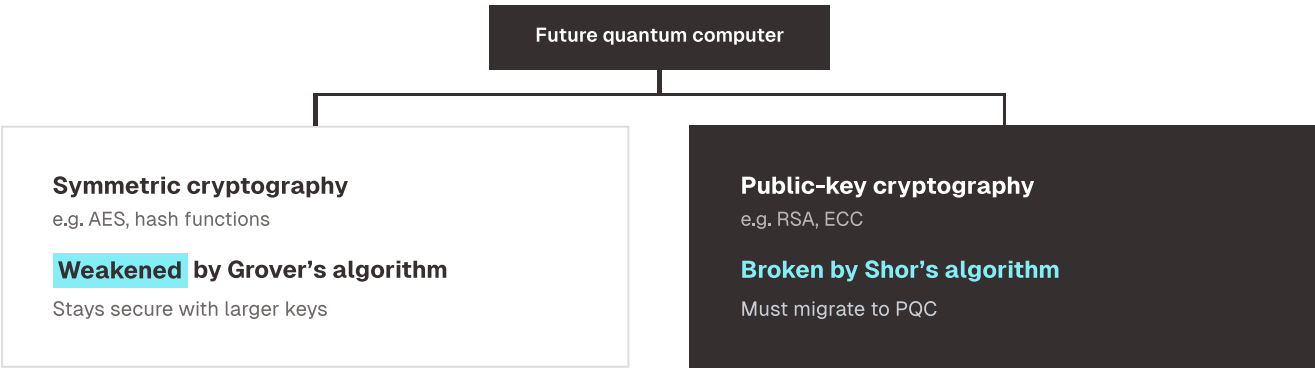
Quantum computing changes that. In 1994, Peter Shor showed that a sufficiently powerful quantum computer could solve both problems efficiently.⁶ The consequence that matters is not simply speed. Shor’s method scales in a way that means increasing the key size no longer buys meaningful protection, so RSA and ECC cannot be strengthened. They have to be replaced.

Symmetric cryptography is affected differently. A second quantum method, Grover’s algorithm, speeds up brute-force search and roughly halves the effective strength of a symmetric key. AES-256 would offer about the protection a 128-bit key gives today. Because key length can be increased, the fix here is straightforward.

In practice it is smaller than that suggests. Organizations already on AES-256 need no change, AES-128 is worth reviewing on a normal lifecycle, and SHA-256 and above remain suitable. Grover’s speedup also requires a very long sequence of operations that does not parallelize well, which is why symmetric cryptography sits low on most migration plans.

That leaves two tasks of very different size. Symmetric cryptography needs a key-length review. RSA and ECC need replacement, which is why national migration programs center on transitioning away from them. The new algorithms are usually deployed in hybrid mode, alongside the existing ones, so protection holds even if one algorithm is later broken.

EXHIBIT 3
How a future quantum computer affects today’s cryptography



Grover’s algorithm roughly halves the effective strength of a symmetric key, which a longer key restores. Shor’s algorithm solves the integer factorization and discrete logarithm problems that RSA, Diffie-Hellman, and elliptic-curve cryptography rest on, so for those algorithms no key length is sufficient. Post-quantum algorithms are built on different mathematical problems that Shor’s algorithm does not solve.

1.3

When a capable machine might arrive, and what sets the deadline

How much time is there? Three kinds of answers are available: the companies building the hardware publish engineering milestones, independent researchers publish probability estimates, and governments publish migration deadlines. Only the third is fixed, and for most organizations it is the one that governs.

The hardware roadmaps have converged on the end of this decade. IBM states it will deliver a fault-tolerant system in 2029, running 100 million gates on 200 logical qubits.⁷ Quantinuum is targeting a universal, fully fault-tolerant machine in the same year.⁸ Microsoft brought its own target forward to 2029 during 2026.⁹ IonQ publishes a larger target still, of 2 million physical and 80,000 logical qubits by 2030.¹⁰ Google has not published a date and is working toward a long-lived logical qubit.¹¹

These are commercial roadmap targets rather than independently verified forecasts, and they are not directly comparable with each other. Different architectures require very different numbers of physical qubits for each logical qubit, so two companies quoting the same year may mean quite different machines. The published range should be read as a range, not as a date.

What the roadmaps do not settle is how much machine cryptography requires. The most recent published estimate puts the factoring of RSA-2048 at fewer than 1 million physical qubits running for under a week.¹² Published roadmap targets for 2029 are in the tens of thousands of physical qubits. The estimate itself has moved: the same lead author's 2019 figure was 20 million qubits, and the reduction came from improvements in algorithms and error correction rather than from hardware.

That asymmetry matters for planning: hardware progress is announced, dated, and can be tracked, while improvements in algorithms and error correction appear on no roadmap and arrive without notice.

Independent assessment sits between the two. The Global Risk Institute's 2025 expert survey, conducted with evolutionQ, put the likelihood of a cryptographically relevant quantum computer at 28% to 49% within 10 years and 51% to 70% within 15, drawing on 26 specialists. That ten-year figure is the highest recorded in the seven years the survey has run.¹³

Governments have not waited for the science to settle. In the UAE, the Cyber Security Council's National Post-Quantum Migration Program and the National Cryptography Center will define the standards, migration requirements, and timelines that designated entities work to^{14–15}, and section 2.4 sets out that framework. Internationally, the UK expects discovery and planning to be complete by 2028, priority services migrated by 2031, and the work finished by 2035.⁴ The EU calls for high-risk systems to move by 2030.¹⁶ A US executive order signed in June 2026 sets 2030 for federal agencies on encryption and directs acquisition rulemaking toward the same year for covered contractors.¹⁷

For an enterprise this is more tractable than the spread of dates suggests. The arrival of a capable machine cannot be controlled or verified, and it is not what sets the schedule. What sets the schedule is how long the organization's data must stay confidential, how long its migration will take, and what its national requirements will oblige it to do. Sections 1.4 and 1.5 take the first two in turn.

PUBLISHED MILESTONES	
IBM	2029
Fault-tolerant system: 100 million gates on 200 logical qubits	
Quantinuum	2029
Universal, fully fault-tolerant system	
Microsoft	2029
Fault-tolerant system, target brought forward during 2026	
IonQ	2030
2 million physical, 80,000 logical qubits	
IBM	2033
2,000 logical qubits	

FOR COMPARISON	
RSA-2048 · fewer than 1 million physical qubits, about a week	
Published estimate, 2025. The 2019 estimate was 20 million.	

Company-published targets, as announced, and not independently verified. Architectures differ, so qubit counts are not directly comparable between companies. These are engineering goals, not dates for breaking RSA.

1.4

Harvest now, decrypt later: why the risk is already here

DATA THAT MUST STAY
CONFIDENTIAL INTO THE 2030S

- Diplomatic communications
- Intellectual property
- Healthcare records
- Financial and account records
- Government and defense records
- Biometric data
- Classified information
- Long-lived personal data

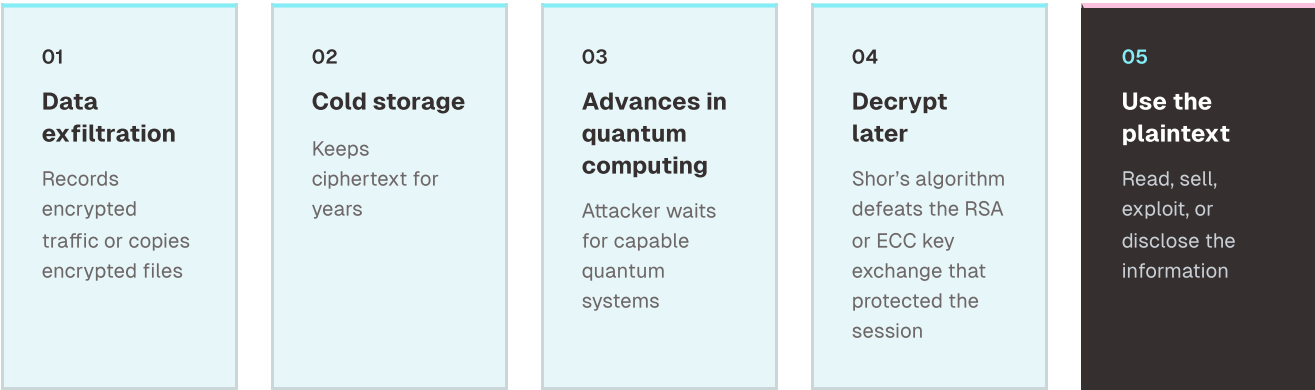
Harvest now, decrypt later describes adversaries collecting encrypted data today with the intention of decrypting it once sufficiently powerful quantum computers exist. The ciphertext cannot be read today. What has already failed is the guarantee, because once a copy is in an adversary’s hands the organization no longer controls how long it stays secret.

The exposure runs through key establishment. The data itself is protected by symmetric encryption, which survives, but the key protecting it was agreed using RSA or elliptic-curve cryptography. Recovering that key later yields the session key, and the session key opens the stored data.

This applies to any information that must remain confidential into the 2030s, and it shifts post-quantum security from a future technology discussion to a present-day data protection issue. The survey findings reflect that shift: 97% of respondents reported awareness of the risk, and 69% said they are actively concerned about its implications for long-term confidentiality and enterprise resilience.

EXHIBIT 4

Harvest now, decrypt later



YEARS CAN PASS

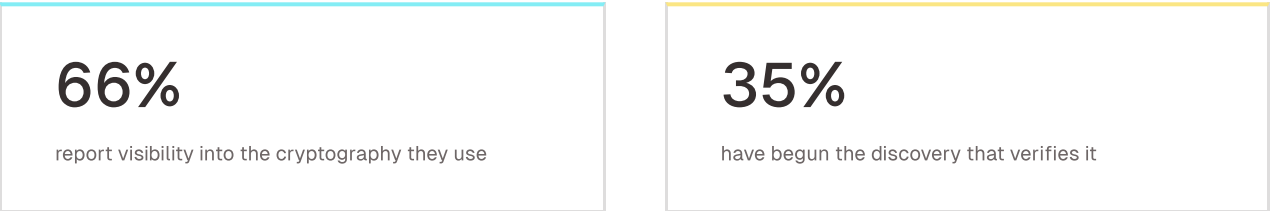
Encrypted data can sit for years until quantum catches up.

1.5

Why migration has to start now: crypto-agility and early planning

Crypto-agility refers to an organization’s ability to replace or upgrade cryptographic algorithms, keys, certificates, and protocols without major operational disruption.

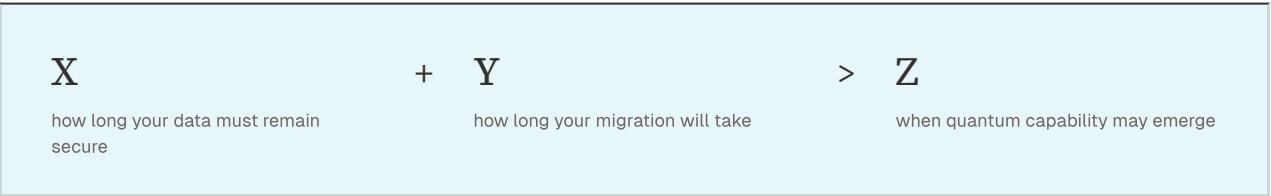
It is becoming essential as enterprises prepare for post-quantum cryptography, because most organizations run complex, fragmented environments where cryptography is embedded across applications, devices, networks, cloud services, and third-party systems. The survey separates two things that are easily confused. Two-thirds of respondents, 66%, report visibility into the keys, certificates, algorithms and protocols they use, while 35% have conducted or initiated the cryptographic discovery that establishes which of those algorithms are quantum-vulnerable. General familiarity with an estate is more common than a verified inventory of it, and section 3.3 sets out the distance between them.



Complexity is not the only reason agility matters. The post-quantum standard set is still expanding, so an organization that hard-codes a single algorithm will face the same exercise again. Section 2.1 sets out what is still to come.

Assumptions can also be tested. In August 2026 a preliminary paper by Daniel Simon claimed a polynomial-time quantum algorithm for the Dihedral Coset Problem, which underlies the lattice assumptions behind the standardized algorithms. Independent review, including work by cryptographers at TII, found gaps in the proof, and at the time of publication the standardized algorithms are assessed as unaffected. No hardness assumption should be treated as permanent, and the protection is the ability to change algorithm without rebuilding.

The timing question resolves into arithmetic each organization can do for itself. Mosca’s inequality, named for the cryptographer who set it out³⁸, holds that if the time data must stay confidential plus the time a migration takes exceeds the time until a capable machine exists, that data cannot be protected. Two of those three terms are already known inside the organization. Only the third is uncertain.



Under harvest now, decrypt later, long-lived data is effectively exposed today, whatever the eventual arrival date.

Migration therefore begins with cryptographic discovery: identifying cryptographic dependencies, flagging systems that rely on vulnerable algorithms, and assigning clear ownership for the transition. Not everything carries equal urgency. Key establishment protecting data with a long confidentiality requirement comes first, while signatures and certificates are assessed according to the lifetime of each credential. NIST,¹ ENISA,⁵ and multiple national agencies have all stressed that post-quantum migration takes years, not months, given infrastructure complexity, vendor dependencies, regulatory requirements, and operational risk.²⁻⁴ In the UAE, the National Cryptography Center will define the standards and migration requirements that designated entities work to,¹⁵ which is a further reason to establish a cryptographic position early. Organizations that begin inventory and assessment now retain control of their own sequencing and budget cycles, and that control is the main thing an early start buys.

02

Where the World Stands

How global standards, national mandates, early enterprise adoption, and the UAE’s own national framework are shaping the transition to quantum-safe security.

2.1 NIST has published the first standards

2.2 Governments are moving from awareness to mandates

2.3 Enterprise adoption is early but accelerating

2.4 The UAE national post-quantum framework

2.5 The GCC policy and initiative landscape

2.1

NIST has published the first standards

The global transition to post-quantum cryptography accelerated significantly following the publication of the U.S. National Institute of Standards and Technology (NIST) Post-Quantum Cryptography standards. Following an eight-year evaluation involving cryptographers, technology companies, academic institutions, and government agencies worldwide, NIST published its first post-quantum cryptography standards in 2024.¹

The initial standards include ML-KEM¹⁸ (Module-Lattice-Based Key-Encapsulation Mechanism) for key establishment, together with ML-DSA¹⁹ (Module-Lattice-Based Digital Signature Algorithm) and SLH-DSA²⁰ (Stateless Hash-Based Digital Signature Algorithm) for digital signatures. These standards establish the foundation for the next generation of quantum-resistant public key cryptography.^{18–20} The standardization effort remains ongoing as NIST continues to expand and refine the post-quantum standard set.

ML-KEM FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Key establishment	ML-DSA FIPS 204 Module-Lattice-Based Digital Signature Algorithm Digital signatures	SLH-DSA FIPS 205 Stateless Hash-Based Digital Signature Algorithm Digital signatures
--	---	--

Since then, NIST has continued to advance the program. FIPS 206, which will standardize FN-DSA based on Falcon, remains in development. NIST previewed the forthcoming initial public draft at its standardization conference in September 2025.¹ HQC was selected in March 2025 as an additional key-encapsulation mechanism. It is code-based rather than lattice-based, which gives the standard set mathematical diversity, and NIST expects final publication in 2027.²¹ In May 2026, NIST advanced nine candidates to the third round of its process for additional digital signature algorithms, a phase expected to run for about two years.²² Draft NIST IR 8547 proposes a transition timeline for quantum-vulnerable public-key cryptography. Schemes at the 112-bit security level, which covers much of what is deployed today, would be deprecated after 2030, and the classical public-key schemes it lists would be disallowed after 2035.²³ In June 2026, NIST released initial working drafts of SP 800-73 and SP 800-78, updating Personal Identity Verification specifications to support ML-KEM and ML-DSA.²⁴

NIST's standards are the reference point most national programs and vendors are working from. Technology vendors, cloud providers, financial institutions, and government agencies are aligning product roadmaps and security strategies around these algorithms, creating a common foundation for interoperability, cryptographic agility, and long-term resilience.¹

For enterprises, the practical point is that the standards needed to begin migration already exist and are finalized. ML-KEM, ML-DSA, and SLH-DSA were published in 2024 and are the basis of the national migration programs published so far. The work still in progress adds options and application-specific guidance rather than changing that starting point, which is why crypto-agility matters more than waiting for the full set to arrive.

2.2

Governments are moving from awareness to mandates

Several governments have moved from awareness campaigns to migration programs with dated requirements. In the United States, National Security Memorandum 10 (NSM-10) directed federal agencies to inventory cryptographic systems, assess quantum-related risks, and prepare migration plans.²⁵ The National Security Agency’s Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)² established requirements for transitioning national security systems to quantum-resistant cryptography.² In June 2026, a further executive order set dated requirements for the first time. Federal agencies are to move their most sensitive systems to post-quantum encryption by the end of 2030 and to post-quantum authentication by the end of 2031. The order also directs federal acquisition rulemaking toward a 2030 requirement for covered contractors, which would reach suppliers selling into US public procurement wherever they are based.¹⁷ Across Europe, governments have adopted a similarly structured approach:

EUROPEAN UNION

The European Union Agency for Cybersecurity (ENISA) has published guidance supporting cryptographic inventory, risk assessment, crypto-agility, and migration planning, helping organizations prepare for the transition to post-quantum cryptography.⁵

UNITED KINGDOM

The United Kingdom’s National Cyber Security Centre (NCSC) has similarly encouraged organizations to begin preparation efforts, warning that post-quantum migration will require significant planning and coordination across complex technology environments.^{3–4}

Collectively, these initiatives reflect growing international consensus that post-quantum readiness is now a strategic cybersecurity priority.

2.3

Enterprise adoption is early but accelerating

Cloudflare has deployed the NIST-selected ML-KEM key agreement across its network and reports that more than 65% of human web traffic passing through it is already protected by post-quantum hybrid encryption. In 2026 it brought forward its own target for full post-quantum coverage to 2029 and identified authentication, rather than encryption, as the harder remaining problem.²⁶ Apple built its PQ3 protocol into iMessage²⁷, Signal added a post-quantum layer to its messaging protocol²⁸, and Amazon Web Services has offered post-quantum signing in its Key Management Service since 2025 and published a phased migration plan in 2026.²⁹

These providers supply the browsers, networks, cloud services and messaging platforms most other organizations are built on, so their migrations move the wider market before an enterprise has started its own program. Adoption beyond the large platform providers is uneven, and many organizations have yet to complete a cryptographic inventory or set a migration plan.

65%+

of human web traffic passing through Cloudflare’s network is already protected by post-quantum hybrid encryption

From planning into production

Cloudflare	ML-KEM key agreement deployed across its network
Apple	PQ3 protocol built into iMessage
Signal	Post-quantum layer added to its messaging protocol
AWS	Post-quantum signing in Key Management Service since 2025; phased migration plan in 2026

2.4

The UAE national post-quantum framework

The United Arab Emirates has established a national approach to post-quantum cryptography (PQC) that combines governance, technical standards, research, and implementation guidance to support an orderly transition to quantum-safe security. This framework provides public and private sector organizations with a structured approach for assessing cryptographic risk, planning migration, and maintaining long-term cryptographic agility.

1 Governance and national oversight

The UAE's national approach is led through the National Cryptography Center (NCC), operating under the UAE Cyber Security Council (CSC). The framework establishes national cryptographic policies, approved standards, and oversight mechanisms to support the country's transition to post-quantum cryptography while promoting consistent implementation across relevant entities.

2 A structured migration process

The framework defines a phased migration approach that guides organizations from initial preparation through to implementation and ongoing compliance. This includes identifying cryptographic dependencies, assessing risk, developing migration plans, validating implementations, and maintaining continuous cryptographic agility as standards continue to evolve.

3 Cryptographic discovery and asset classification

Migration begins with establishing visibility into cryptographic assets. Organizations are expected to identify where cryptography is used across applications, infrastructure, networks, cloud environments, certificates, keys, and protocols before classifying assets according to business criticality and quantum risk. This inventory provides the foundation for prioritizing migration activities.

4 Migration planning and approved cryptography

Organizations develop Migration Plan Proposals that define migration priorities, implementation timelines, and governance responsibilities. The framework also promotes the adoption of approved cryptographic algorithms and nationally recognized cryptographic libraries to support secure and interoperable implementations.

5 Testing, compliance, and continuous agility

Before deployment, implementations are expected to undergo appropriate testing and validation. The framework supports migration through testing, catalog inclusion, migration audits, and compliance assessment while encouraging organizations to build long-term cryptographic agility so future algorithm changes can be managed with minimal operational disruption.

2.5

The GCC post-quantum policy and initiative landscape

While this report’s survey findings focus on organizations in the United Arab Emirates, Saudi Arabia, and Qatar, post-quantum cryptography has become an emerging priority across the wider Gulf region. GCC countries have announced initiatives supporting quantum-safe cybersecurity through national strategies, regulatory frameworks, research and investment. These span post-quantum cryptography, which replaces vulnerable algorithms on existing systems, and quantum key distribution, which requires specialized hardware. Both are quantum-safe measures, but they address different problems. These developments provide important context for the regional readiness landscape and should be considered independently of the survey findings presented in this report.

Saudi Arabia

Saudi Arabia’s National Cybersecurity Authority has issued National Cryptographic Standards that set minimum cryptographic requirements for national entities and already address post-quantum cryptography.³⁰ A proposed update consulted on in late 2025 would add post-quantum algorithms and quantum key distribution to that framework.³¹ In 2026 the Communications, Space and Technology Commission began sector-level work with telecommunications operators on readiness for quantum-resistant cryptography.³² At the time of publication, no national deadline for economy-wide post-quantum migration had been identified.

Bahrain

Bahrain has moved into implementation. In December 2025 the National Cyber Security Centre launched a national cybersecurity modernization program extending across more than 60 government environments, covering identification and assessment of cryptographic assets, cryptographic governance and remediation in preparation for post-quantum security. It forms part of the National Cyber Security Strategy 2025 to 2028.³³ At the time of publication, no national completion date or Bahrain-specific approved algorithm profile had been identified.

Oman

Oman has identified quantum cybersecurity as an emerging investment area under its Hadatha 2026 to 2030 cybersecurity roadmap, and has published an investment opportunity to establish a Quantum Cybersecurity Center in Muscat focused on quantum key distribution.³⁷ The center is an investment opportunity rather than an operating facility. At the time of publication, no national post-quantum migration program had been identified.

Qatar

Qatar is building national quantum capability across research, investment, and communications. The Qatar Centre for Quantum Computing at Hamad Bin Khalifa University was established with government support.³⁴ A joint venture incorporated in Qatar in 2025 supports up to USD 1 billion of private-sector investment over ten years.³⁵ In May 2026 Ooredoo Qatar, the university and the Ministry of Defence established Qatar’s first operational quantum-safe communications link, using quantum key distribution rather than post-quantum cryptography.³⁶ At the time of publication, no national post-quantum migration program specific to Qatar had been identified.

Kuwait

Publicly visible quantum activity in Kuwait is primarily academic. At the time of publication, no publicly announced national post-quantum cryptography migration program, migration timetable or national quantum strategy had been identified. This observation is included for transparency and does not imply the absence of ongoing research, planning or internal government activity.

03

Survey Findings
and Analysis

Organizations across selected GCC markets recognize the quantum threat and are funding a response, with 84% planning or building a transition and 64% carrying a budget for it. Execution sits at an earlier stage, with 42% working to a defined roadmap and 35% having begun cryptographic discovery, held back by cost and complexity rather than doubt.

3.1 The threat is real, and it is close

3.2 Funding is in place ahead of delivery capacity

3.3 Reported visibility runs ahead of verified discovery

3.4 How enterprises track their cryptography today

3.5 What is holding the transition back

3.6 The vendor landscape is still forming, and delivery decisions are still open

3.7 Sovereignty has emerged as a key procurement consideration across the GCC

3.8 Enterprises are seeking practical implementation support

3.9 Every sector is at a similar early stage on discovery

3.10 What the findings mean for each audience

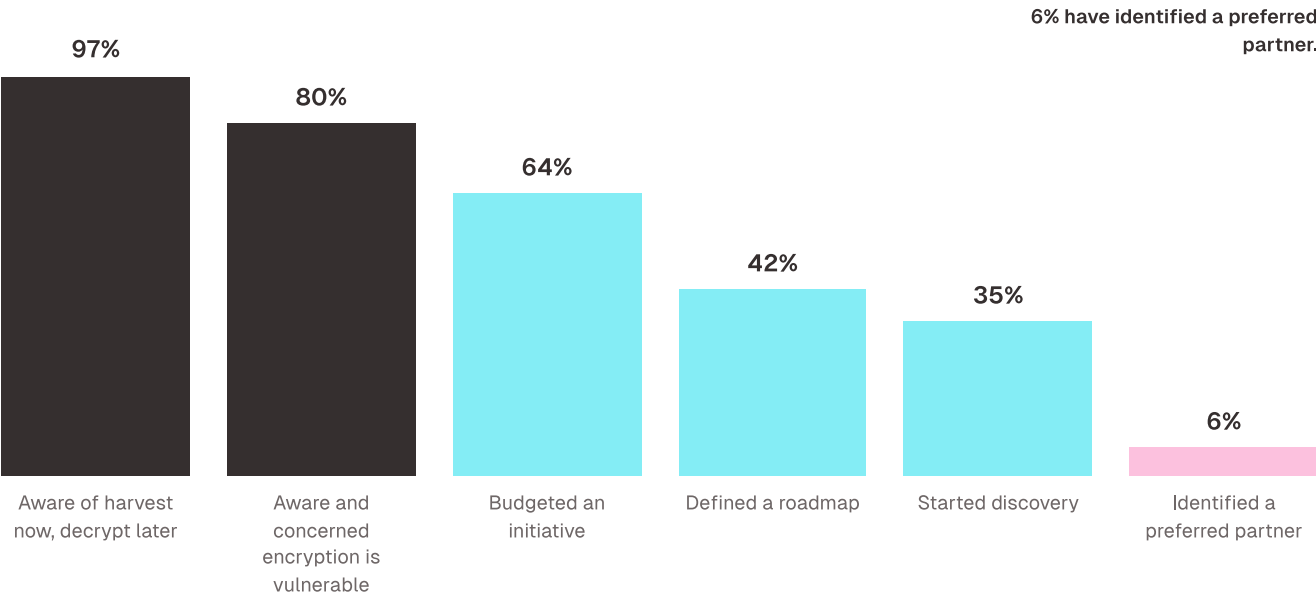
This chapter presents nine principal findings from the survey. Together, they show that surveyed organizations widely recognize the quantum threat and are beginning to allocate resources to address it. However, progress remains uneven. While awareness and investment are increasing, operational readiness, including cryptographic discovery, migration planning and vendor selection, is at an earlier stage.

EXHIBIT 5

% of respondents · n = 125

Recognition is broad. The operational steps are less far along.

Share of respondents reporting each measure. Each comes from a separate question.



Source: QuantumGate Post-Quantum Readiness Survey, 2026 (n=125). Each figure comes from a separate survey question. Respondents did not pass through these measures in sequence, and more than a third of those who have begun discovery do not yet have a defined roadmap.

Almost all respondents, 97%, recognize that data harvested today could be decrypted later. Only 6% have identified a preferred partner to help them prepare.

Three gaps define readiness across these markets. A visibility gap, because reported visibility runs ahead of verified discovery; a capability gap, because funding and plans are ahead of delivery capacity; and a delivery gap, because few organizations have settled how the migration will be delivered or by whom. The findings that follow trace each in turn.

3.1

The threat is real, and it is close

The survey suggests that, across selected GCC markets, debate over whether quantum computing represents a material cybersecurity risk has largely given way to discussion about implementation and preparedness. Four in five, 80%, are both aware and actively concerned that quantum computers will make current encryption vulnerable. Awareness of the harvest-now, decrypt-later threat is higher still at 97%. A majority, 58%, believe a cryptographically relevant quantum computer could break today's public-key cryptography within five years. Just over a quarter expect cryptographically relevant quantum computers to emerge within the next two years.

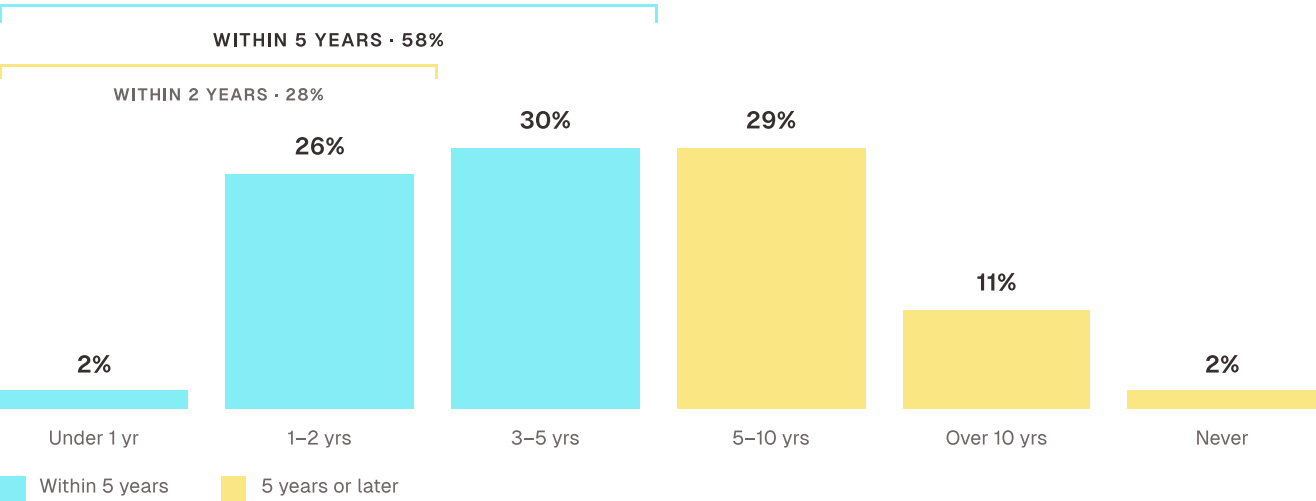
For a security leader the practical consequence is the shelf life of the data rather than the arrival date of the machine. Any data that must stay confidential beyond a few years is already exposed to collection today.

EXHIBIT 6

% of respondents · n = 125

58% of surveyed leaders believe a quantum computer could break today's public-key cryptography within five years

When do you expect a quantum machine capable of breaking today's cryptography?



Source: QuantumGate Post-Quantum Readiness Survey, 2026 (n=125).

3.2

Funding is in place ahead of delivery capacity

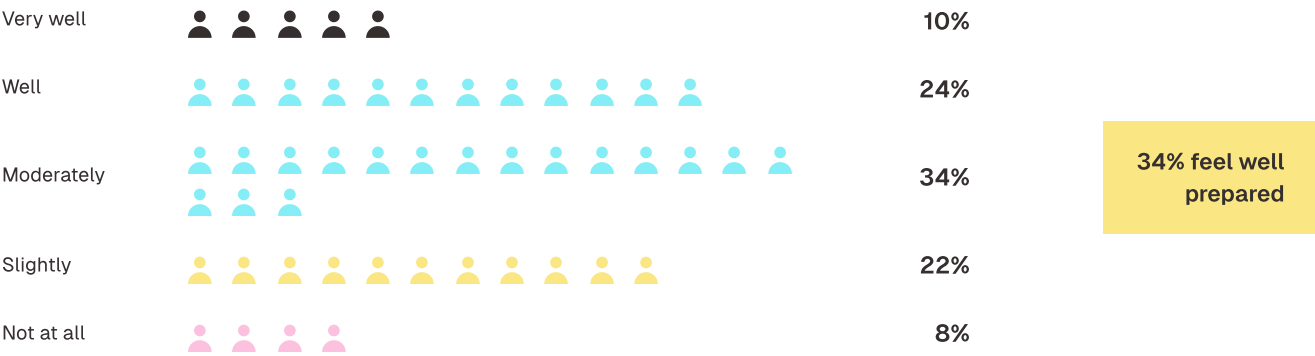
Conviction has translated into commitment. 84% are either planning or actively building a transition, with 42% working to a defined roadmap and 42% under way but yet to define one. 15% have not started and 1% were unable to say. Funding is following: 64% report a budgeted initiative, and of those without one (n=43), most, 58%, intend to budget in the coming years.

Confidence and capability, though, have not kept pace. 34% rate themselves well or very well prepared, roughly two-thirds place themselves at moderate or below, and most migration timelines run three to five years or longer, which puts a premium on starting early. Organizations are willing to fund the work; fewer have converted that funding into operational capability.

EXHIBIT 7 % of respondents · n = 125

About a third of enterprises already feel well prepared

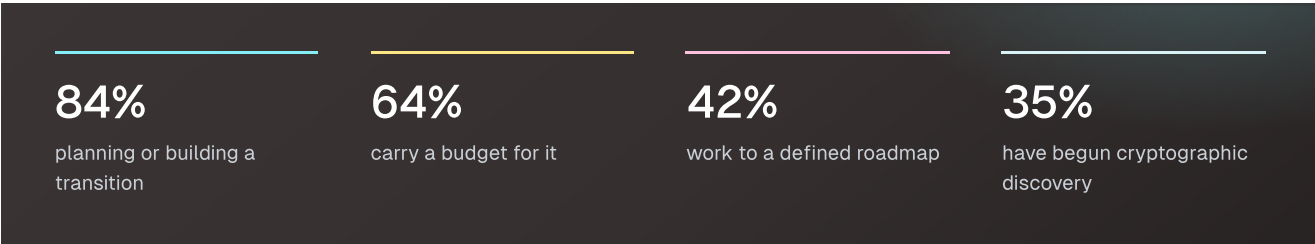
Self-assessed preparedness for the post-quantum transition; each icon represents about 2% of respondents.



Figures rounded; 1% answered don't know.
Source: QuantumGate Post-Quantum Readiness Survey, 2026 (n=125).

EXHIBIT 8

The readiness gap, by the numbers



Source: QuantumGate Post-Quantum Readiness Survey, 2026 (n=125).

3.3

Reported visibility runs ahead of verified discovery

Cryptographic visibility is where self-assessment and practice diverge most. Two-thirds (66%) say they have visibility into all cryptographic keys, certificates, algorithms, and protocols currently in use, and 30% say they do not. But visibility in that general sense is not the same as discovery: the systematic inventory that locates quantum-vulnerable algorithms across an estate. 35% have conducted or initiated that discovery, the essential first step of any migration, while 54% plan to but have not started.

Read together, the two answers suggest confidence outpaces verification. Among the organizations reporting full visibility (n=83), 41% have conducted or initiated a cryptographic inventory. The two questions measure different things: general visibility of cryptographic assets, and a specific assessment of which algorithms are quantum-vulnerable. The gap between them suggests the first is more common than the second.

Organizations cannot plan a migration until they know where vulnerable cryptography resides.¹ On this evidence, cryptographic discovery is the principal operational bottleneck to post-quantum readiness. Without it, most organizations cannot reliably estimate the size, cost, or duration of a migration program.

3.4

How enterprises track their cryptography today

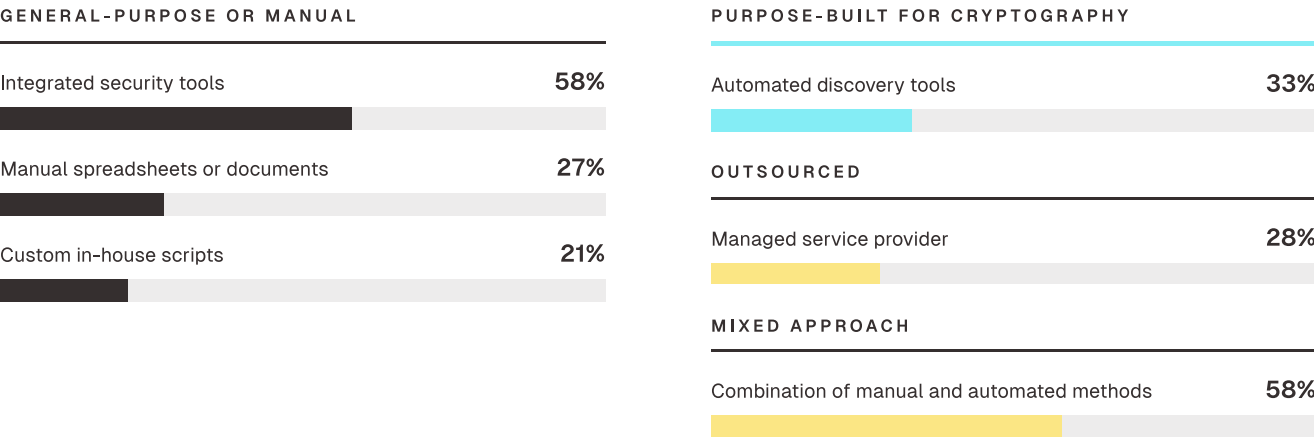
Finding cryptography once is not enough. To plan and run a migration, an organization has to keep an accurate, current picture of its cryptography as it changes over time. The survey shows most are not yet equipped to do that.

The tools in use are mostly general-purpose or manual. Integrated security tools are the most common single method at 58%, and the same share describe using a combination of manual and automated methods. Only a third, 33%, use software built specifically to discover cryptography automatically. Many still rely on methods that capture only a snapshot: 27% track their cryptography in spreadsheets or documents, and 21% use custom in-house scripts. A further 28% rely on a managed service provider, and just 2% have no formal process at all. Organizations use more than one method, so these figures add to more than 100%.

EXHIBIT 9

% of respondents · n = 125

76% track cryptography with general-purpose or manual tools



Respondents could select more than one method, averaging 2.3 each, so figures sum to more than 100%. Only 2% have no formal process. Three quarters, 76%, use at least one of the three general or manual methods listed above; the combined-approach option is shown separately and is not counted in that figure. Integrated security tools such as SIEM and EDR give partial visibility only. Only 6% use purpose-built discovery without a general or manual method. Source: QuantumGate Post-Quantum Readiness Survey, 2026 (n=125).

This matters because cryptography does not stand still. Certificates expire and are reissued, keys rotate, and new services appear across applications, devices, networks, and cloud environments all the time. A spreadsheet or a script records a single moment, so in a large, changing estate it is out of date almost as soon as it is finished, and it cannot reliably find the quantum-vulnerable algorithms a migration has to fix first.

Reviews are also infrequent. Only 27% audit their cryptography on a fixed schedule. 44% review it only from time to time, with no set cadence, 22% only when they are already rebuilding a major system, and 6% rarely or never. Two things follow from this. Most organizations have not started discovery, and the methods many would start with record a single moment rather than a changing estate. An inventory that is accurate on the day it is finished can be out of date within weeks.

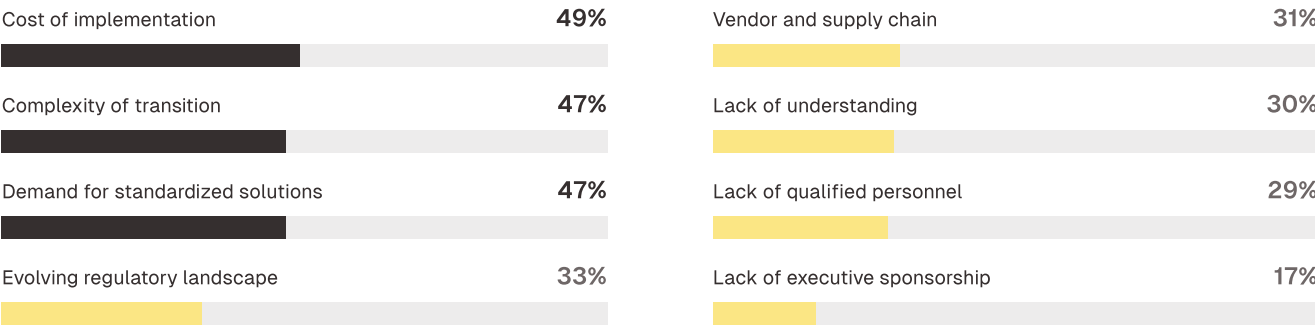
3.5

What is holding the transition back

EXHIBIT 10

% naming each a top-three barrier · n = 125

Cost and complexity are what hold the transition back



Respondents could select more than one option, so figures sum to more than 100%.
The underlying algorithms were standardized in 2024; the gap cited relates to production-ready products, integration and implementation guidance.
Source: QuantumGate Post-Quantum Readiness Survey, 2026 (n=125).

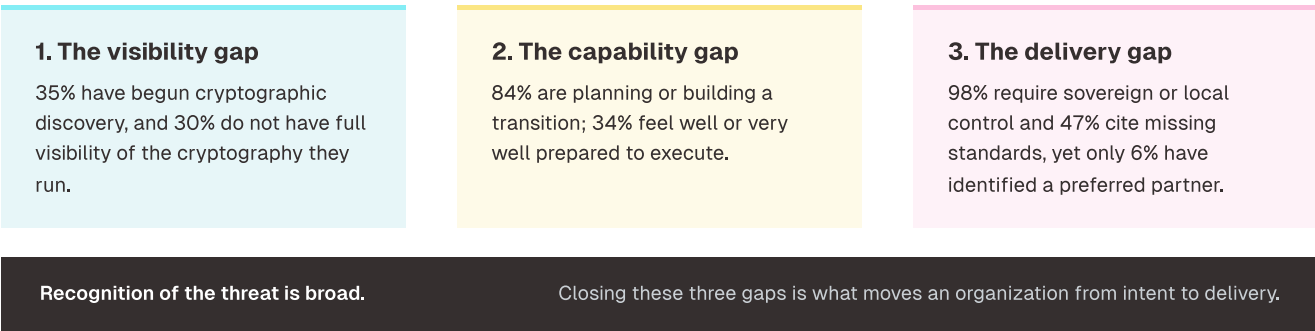
What holds enterprises back is execution and economics. Three barriers cluster at the top and sit within two points of each other: cost of implementation at 49%, complexity of the transition and demand for standardized solutions at 47% each. Cost is also the barrier most often named first, by 24%. The evolving regulatory landscape, supply-chain dependencies, weak awareness, and a shortage of qualified personnel cluster in the middle, while lack of executive sponsorship sits at the bottom of the list, named a top-three barrier by 17%. The leading barriers are all practical. None of them is doubt about whether the threat is real.

Regulatory direction in the region is advancing, and demand for more of it is high: 37% of respondents name regulatory guidance and mandates among the support they most want, among the four most-requested forms of support. National programs are phased by design, bringing sectors and entities into scope in stages, so organizations ahead of their own designation are looking for help translating national direction into requirements, timelines, and controls for their estate.

One finding warrants particular attention for vendors and regulators: standardized solutions are cited as a leading barrier even though the underlying algorithms were standardized in 2024. The gap enterprises feel is not in the cryptography itself but in ready-to-deploy products, tooling, and guidance built on it. The results suggest organizations are looking past awareness campaigns toward practical implementation support: standardized tooling, migration frameworks, and operational guidance.

EXHIBIT 11

Three gaps separate awareness from quantum-safe operations



Source: QuantumGate Post-Quantum Readiness Survey, 2026 (n=125).

3.6

The vendor landscape is still forming, and delivery decisions are still open

The survey also provides insight into the current maturity of the regional post-quantum vendor landscape. A clear majority, 58%, are actively evaluating multiple PQC vendors, 35% have not identified one at all, and 6% have identified a preferred partner. The remainder were unable to say. These findings indicate that many organizations have begun evaluating the market but have not yet committed to a preferred implementation partner.

Vendor selection is likely to become increasingly important over the next several years as organizations progress from planning to implementation. Once migration programs are underway, enterprises may be less inclined to change providers because of the complexity of integrating cryptographic discovery, key management and migration processes into existing security architectures. Most enterprises are still evaluating, so the decisions taken over the next two years will shape migration programs for years afterward.

Partner selection is not the same as readiness. Some organizations will deliver the migration internally, and others will use a hybrid model with external support for specific stages such as cryptographic discovery or key management. Each organization should define which route it will take, internally, through an external partner, or as a hybrid, and assign clear roles and responsibilities against it. That decision shapes the skills, budget, and governance a program needs, so it is worth settling early.



3.7

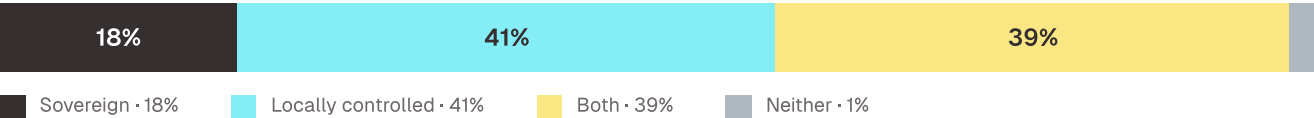
Sovereignty has emerged as a key procurement consideration across the GCC

Almost every organization, 98%, requires cryptographic solutions that are nationally governed, locally controlled, or both. Local control such as customer-managed keys or on-premises operation is required by 80%, sovereign solutions specifically by 58%, and only 1% require neither. On these findings, sovereign or local control functions as a procurement condition in these markets rather than a point of differentiation between suppliers.

EXHIBIT 12

% of respondents · n = 125

98% Sovereignty is a baseline procurement requirement
98% of enterprises require sovereign or locally controlled cryptography



Categories are exclusive. In total, 58% require sovereign control and 80% require local control, in each case combining the single-requirement group with the group requiring both. Components are rounded, so they do not always sum exactly. 1% answered don't know.

Source: QuantumGate Post-Quantum Readiness Survey, 2026 (n=125).

3.8

Enterprises are seeking practical implementation support

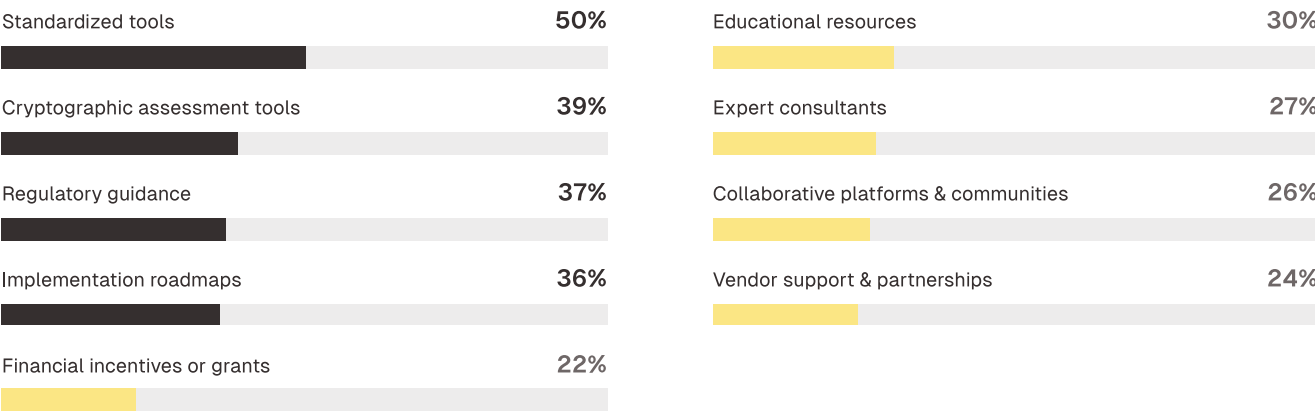
Asked which forms of support would most effectively accelerate post-quantum readiness, respondents selected across the full range of options. Standardized tools and software lead at 50%, followed by cryptographic assessment tools (39%), regulatory guidance and mandates (37%), and practical implementation guides and roadmaps (36%). Educational resources and training (30%), access to expert consultants (27%), collaborative platforms and communities (26%), vendor support and partnerships (24%), and financial incentives or grants (22%) follow.

EXHIBIT 13

% of respondents • n = 125

Enterprises are seeking practical implementation support

Most-requested support for a quantum-safe transition



Respondents could select more than one option, so figures sum to more than 100%.
Source: QuantumGate Post-Quantum Readiness Survey, 2026 (n=125).

The gaps between neighboring options are within the range that sampling variation at this base size would produce, so the list suggests a set of parallel needs rather than a strict order of priority. The pattern points to a migration that organizations expect to run across technology, governance, and skills at once.

Organizations are looking for tooling and assessment capability, national direction they can plan against, step-by-step guidance, and the training and external expertise to carry it out.

3.9

Every sector is at a similar early stage on discovery

Readiness is not uniform across sectors. Exhibit 14 sets four measures side by side for the sectors with enough respondents to report separately: awareness of the threat, cryptographic discovery, migration roadmaps, and self-assessed preparedness. These are sub-samples of the total, so the figures indicate direction rather than precise levels, and close differences should not be read as rankings.

EXHIBIT 14

% of sector sub-sample

Discovery sits below half in every sector reported

Four measures across the sectors with enough respondents to report separately

	AWARE AND CONCERNED	DISCOVERY	ROADMAP	PREPARED
Financial	89%	38%	46%	32%
Telecom	83%	44%	44%	22%
Energy	80%	28%	32%	40%
Healthcare	70%	25%	30%	25%

Cyan and dark = more ready, yellow and pink = less. Sector figures are based on sub-samples and are indicative. Sectors with too few respondents to report separately are not shown.
Source: QuantumGate Post-Quantum Readiness Survey, 2026 (n=125).

Awareness is high across all four sectors, from 70% to 89%. Discovery is not, ranging from 25% to 44%. The two measures do not move together. Energy reports the highest share feeling well prepared, at 40%, alongside one of the lower rates of discovery at 28%. Telecommunications reports the reverse. Self-assessed preparedness is not tracking the work that underpins it, and that pattern holds across the sample rather than distinguishing any one sector.

What stands out is not the spread between sectors but the level they share. Discovery sits below 50% in every sector shown. On this evidence no sector in the sample has completed the first step of a migration at scale, which makes the shared position more instructive than the differences.

3.10

What the findings mean for each audience

The survey points to different priorities for the main groups it concerns.

For CISOs and security leaders

Begin with cryptographic discovery: an inventory of where cryptography is used and what depends on it. Migration cannot be planned or sequenced until that is known. Because harvest-now, decrypt-later threatens confidentiality, give first priority to data with long confidentiality lifetimes and to systems whose secrecy relies on quantum-vulnerable public-key cryptography, such as TLS, VPNs, and encrypted archives that use RSA or ECC for key exchange. Migrating key establishment to the standardized post-quantum algorithm ML-KEM, typically deployed in a hybrid mode alongside existing cryptography, addresses that exposure first. Signature and authentication migration must still be assessed according to the lifetime and security role of each credential, certificate, code-signing key, and root of trust. Prioritize by the shelf life of the data, not the age of the system. Move cryptographic auditing from event-driven to scheduled. Build crypto-agility so the next algorithm change is a configuration change and not a rebuild.

For boards and investors

Funded demand alongside limited capability is both a risk and an opportunity. Roughly two-thirds of surveyed enterprises have a budget for post-quantum work, yet only one in three feels well prepared and 6% have identified a preferred partner. The funding is committed; the delivery capacity is not yet built.

For policymakers and regulators

Organizations are actively looking for standards, guidance, and mandates to help them move forward. A lack of standardized solutions is cited as a leading barrier even though the core algorithms were standardized by NIST in 2024, which suggests the opportunity now lies in supporting production-ready products, protocol integration, and implementation guidance built on those standards. Organizations report cost and implementation complexity as their main challenges, and 98% require sovereign or local control. What they are asking for is regulatory guidance, implementation frameworks and nationally aligned migration programs, building on the work already underway across the region.

04

Strategic Insights

Enterprises in these markets do not need to be persuaded that the quantum threat is real. They need a sequenced, affordable path from awareness to action. Six recommendations, in the order to take them.

- | | | | |
|---|--|---|---|
| 1 | Start with cryptographic discovery and inventory | 4 | Build crypto-agility for the next transition |
| 2 | Turn discovery into continuous visibility | 5 | Attack cost and complexity with standards |
| 3 | Plan and migrate in phases | 6 | Convert conviction into sponsorship and mandate |

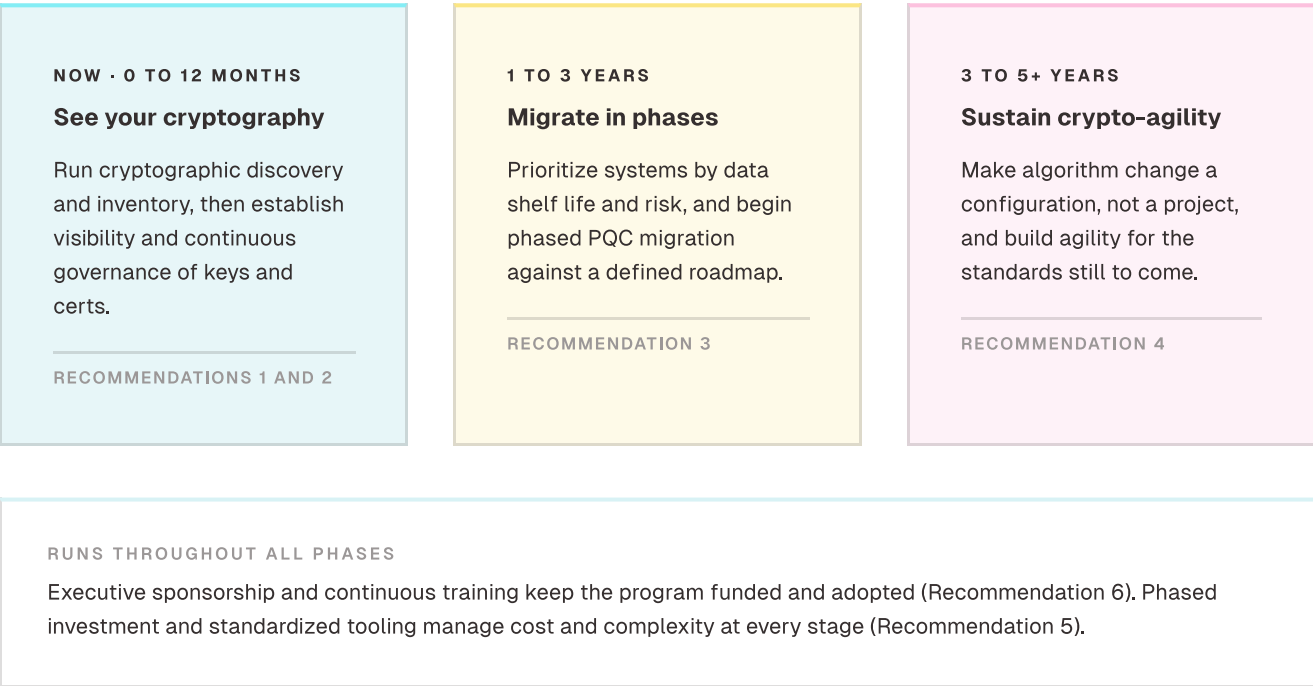
Strategic insights

The survey findings highlight several priorities for organizations preparing for the transition to post-quantum cryptography. The next phase of readiness rests on three capabilities rather than on further recognition of the need: seeing what an estate actually runs, planning from that evidence rather than from assumption, and building systems in which an algorithm change is a configuration change.

The six recommendations below respond to the three gaps set out in section 3. They are deliberately ordered, because each depends on the one before it. Discovery has to come before planning, and planning before migration.

EXHIBIT 15

A phased path from visibility to durable crypto-agility



1 **Start where the gap is widest: cryptographic discovery and inventory.**

Cryptographic discovery forms the foundation of every successful migration program, and it is also the least-completed step in the survey: only 35% of enterprises have begun it. Before an organization can plan a migration, set a budget, or choose a vendor, it has to know which keys, certificates, algorithms, and protocols it runs, where they live, and what data they protect. The first ninety days should produce an authoritative cryptographic inventory rather than additional awareness activities.

2 **Turn one-time discovery into continuous visibility and governance.**

A one-time inventory becomes outdated almost immediately in dynamic enterprise environments. Two-thirds of enterprises report full visibility today, but only 27% audit their cryptography on a fixed schedule, and 22% look only when a major system is already being rebuilt. The recommendation is to move cryptographic oversight from event-driven to continuous, with clear ownership, so that the inventory stays current and drift is caught early. Point-in-time inventories and continuous oversight are different capabilities, and only the second keeps pace with a changing estate.

3 **Plan and migrate in phases, sequenced by risk and data shelf life.**

The data shows 84% of enterprises planning or building a transition but only 10% feeling very well prepared, which means intent has run ahead of execution. The way to close that gap is a phased migration that starts with the highest-risk, longest-confidentiality systems. Under harvest now, decrypt later, any data that must stay secret beyond a few years is the priority, irrespective of when cryptographically relevant quantum computers become available. Key establishment for that data is the first candidate, typically deployed alongside existing cryptography rather than replacing it outright.

4 **Design for the next transition, not just this one: build crypto-agility.**

Among respondents who gave a timeline, most expect migration to run three to five years or longer, and the cryptographic standards themselves will keep evolving. Organizations that embed a single algorithm will face the same disruption again at the next change. Building crypto-agility, the ability to swap algorithms through configuration rather than re-engineering, reduces the scale of future transitions and protects the investment being made now.¹

5 **Attack cost and complexity with phasing, standardized tooling and approved local cryptography.**

Cost at 49%, complexity at 47% and the absence of standardized solutions at 47% cluster at the top of the barrier list. Phased implementation is how the first two are managed. Phased investment spreads cost across budget cycles and ties spend to risk reduction, while standardized, NIST-aligned tooling avoids bespoke builds and reduces the integration burden that drives complexity. Nationally approved algorithm profiles and validated local cryptographic libraries work the same way, giving organizations an implementation to build on rather than one to develop and assess for themselves. Because 98% of respondents already require sovereign or locally controlled cryptography, selecting tooling that meets those requirements at the outset avoids migrating a second time for compliance reasons. The notable point is that the cryptography is now standardized; the remaining work is operational, which is precisely where standardized tooling pays off.¹

6 **Convert executive conviction into sponsorship, training, and mandate.**

Lack of executive sponsorship was named least often of the barriers tested, by 17%, and 80% of respondents are themselves concerned about the threat. Concern is therefore not the constraint. What converts it into progress is a funded mandate, a named owner and the in-house skills to execute. Multi-year programs need that structure to survive budget cycles and leadership changes.

Conclusion

Across these markets the case for acting is made, the funding is committed, and national frameworks are taking shape. What remains is operational, and it is more tractable than it looks.

The conditions for migration now exist. The core algorithms were finalized in 2024 and can be deployed today. National cryptographic authorities across the region are defining the standards and migration requirements that designated entities will work to. Migration deadlines in major jurisdictions now carry dates and organizations in these markets are therefore planning against a known schedule.

Enterprises in key GCC markets have already made the harder commitments. 64% carry a budget for post-quantum work and four in ten have a defined roadmap. Lack of executive sponsorship is the least-cited barrier of those tested, at 17%, and 80% of respondents are themselves concerned about the threat. The argument that usually takes longest inside an organization has largely been won.

What remains is a single operational step. Cryptographic discovery is what converts commitment into a plan: an inventory of which keys, certificates and algorithms an organization runs and what they protect. A third of enterprises have already begun it, and it is the step that makes a migration possible to size, sequence and contract for.

The starting position is stronger than it first appears. Two-thirds of organizations report full visibility of their cryptography, and among them 41% have carried out a discovery exercise. General visibility and a verified, quantum-specific inventory are different things, so for many organizations the work ahead is confirming and extending what they already have rather than building it from nothing.

Two decisions taken in this window will shape the programs that follow. Most enterprises, 58%, are still choosing a delivery route, and that choice sets the skills, budget and governance a program will need. 98% require cryptographic solutions that are nationally governed, locally controlled, or both, making national or local control a standing procurement requirement across these markets.

By 2028, the earliest of the published international migration milestones, a prepared organization will be able to show four things: a cryptographic inventory that stays current, a migration roadmap sequenced by the shelf life of the data, a defined delivery model with named ownership, and cryptographic auditing on a regular cycle. None of these depend on when a capable quantum computer arrives. Each takes time to build, and each fits inside existing budget cycles.

The transition has begun, and these markets enter it with the standards published, national frameworks taking shape and enterprise funding already committed. The next two years turn that position into deployed capability.

The organizations behind this report

The transition to post-quantum security will require coordinated action across policy, standards, research, and enterprise implementation. This report was developed through the collaboration of organizations contributing to these different areas of the UAE's post-quantum ecosystem.



UAE Cyber Security Council

The UAE Cyber Security Council is the national authority responsible for strengthening the country's cybersecurity resilience. It develops national cybersecurity strategy and policy, coordinates cyber resilience efforts across government and critical sectors, and works with public and private organizations to help protect the UAE's digital infrastructure.

csc.gov.ae/en



National Cryptography Center

The National Cryptography Center (NCC) is responsible for defining the UAE's national cryptographic standards and migration requirements. As part of the National Post-Quantum Migration Program, it provides a common national reference for approved cryptographic algorithms, cryptographic discovery and assessment, and post-quantum migration guidance for designated entities.

uaencc.gov.ae/en



Technology Innovation Institute

The Technology Innovation Institute (TII) is the applied research arm of Abu Dhabi's Advanced Technology Research Council (ATRC). Its cryptography researchers have contributed to the NIST post-quantum cryptography standardization process, including work on HQC and additional digital signature candidates, while advancing sovereign post-quantum cryptographic research and technologies.

tii.ae



QuantumGate

QuantumGate is a UAE-based post-quantum cybersecurity company focused on helping organizations prepare for the transition to quantum-safe cryptography. Its capabilities support cryptographic discovery and visibility, migration planning, crypto-agility, and sovereign deployment, enabling organizations to strengthen post-quantum readiness while maintaining control of their cryptographic infrastructure and sensitive data.

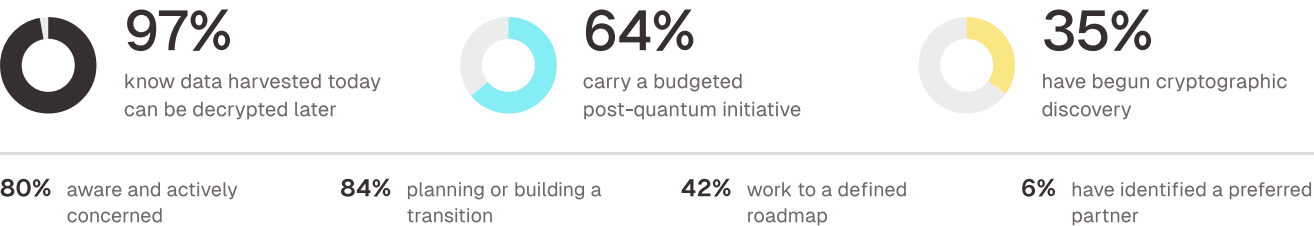
quantumgate.ae

Together, these organizations contribute complementary capabilities that support different aspects of the transition to post-quantum security, from national strategy and cryptographic standards to applied research and enterprise implementation. Through continued collaboration, they are helping strengthen cyber resilience and advance post-quantum readiness across the UAE and the wider GCC.

Recognition is broad. Discovery is the bottleneck.

01 THE READINESS LADDER

% OF RESPONDENTS · N = 125



Each figure is a separate survey question, not a stage respondents passed through in sequence.

02 TWO GAPS SEPARATE INTENT FROM EXECUTION

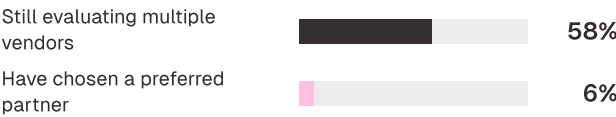
INTENT · THEN REALITY

THE CAPABILITY GAP



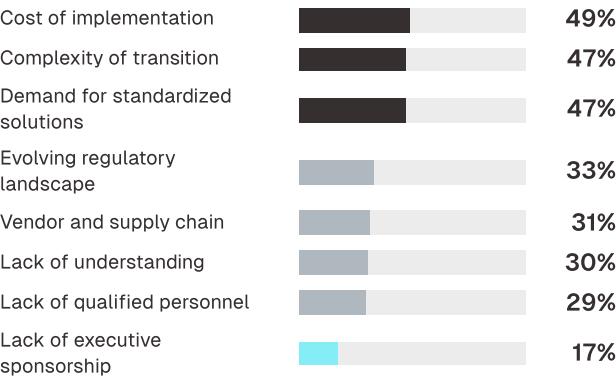
The money is committed — 64% carry a budget. The delivery capacity is not yet built.

THE DELIVERY GAP



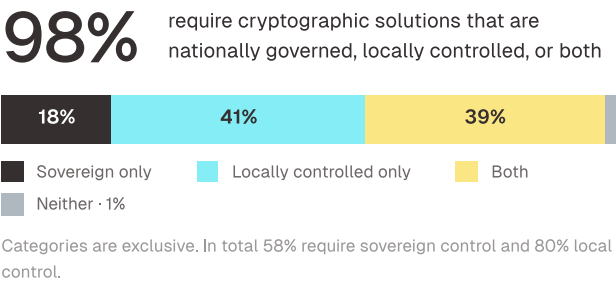
A further 35% have identified no vendor at all. In-house, partner or hybrid is still undecided.

03 WHAT HOLDS THE TRANSITION BACK



Top-three barriers, more than one selection allowed. Every leading barrier is practical.

04 SOVEREIGNTY IS A BASELINE REQUIREMENT



05 THE PATH FORWARD, IN ORDER

EACH STEP DEPENDS ON THE ONE BEFORE IT

NOW · 0 TO 12 MONTHS

See your cryptography

Run discovery and inventory, then hold it as continuous visibility. Only 27% audit on a fixed schedule today.

1 TO 3 YEARS

Migrate in phases

Sequence by data shelf life. Key establishment for long-lived data first, in hybrid mode.

3 TO 5+ YEARS

Sustain crypto-agility

Make the next algorithm change a configuration change, with a funded mandate and a named owner.

06 THE DATES ARE ALREADY SET

58% EXPECT A CAPABLE MACHINE WITHIN FIVE YEARS

2028

UK: discovery and planning complete

2029

Cloudflare targets full PQ coverage

2030

US federal encryption; EU high-risk systems

2031

US federal authentication; UK priority services

2035

NIST draft guidance disallows classical public-key

Source: QuantumGate Post-Quantum Readiness Survey, 2026 (n=125). Self-reported; rounded to the nearest whole percentage.

Glossary of terms

Algorithm names follow the finalized NIST designations, not their submission names. Where a submission name is still in common use (Kyber for ML-KEM, Dilithium for ML-DSA, SPHINCS+ for SLH-DSA), this report uses the standardized name throughout.

Crypto-agility (cryptographic agility)

The ability to replace or adapt cryptographic algorithms, keys, certificates and protocols without interrupting operations.

Cryptographic asset

Any algorithm, key, certificate, protocol, application, device, or system that uses cryptography.

Cryptographic discovery

A systematic inventory of where cryptography is used across an estate and which algorithms are quantum-vulnerable. Distinct from general visibility.

Cryptographic sovereignty

Covers two requirements the survey asked about separately: national governance of cryptography, and local control such as customer-managed keys or on-premises operation.

CRQC

Cryptographically relevant quantum computer: one capable of breaking the public-key cryptography in general use today.

Data shelf life

The period for which information must remain confidential. The primary variable for sequencing a migration.

ECC

Elliptic-curve cryptography. Public-key algorithms resting on the elliptic-curve discrete logarithm problem. Vulnerable to Shor’s algorithm.

Grover’s algorithm

A 1996 quantum algorithm that speeds up brute-force search, roughly halving the effective strength of a symmetric key.

Harvest now, decrypt later

Collecting encrypted data today in order to decrypt it once a capable quantum computer exists.

Hybrid mode

A post-quantum algorithm deployed alongside a classical one, so security holds if either remains unbroken.

Key establishment

How two parties agree a shared secret key over an untrusted channel. The first priority where data must stay confidential for years.

Logical qubit

An error-corrected qubit assembled from many physical qubits. Roadmaps are quoted in logical qubits, attack costs in physical ones.

ML-DSA (FIPS 204)

Module-Lattice-Based Digital Signature Algorithm. A NIST-standardized post-quantum signature scheme.

ML-KEM (FIPS 203)

Module-Lattice-Based Key-Encapsulation Mechanism. The first NIST-standardized algorithm for key establishment.

Post-quantum cryptography (PQC)

Algorithms designed to resist attacks from both classical and quantum computers, running on conventional hardware.

Public-key cryptography

Algorithms using a paired public and private key. Enables key agreement and signatures without a shared secret.

Quantum key distribution (QKD)

Key exchange using quantum physics and dedicated hardware. Distinct from post-quantum cryptography, which runs on conventional systems.

RSA

A public-key algorithm whose security rests on the difficulty of factoring large integers. Vulnerable to Shor’s algorithm.

Shor’s algorithm

A 1994 quantum algorithm that solves integer factorization and discrete logarithms efficiently, breaking RSA and ECC on a capable machine.

SLH-DSA (FIPS 205)

Stateless Hash-Based Digital Signature Algorithm. A NIST-standardized scheme built on hash functions rather than lattices.

Symmetric cryptography

Algorithms such as AES, together with hash functions. Weakened by Grover’s algorithm but not broken; AES-256 remains sufficient.

References

1	NIST (2024) <i>Post-Quantum Cryptography Standardization Project</i> . csrc.nist.gov	20	NIST (2024) <i>FIPS 205: Stateless Hash-Based Digital Signature Standard</i> . csrc.nist.gov
2	National Security Agency (2022) <i>Commercial National Security Algorithm Suite 2.0</i> . nsa.gov	21	NIST (2025) <i>IR 8545: Status Report on the Fourth Round of the Post-Quantum Cryptography Standardization Process</i> . csrc.nist.gov
3	National Cyber Security Centre (2020) <i>Preparing for Quantum-Safe Cryptography</i> . ncsc.gov.uk	22	NIST (2026) <i>IR 8610: Status Report on the Second Round of the Additional Digital Signature Schemes</i> . csrc.nist.gov
4	National Cyber Security Centre (2025) <i>Timelines for Migration to Post-Quantum Cryptography</i> . ncsc.gov.uk	23	NIST (2024) <i>IR 8547: Transition to Post-Quantum Cryptography Standards, Initial Public Draft</i> . csrc.nist.gov
5	ENISA (2021) <i>Post-Quantum Cryptography: Current State and Quantum Mitigation</i> . enisa.europa.eu	24	NIST (2026) <i>Post-Quantum Cryptography Updates to the Personal Identity Verification Standards: SP 800-73 and SP 800-78 working drafts</i> . csrc.nist.gov
6	Shor, P. W. (1994) 'Algorithms for Quantum Computation: Discrete Logarithms and Factoring', <i>Proceedings of the 35th Annual Symposium on Foundations of Computer Science</i> , pp. 124–134.	25	The White House (2022) <i>National Security Memorandum 10: Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems</i> . whitehouse.gov
7	IBM (2025) <i>IBM Quantum Roadmap: Large-Scale Fault-Tolerant Quantum Computing</i> . ibm.com/quantum	26	Cloudflare (2026) <i>Cloudflare Targets 2029 for Full Post-Quantum Security</i> . blog.cloudflare.com
8	Quantinuum (2025) <i>Accelerated Hardware Roadmap</i> . quantinuum.com	27	Apple (2024) <i>iMessage with PQ3: A New State of the Art in Quantum-Secure Messaging</i> . security.apple.com
9	Microsoft (2026) <i>Microsoft Quantum Roadmap</i> . quantum.microsoft.com	28	Signal (2023) <i>The PQXDH Key Agreement Protocol</i> . signal.org
10	IonQ (2025) <i>Technical Roadmap</i> . ionq.com/roadmap	29	Amazon Web Services (2024, updated 2026) <i>AWS post-quantum cryptography migration plan</i> . aws.amazon.com
11	Google Quantum AI (2025) <i>Our Quantum Computing Roadmap</i> . quantumai.google	30	National Cybersecurity Authority (2020) <i>National Cryptographic Standards</i> . nca.gov.sa
12	Gidney, C. (2025) <i>How to Factor 2048 Bit RSA Integers with Less Than a Million Noisy Qubits</i> . arXiv:2505.15917	31	National Cybersecurity Authority (2025) <i>National Cryptographic Standards NCS-2, public consultation</i> . nca.gov.sa
13	Global Risk Institute and evolutionQ (2026) <i>Quantum Threat Timeline Report 2025</i> . globalriskinstitute.org	32	Communications, Space and Technology Commission (2026) <i>Sector Readiness for the Transition to Quantum-Resistant Cryptography</i> . cst.gov.sa
14	UAE Cyber Security Council (2026) <i>National Post-Quantum Migration Program</i> . csc.gov.ae	33	National Cyber Security Centre (2025) <i>National Cybersecurity Modernization Program</i> . ncsc.gov.bh
15	National Cryptography Center (2026) <i>National Cryptographic Standards and Migration Requirements</i> . uaencc.gov.ae	34	Hamad Bin Khalifa University (2026) <i>Qatar Centre for Quantum Computing</i> . hbku.edu.qa
16	European Commission (2025) <i>Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography</i> . digital-strategy.ec.europa.eu	35	Quantinuum and Al Rabban Capital (2025) <i>Joint Venture to Advance Quantum Technologies in Qatar</i> . quantinuum.com
17	The White House (2026) <i>Executive Order: Securing the Nation Against Advanced Cryptographic Attacks, June 22</i> . whitehouse.gov	36	Ooredoo Qatar (2026) <i>Qatar's First Quantum-Safe Communications Link</i> . ooredoo.qa
18	NIST (2024) <i>FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard</i> . csrc.nist.gov	37	Ministry of Transport, Communications and Information Technology (2026) <i>Quantum Cybersecurity Center Investment Opportunity</i> . mtcit.gov.om
19	NIST (2024) <i>FIPS 204: Module-Lattice-Based Digital Signature Standard</i> . csrc.nist.gov	38	Mosca, M. (2015) 'Cybersecurity in an Era with Quantum Computers: Will We Be Ready?', <i>IACR Cryptology ePrint Archive</i> , Report 2015/1075. eprint.iacr.org



The State of Post-Quantum Readiness in Key GCC Markets

Research Report • September 2026

Supported by

