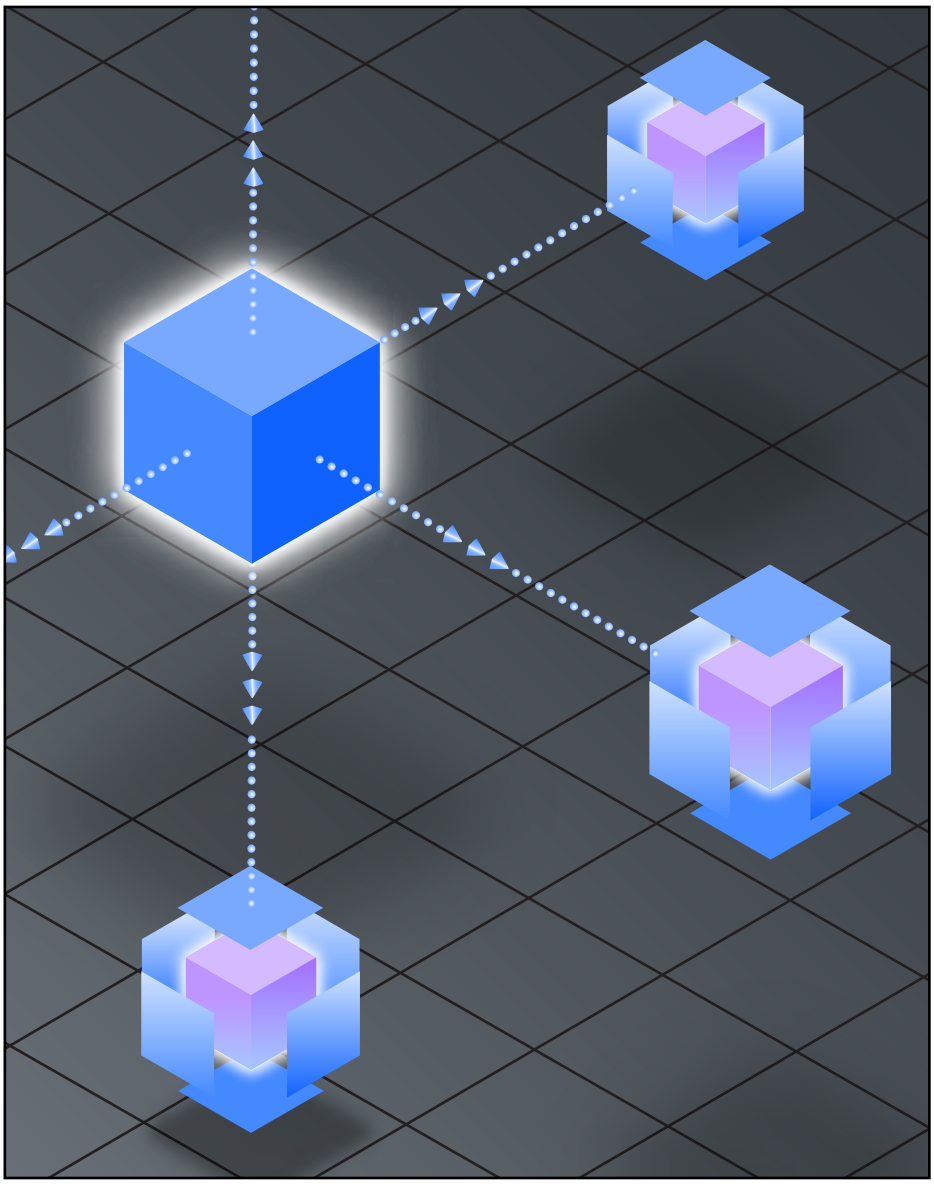


Secure the post-quantum future

How quantum safety strengthens cyber resilience for today and tomorrow

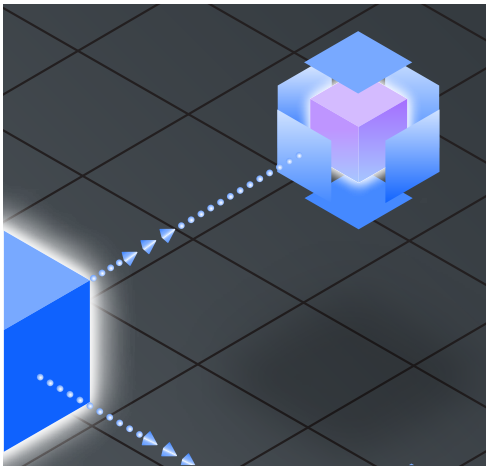
CSA cloud security alliance®

IBM

How IBM can help

IBM Quantum Safe™ delivers the technology, strategic guidance, and services required to enable end-to-end quantum-safe transformation. By combining advisory, system integration, and operational services, we help organizations build lasting cryptographic agility and resilience. For more information visit https://www.ibm.com/services/quantum-safe

Contents



Key takeaways

Quantum computing will fundamentally transform data security, forcing businesses to reimagine their entire approach to protecting systems and information.

73% of organizations report that business and technology leaders are working closely on their quantum-safe strategy.

But only 19% of organizations have near-term maturity goals for their quantum-safe initiatives.

The gap between awareness and action is hampering quantum-safe transformation efforts—as is a scarcity of required skills.

Still, readiness scores are higher overall than in 2023.

The perspective that quantum safety is a technology challenge and one that can be outsourced can lead to a dangerous oversight in terms of organizational preparedness.

62% of respondents believe vendors will handle quantum-safe transition requirements, while 56% continue to view quantum safety as purely a technical issue.

The quantum-safe landscape shows a paradox: organizations facing similar risks vary in preparedness, while equally responsive organizations face different challenges.

This highlights the need for tailored strategies that align organizational risk with response capacity.

Foreword

Quantum computing is moving from the realm of research into practical capability, with profound implications for the security of our digital world. The potential for these systems to break today's widely used encryption methods is no longer hypothetical. Data of long-term value—secured today with traditional encryption—can already be stolen and stored for future decryption once quantum capabilities mature. In time, virtually all sensitive data will face this risk.

The Cloud Security Alliance (CSA) has long raised awareness about this risk, helping the cloud and cybersecurity communities recognize that quantum risk is both a present and future challenge. This is not merely a technical issue; it is a strategic concern for every organization that relies on digital trust to serve customers, protect intellectual property, and meet regulatory obligations.

Meeting this challenge demands more than new algorithms—it requires governance, clear ownership, and coordinated leadership to drive enterprise-wide action. Quantum-safe preparation should be viewed not just as insurance against a distant risk, but as a capability that delivers business value and transformation—regardless of when quantum computing matures. Done right, it strengthens data security, improves understanding of cryptographic risks, and builds the organizational muscle to manage complex technology transitions through rigorous governance programs. These benefits are immediate and measurable.

This joint report from IBM and CSA examines global quantum-safe readiness and the gap between awareness and execution. The time to act is now—organizations embedding governance-driven, quantum-safe principles into their security, transformation, and innovation agendas will be best positioned to safeguard their digital foundations in the quantum era.

Jim Reavis
CEO, Cloud Security Alliance

Mark Hughes
Global Managing Partner, Cybersecurity Services, IBM

Introduction

Quantum computing will fundamentally transform data security, forcing businesses to reimagine their entire approach to protecting systems and information.

At the heart of this challenge is cryptography—the science of protecting information through encryption, which ensures that sensitive data remains confidential and unaltered during storage or transmission. Current encryption methods, while robust against today's risks, could be broken by sufficiently powerful quantum computers.

Governments are already acting. In 2024, the US National Institute of Standards and Technology (NIST) published three post-quantum cryptography (PQC) standards designed to withstand quantum-enabled attacks.[1] These serve as global benchmarks for compliance and best practice. NIST is assessing additional algorithms for post-quantum data encryption. The UK's National Cyber Security Centre advises high risk systems to migrate to PQC by 2030, with full adoption by 2035.[2] Europe is aligning with NIST while pursuing national strategies, and many Asia Pacific countries are building their own PQC frameworks.[3]

However, quantum computers capable of breaking today's encryption may emerge five to six years before most organizations complete their transition. Threat actors are already using "harvest now, decrypt later" tactics—stealing encrypted data today to unlock once quantum capabilities mature.[4]

Meanwhile, IBM Institute for Business Value (IBM IBV) research (2023) finds most leaders expect the shift to take more than a decade.[5] The pace of these efforts is tempered by the complexity of identifying vulnerabilities and dependencies across thousands of applications and services.

Malicious actors are already using "harvest now, decrypt later" tactics—stealing encrypted data today to unlock once quantum capabilities mature.[4]

The takeaway: the timeline to act is shorter than it seems, and preparing now is essential to safeguard the digital backbone of every organization.

When quantum computers achieve sufficient scale and stability, they will render many current encryption methods obsolete—and cryptography touches every corner of our digital world (see Figure 1). This underscores the urgency of developing quantum-safe solutions. While challenging, the transition is achievable through early preparation and industry collaboration.

To assess quantum-safe preparedness, the IBM IBV, in collaboration with Phronesis Partners, surveyed 750 executives across 28 countries and 14 industries. These executives lead business, operations, security, or technology functions within their organizations, and all organizations surveyed generate at least $250 million in annual revenue. (See “Research methodology” on page 36.)

Our research indicates some leaders are charting a path forward. By examining leadership priorities and practices, we identify the top 10% of quantum-safe adopters—Quantum-Safe Champions (QSCs) (see Perspective, “The Quantum-Safe Readiness Index” on page 8)—and how they navigate this complex transition. We also uncover critical gaps between intention and execution and outline steps to secure the post-quantum future.

> “For us, quantum computing first entered our strategic radar through the cybersecurity lens. Its ability to render today’s encryption obsolete has profound implications for national infrastructure.”
>
> **Harrison Lung,** Group Chief Strategy Officer, e&, UAE

Figure 1

Why quantum safety impacts your organization
Cryptography touches every corner of the digital world

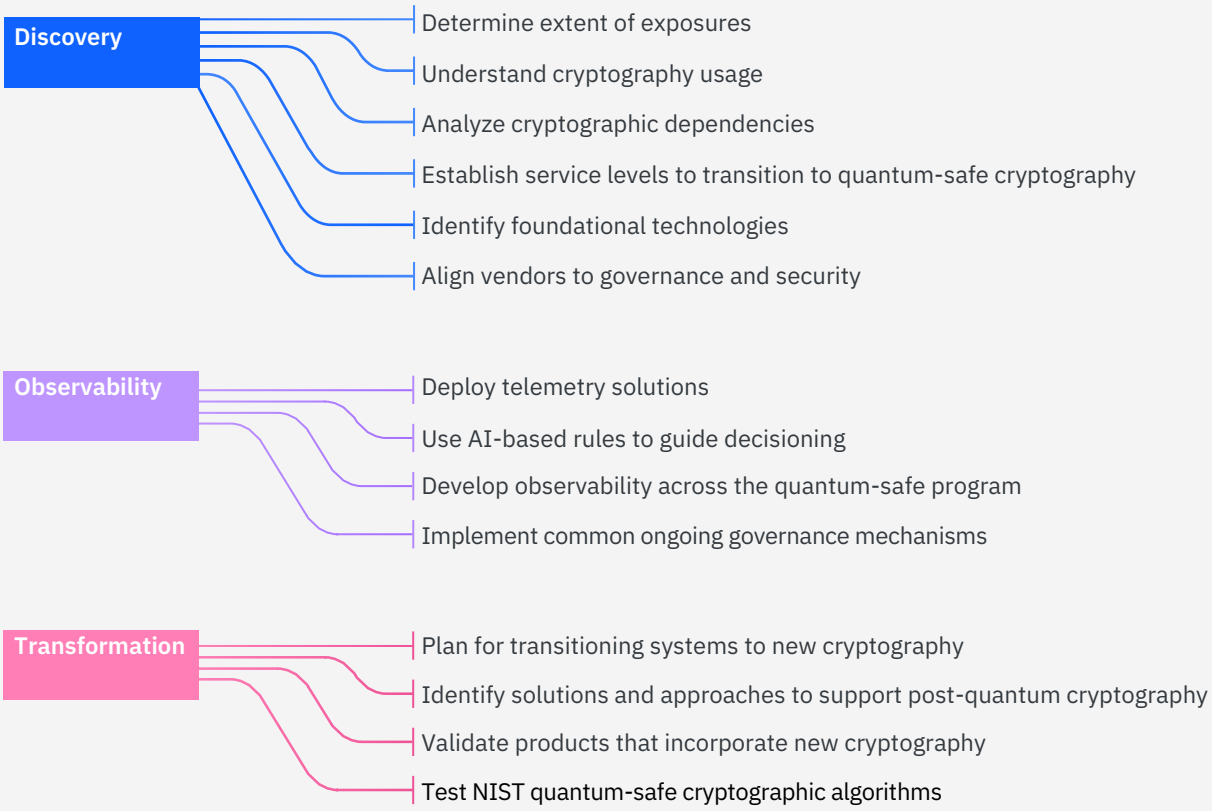
Note: Defined acronyms are Domain Name Service (DNS); Hypertext Transfer Protocol (HTTPS); Secure File Transfer Protocol (SFTP); electronic IDentification, Authentication, and trust Services (eIDAS); PDF Advanced Electronic Signature (PAdES); Advanced Electronic Signatures (AES); Europay, Mastercard, and Visa (EMV); Society for Worldwide Interbank Financial Telecommunication (SWIFT); Pretty Good Privacy (PGP); Public Key Infrastructure (PKI); and Lightweight Directory Access Protocol (LDAP).
Source: IBM Institute for Business Value

Perspective

The Quantum-Safe Readiness Index

The IBM Quantum-Safe Readiness Index (QSRI) assesses the global state of readiness for security in the quantum era, as measured by the readiness of individual organizations. The QSRI is intended to help leaders and stakeholders understand how their organizations are progressing in their quantum-safe initiatives.

The QSRI evaluates 14 activities, or indicators, across three key areas: quantum-safe discovery, observability, and transformation (see figure). Scores provide an indication of the organization's relative progress in their journey to becoming a quantum-safe organization. These 14 indicators are grouped into the below three categories and weighted based on IBM's subject-matter expertise and experience with clients. Scores are calculated based upon a 100-point index, with 100 representing the maximum possible score. The QSRI, first defined in 2023, is intended to assess (and re-assess) the quantum-safe readiness of an organization, industry, or region over time. (See "Research methodology" on page 36.)

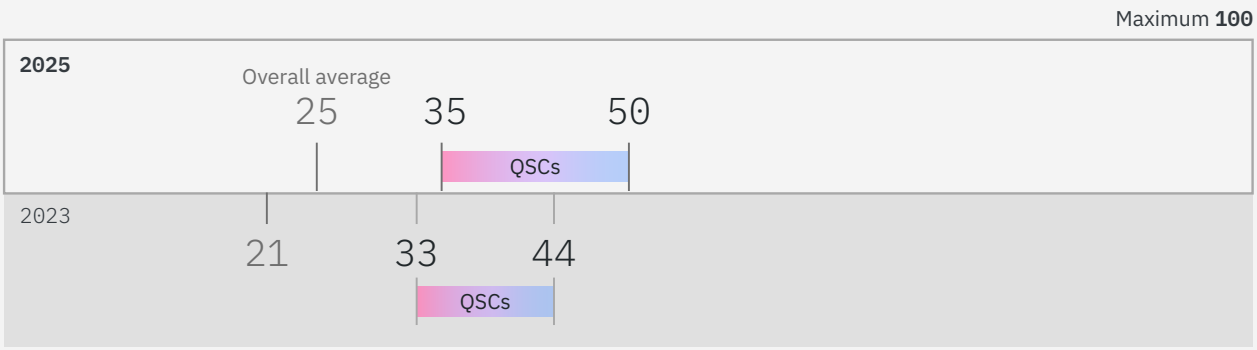


In 2025, the average quantum-safe readiness score is 25 on a 100-point scale—up 4 percentage points from the average score of 21 in 2023. This score represents a global average, reflecting organizations across industries and regions. We have designated organizations with the highest QSRI scores—the top 10%—as Quantum-Safe Champions (QSCs). QSCs scored 35 or above, with 50 being the highest score attained by any organization, up from 44 in 2023 (see figure).

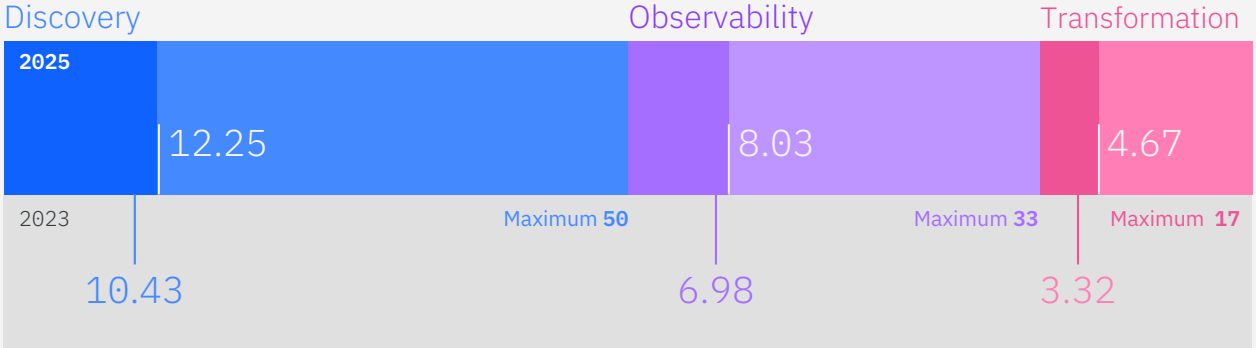
Given quantum safety is only now gaining greater visibility—with many organizations still in the planning stages—the quantum-safe readiness score is most influenced by early-stage activities such as an organization's discovery capabilities.

The 2025 QSRI shows gradual overall progress toward quantum resilience, with early phases—Discovery and Observability—advancing more quickly as organizations improve their ability to identify and monitor cryptographic risks. The Transformation phase is also improving but remains at low absolute scores, indicating strong early-stage momentum. Sustained focus and investment will be essential to convert preparedness into true quantum-safe capability.

The average quantum-safe readiness score: 25 out of 100



Measuring progress toward quantum-safe readiness



Section 1

The awareness-action disconnect

Defining the current state of quantum-safe readiness is the vast chasm between awareness and meaningful action.

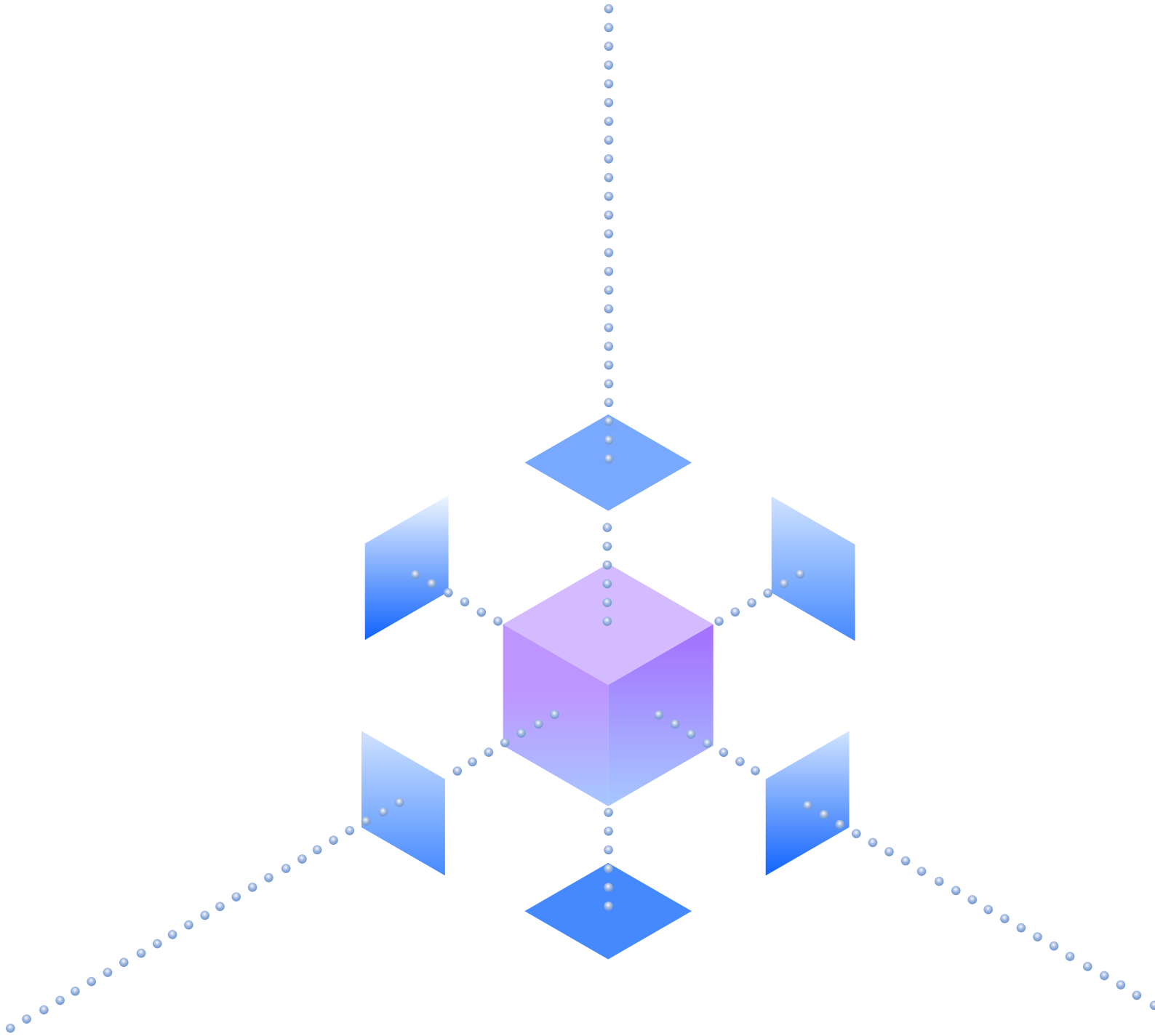
There's no dearth of recognition here—73% of organizations report business and technology leaders are working closely on their quantum-safe strategy. This figure suggests a level of cross-functional engagement that should, in theory, translate into robust preparedness initiatives. What informs this collaboration is the need to assess how operational risks are evolving. This underscores the importance of taking a risk-based approach as a way to bring cross-functional stakeholders together.

Yet many organizations are still trying to rationalize quantum-safe investments. Only 19% have identified near-term maturity goals for their quantum-safe initiatives. While 48% of QSCs have identified near-term maturity goals, this disconnect still reveals a fundamental problem. Organizations are engaging in the ritual of preparation—convening committees, holding discussions, commissioning reports—while failing to establish the concrete milestones and measurable objectives that transform intentions into reality. For example, just 30% of organizations have inventoried applications, data, and services to understand how cryptography is implemented across the organization—a critical starting point toward making future progress that informs risk assessment and prioritization activities.

The gap between strategy and execution is most evident when looking at the adoption of benchmarking and crypto-agility practices, with more than seven in ten organizations (71%) indicating they are actively benchmarking their quantum-safe capabilities relative to peers and 70% reporting they already have a crypto-agility program in place. Note: Crypto-agility is the ability to rapidly adapt cryptographic algorithms and data encryption protocols to an evolving security threat.

If so, and in fact crypto-agility programs have been established—why are we seeing such halting progress in terms of quantum-safe readiness?

Many business stakeholders may not appreciate the lag between demand and deployment, and between technology planning and operational execution. If organizations delay quantum-safe transition efforts until they have no choice, remediation and establishing crypto-agility could prove far more costly and more challenging than if they take a longer-term, programmatic approach that builds capabilities over time.



"Retrofitting later is always more painful and expensive. If we can remediate today, it's going to be much cheaper than if we wait. That is something I understand very clearly, even if I don't know the technical side of quantum computing yet."

Maj. Manjit Rajain, Founder & Global Chairman, Tenon Group

A strategic asset: The cryptographic inventory

One of the most telling indicators of strategic immaturity is the underutilization of insights from a cryptographic inventory. The inventory process requires organizations to perform a comprehensive assessment of their digital infrastructure to map cryptographic implementations and dependencies—whether that's an API, cloud provider, IoT device, third-party solution, or something else.

The goal is to create a thorough inventory of cryptographic assets, providing a definitive map of information flows, shared resources, interdependencies, and mission-critical assets and services. An inventory must also examine internal and external dependencies across the software supply chain and prioritize vulnerabilities. These are the initial steps in developing a quantum-safe transformation roadmap.

The challenge is that organizations run thousands of applications, built from millions of lines of code, and each application depends on cryptography. Identifying vulnerabilities is like finding a needle in the haystack. And manual cryptographic discovery can take months. However, this analysis can also inform broader business transformation efforts, such as those related to data insights or AI operations, so the investment is well spent.

And yet, as noted earlier, fewer than one in three organizations (30%) have completed a cryptographic inventory (see Figure 2). Even fewer (24%) apply these insights to business transformation initiatives—a critical step in improving readiness and establishing priorities. For example, not all data types must be prioritized. Long lifecycle data (such as root certificates, regulatory data, and infrastructure keys) requires immediate attention, while short-lived communications may have lower priority. That so few organizations are acting on insights from a cryptographic inventory represents a missed opportunity and a lost chance to extend the value of other change initiatives.

In reality, organizations may need to operate two cryptographic regimes in parallel—one for classical encryption and the other for quantum-safe encryption.[6] The hybrid approach will require concerted testing and deployment planning to facilitate successful interoperations. This is yet another reason why moving from awareness to action is a priority—and why the cryptographic inventory can become a strategic asset.

Figure 2

Cryptographic inventory
A missed opportunity for strategic advantage

30%
of organizations have taken cryptographic inventory

But only

24%
engage with insights arising from their inventories.

Q. What is the extent to which your organization is prepared for quantum-safe security in the following areas? Taking inventory of applications, data, and services to understand how cryptography is currently being used. Applying findings from cryptographic inventory to business transformation initiatives.

"The way we explain it internally is that this is going to happen no matter what—the only uncertainty is when. And because it's a complex project that will take years, the moment to start is now."

Rafael Cantó, IP Network Manager, CTIO office, Telefonica, Spain

Case study

IBM CIO Office—Managing quantum-era cryptographic risk[7]

As quantum computing begins to deliver value, the security landscape faces change to the status quo. Alongside quantum computing advancement, IBM prioritizes the need for organizations to be quantum safe and has developed three of the four post-quantum cryptography algorithms that have been selected by NIST for standardization.

Early on, IBM recognized a risk that today's cryptography could be tomorrow's liability. Consequently, IBM's CIO Office established clear goals to discover cryptographic artifacts with near-zero manual effort, generate an actionable Cryptographic Bill of Materials (CBOM) for full visibility, identify and remediate crypto-agility anti-patterns before they reach production, and proactively manage quantum-era cryptographic risk with measurable outcomes.

Like every organization, IBM must identify all instances of data encryption used in its applications to reduce security risk and meet NIST PQC migration requirements. With thousands of homegrown applications and disparate codebases, manual discovery was impractical. The IBM CIO Office realized cryptography is often buried deep in code across dozens of libraries, making comprehensive visibility nearly impossible without automation.

IBM's CIO Office demonstrates that establishing quantum-resilient cryptographic hygiene does not require massive organizational disruption.

The IBM CIO Office leveraged IBM's Guardium® Quantum Safe Explorer solution to discover cryptographic artifacts with near-zero manual effort. The solution automated scans, integrated with the IT application build pipeline, and was incorporated into regular DevSecOps routines—thus avoiding the need for manual audits.

In just a few hours, the IBM CIO Office team scanned:

- **5,815** repositories
- **440,689** files
- **47.6 million** lines of code.

As well, the team:

- Identified **3,943** issues requiring quantum-safe remediation
- Detected **2,499** crypto-assets.

These automated CBOMs enabled audit compliance while dashboards provided leadership with enterprise-wide visibility into cryptographic risk exposure. The solution discovered numerous legacy components using key sizes too small by quantum-safe standards, hardcoded cryptographic parameters, and missing crypto-agility patterns.

The IBM CIO Office demonstrates that quantum-resilient cryptographic hygiene does not require massive organizational disruption. Using an automated crypto-discovery solution, transformation leaders could quickly ascertain potential risk exposure and then streamline deployment across an intensive continuous integration / continuous deployment (CI/CD) environment. The outcome was expedited using an interactive dashboard that offered enterprise-wide visibility and actionable insights.

Digital transformation as a readiness driver

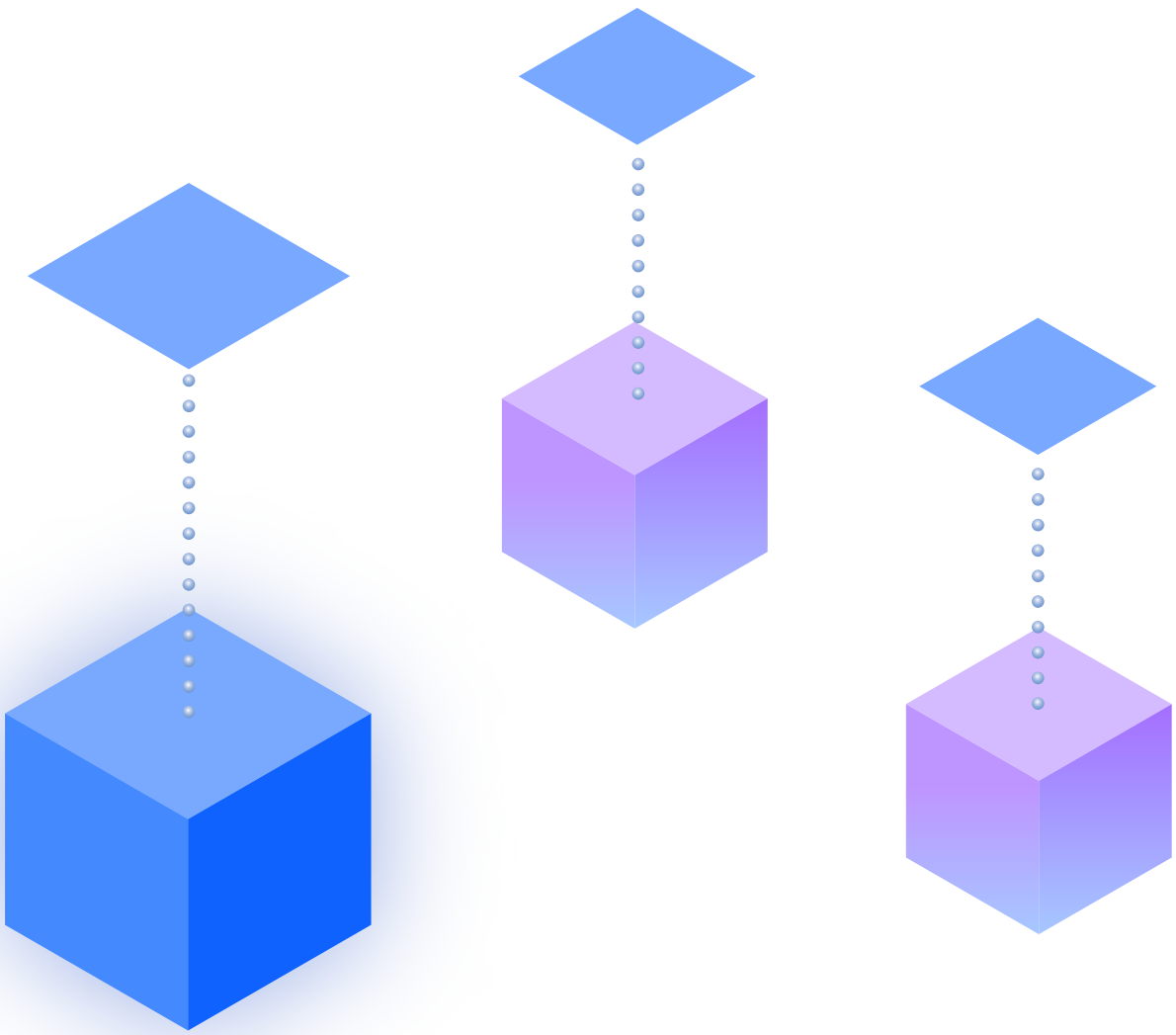
Despite these challenges, QSCs are starting to differentiate from their peers. Most notably, organizations demonstrating maturity in digital transformation show stronger quantum-safe readiness positioning.

49% of QSCs outperform in digital transformation versus 34% for all others. This correlation reflects similarities in the capabilities required for both challenges.

Digital transformation and quantum-safe preparation both require organizations to think systemically about change—in terms of technology, process, and people. Both demand the ability to manage complex, multiyear transitions while maintaining operations. Both necessitate collaboration among traditionally separate functions. And both require treating technology transformation as a business opportunity rather than merely a technical upgrade.

However, even these advantages come with caveats. Despite 64% of organizations viewing quantum safety as a continuous transformation program, delays in completing core planning assets such as a cryptographic inventory suggest change may be perceived as a “one-time quick fix” rather than as part of a “cryptographic agility” program that will play out over several years.

Organizations with strong digital transformation track records bring several advantages to quantum-safe preparation. For example, among organizations characterized as QSCs, 53% outperform their peers in IT resiliency and business continuity.



Beyond readiness: Investing for resilience

While organizations that outperform on agility, innovation, digital transformation, and talent demonstrate greater quantum-safe readiness, many of these same organizations struggle to justify quantum-safe investments within traditional ROI frameworks.

In fact, 58% of QSCs cite difficulties justifying their quantum-safe budgets without a more defined ROI.

This dichotomy reflects a fundamental tension in how organizations approach emerging risks. Innovation-oriented companies can be more comfortable with uncertainty and more willing to invest in capabilities before clear payoffs emerge. Yet even these organizations find it challenging to build compelling business cases for quantum-safe investments, particularly given the uncertainty around timing and specific risk vectors.

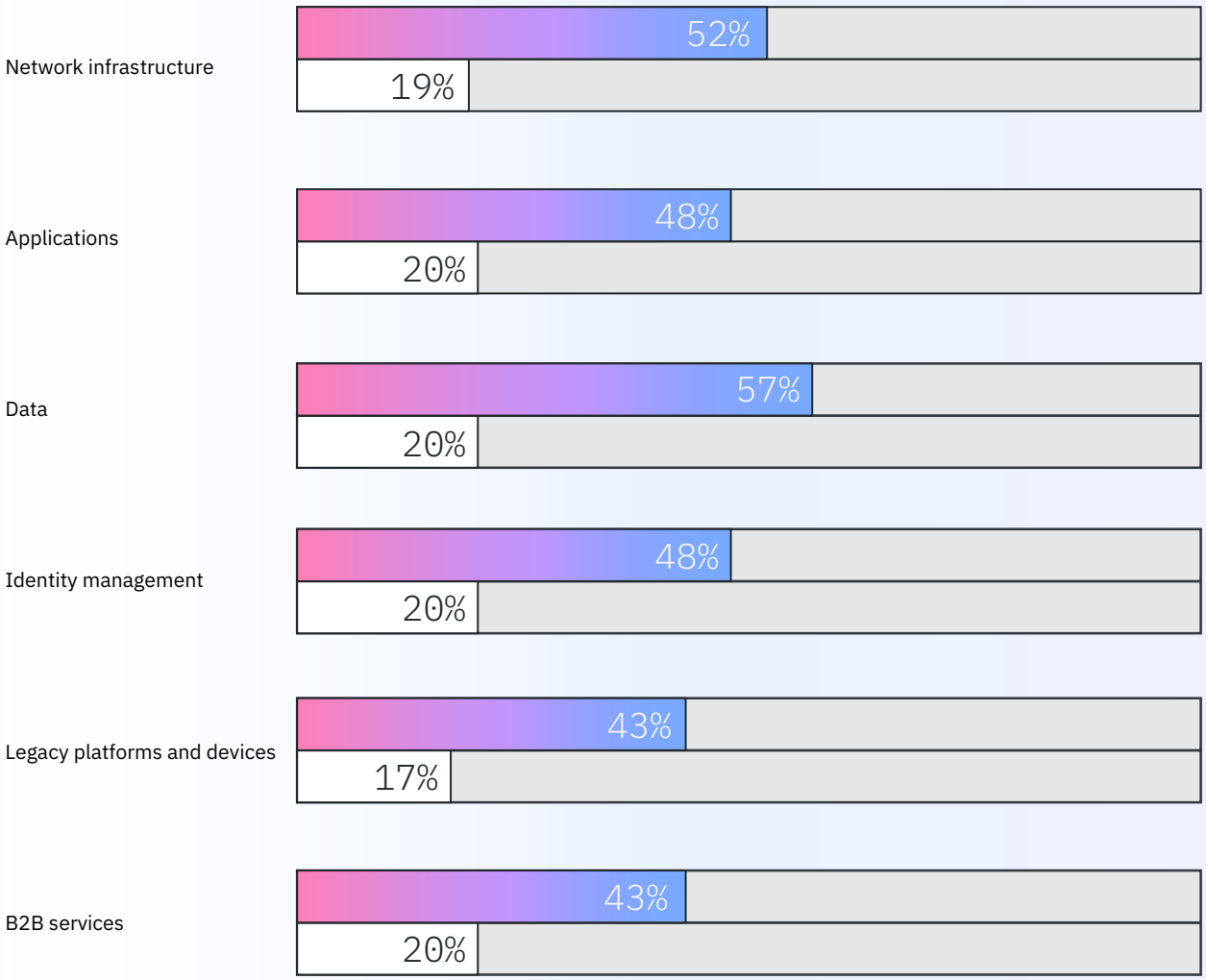
The resolution? Shift organizational perspective. Reframe quantum-safe preparation not as insurance against a specific future risk, but as a capability that delivers business value and transformation benefits regardless of when quantum computing capabilities mature. Organizations approaching quantum safety as an opportunity to strengthen their overall data security posture, improve their understanding of cryptographic risks, and build organizational capabilities for managing complex technology transitions can justify investments based on immediate benefits. QSCs exemplify this (see Figure 3).

"One of the biggest side benefits of this work is that it forces us to link every single asset and connection to the corresponding solution and business process. That's valuable not just for quantum safe, but for incident handling, vulnerability management, and other security processes."

Manuel García-Cervigón, Strategic Product Portfolio Architect at Nestlé, Spain

Figure 3

Resiliency across the board
QSCs report substantially better metrics than their peers



Q. How resilient is your organization in the above areas? Percent reporting somewhat better than peers and significantly better than peers.

Section 2

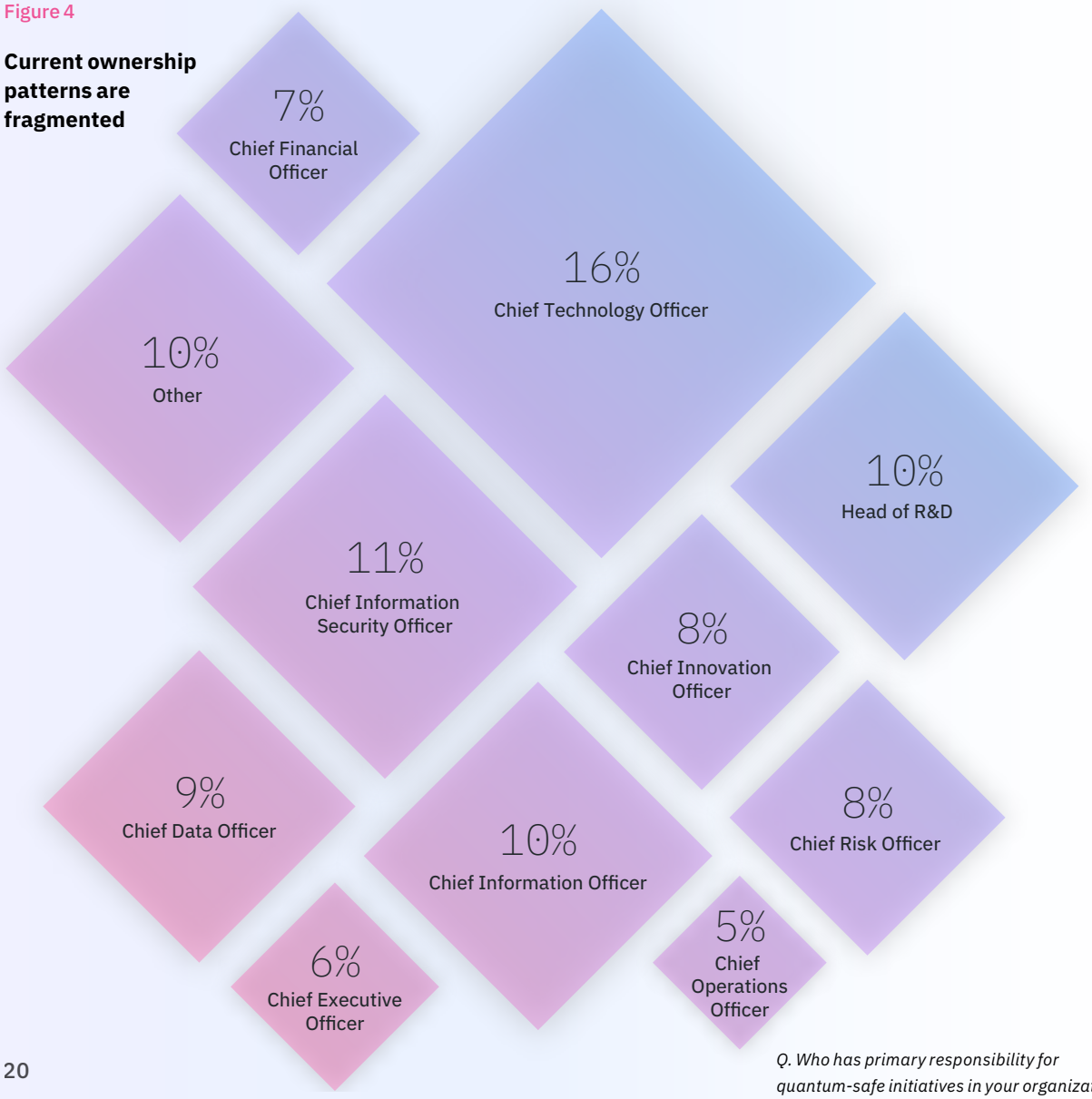
Leading together: Governance, collaboration, and skills

Given the extent to which we rely upon digital encryption protocols, the quantum-safe challenge demands unprecedented coordination across organizational functions.

Yet current ownership patterns reveal a fragmented landscape that can undermine effective action. Chief Technology Officers (CTOs) emerge as the most-cited owners of quantum-safe initiatives, with 16% taking the most active role, followed by Chief Information Security Officers (CISOs) at 11% and Chief Information Officers (CIOs) at 10% (see Figure 4).

Figure 4

Current ownership patterns are fragmented



Q. Who has primary responsibility for quantum-safe initiatives in your organization?

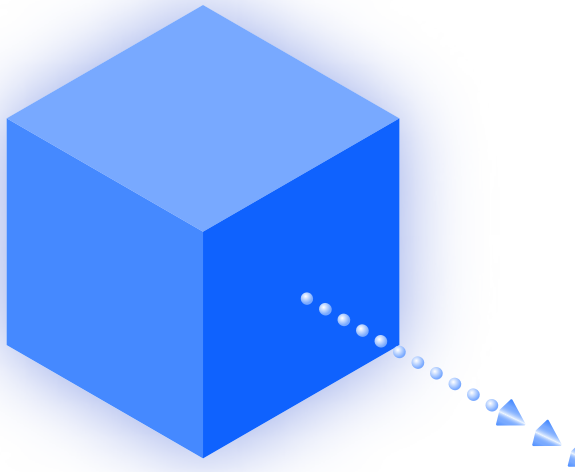
While this distribution might seem reasonable given the technical nature of the challenge, it skews quantum safety to primarily a technology problem rather than an enterprise-wide business imperative. When cryptographically relevant quantum computers become widely available, the impact will extend far beyond technical infrastructure to affect customer relationships, regulatory compliance, competitive positioning, and business processes. It's an enterprise-wide resilience that requires business as well as technical ownership.

What's notable is a lack of consensus for who should own the quantum-safe transformation program. In different organizations, responsibilities are allocated across a mix of technology, security, business, and operations executives. This makes it hard to build awareness, accountability, and agency across functions.

Our research also reveals a split in how organizations view quantum's relationship to other advanced technologies. Nearly half of respondents (45%) see quantum computing as complementary to AI and high-performance computing, while just over one in four (26%) view it as a distant, unrelated capability.

Without clear agency and accountability, quantum-safe initiatives can become enmeshed in organizational politics, resource conflicts, and competing priorities. CTOs may focus on technical standards and implementation timelines, CISOs on risk assessment and compliance requirements, and CIOs on operational continuity and cost management. While all these perspectives are necessary, the absence of unified leadership often results in suboptimal solutions that satisfy technical requirements without addressing broader business needs. Unclear ownership and accountability are challenges across the board, with 42% of all organizations citing it as a barrier to the quantum-safe readiness of their organization.

Without clear agency and accountability, quantum-safe initiatives can become enmeshed in organizational politics, resource conflicts, and competing priorities.



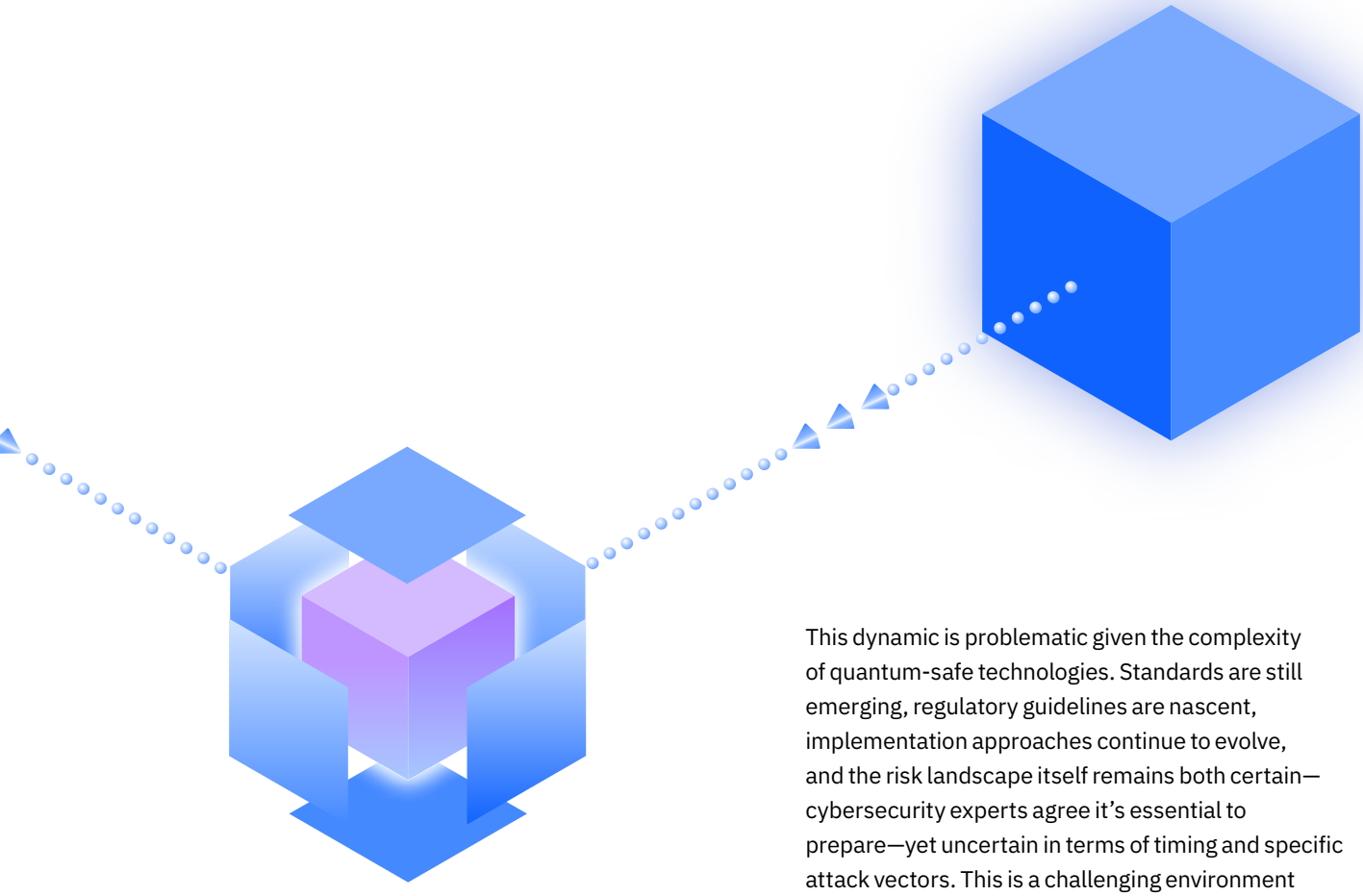
Balancing internal ownership with vendor dependency

Compounding this uncertainty is an overestimation of the role of external vendors in solving quantum-safe remediation issues. 62% of respondents believe vendors will handle quantum-safe transition requirements for them, while 56% continue to view quantum safety as purely a technical issue.

This perspective—that quantum safety is a technology challenge and one that can be outsourced—can lead to a dangerous oversight in terms of organizational preparedness. And it also creates a perilous assumption that vendors and supply chains are indeed quantum safe themselves.

Our conversations with leaders suggest organizations are wise to approach vendors as partners who can provide tools and expertise. The organization itself must provide the organizational change management, stakeholder alignment, in-house quantum-safe literacy, and business continuity planning that successful transition demands. In this regard, the transition to quantum-safe cryptography is very much a shared responsibility—requiring accountability from senior leaders, stakeholders across the organization, and key ecosystem partners.

More subtly, vendor dependency can create a false sense of security that impedes genuine preparedness. When leaders believe quantum safety is a short-term or one-off migration, they might fail to develop the internal capabilities, governance structures, and institutional knowledge necessary for effective oversight and adaptation. The result: organizations that may have heavily invested in quantum-safe solutions but lack the organizational muscle memory to deploy, manage, and evolve them effectively.



This dynamic is problematic given the complexity of quantum-safe technologies. Standards are still emerging, regulatory guidelines are nascent, implementation approaches continue to evolve, and the risk landscape itself remains both certain—cybersecurity experts agree it's essential to prepare—yet uncertain in terms of timing and specific attack vectors. This is a challenging environment to make investment decisions.

Traditional ROI measures might be hard to quantify given the organization's extensive reliance on cryptography and the fact that every industry and organization has a unique combination of assets and capabilities secured by data encryption. In this regard, partners can provide valuable guidance—helping to inform the business case based on leading practice and their work with clients across industries.

"While NIST has standardized post-quantum algorithms, global standards bodies are still integrating them into protocols. For sectors like telecommunications, adoption timelines are closely tied to these developments and the readiness of vendors to support quantum-safe products."

Wee-Sain Koh, Cluster Director (Engineering) BizTech Group, Infocomm Media Development Authority (IMDA) Singapore

The upside of collaborative consortia

Beyond internal coordination issues, organizations often face obstacles in their external collaboration strategies.

While there is broad recognition that preparing for quantum-related risks could be more effective through industry-wide coordination, actual participation in such collaborative efforts remains inconsistent (see Figure 5).

Some organizations may hesitate to join or fully engage in joint initiatives due to practical and cultural considerations. For example, effective participation in a consortium can require significant time, resource allocation, and alignment across differing organizational priorities and timelines. Establishing governance structures that maintain trust, protect competitive interests, and ensure fair representation is necessary to assure participants their competitive posture will be enhanced, not compromised.

Organizations may also perceive consortia as difficult to join. But the truth is, not only are most consortia welcoming to enterprises within their industry, they also value members from other industries. The idea is to listen, learn, and grow.

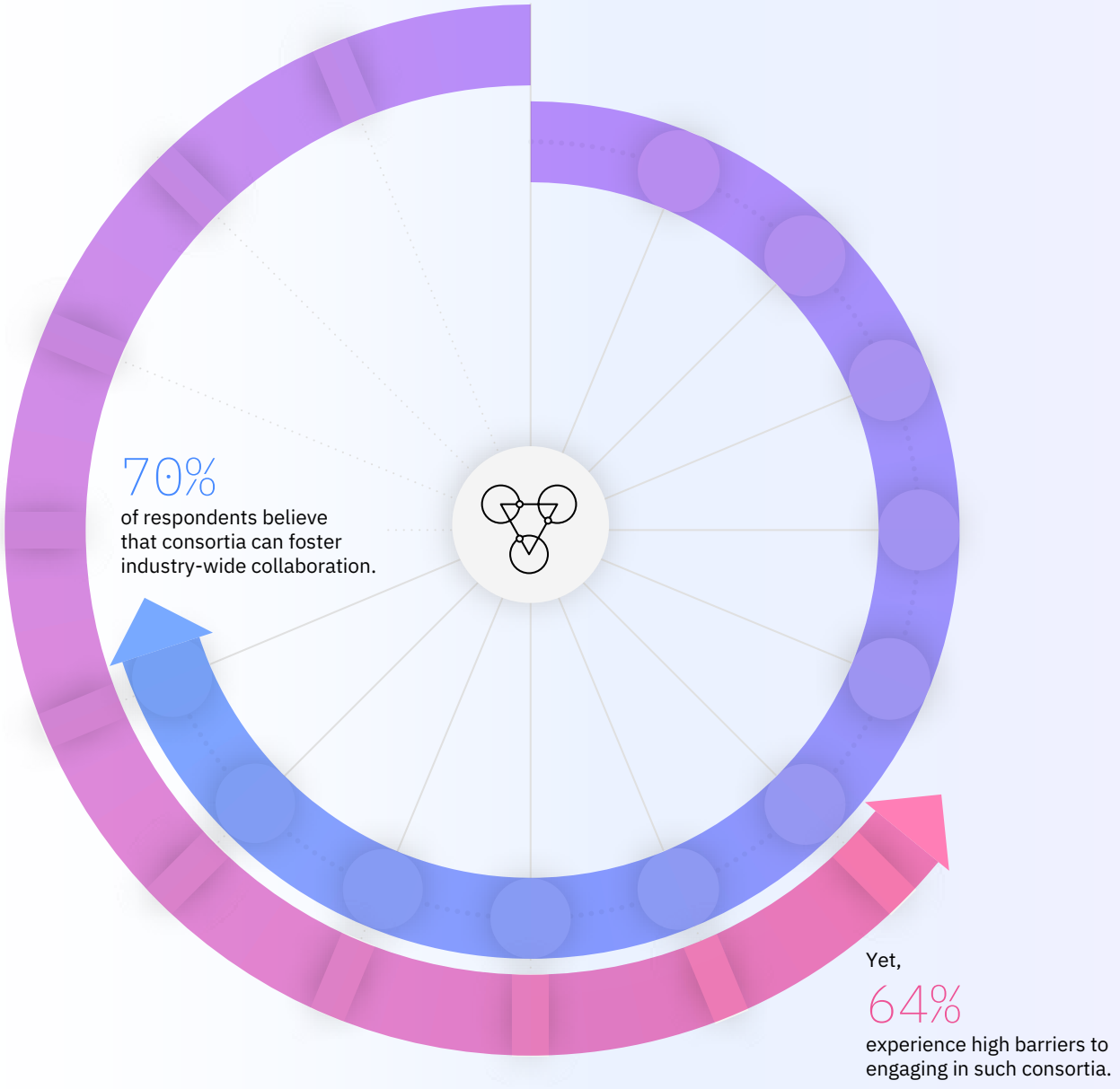
Importantly, participation in a consortium does not require members to share sensitive enterprise-specific details, such as internal encryption practices, proprietary roadmaps, or competitive strategies. Instead, consortia typically focus on sharing nonsensitive insights, developing common standards, advocating for supportive policies, and coordinating approaches to challenges that affect an entire sector.

Cultural barriers can still arise, often rooted in a competitive mindset or concerns about intellectual property. Overcoming these hurdles requires building confidence that collaboration can strengthen—not compromise—an organization's market position, while also contributing to collective resilience against emerging threats such as those posed by post-quantum security vectors.

Importantly, participation in a consortium does not require members to share sensitive enterprise-specific details such as internal encryption practices. Instead, consortia focus on sharing nonsensitive insights, developing common standards, and coordinating approaches to sector-wide challenges.

Figure 5

Consortia: High rewards but high barriers



Q. To what extent do you agree with the following statements about the role of ecosystems in advancing quantum-safe security? Consortia can foster industry-wide collaboration related to quantum-safe transformation. There is a high barrier of entry to quantum-safe consortia.

The criticality of skills to quantum-safe transformation

The skills gap manifests in several critical ways, directly impeding quantum-safe progress.

According to organizations we surveyed, they're operating with only about two-thirds of the quantum-safe cryptography expertise necessary for quantum-safe protocol implementation, leaving a critical 36% skills gap.

Organizations lack the internal expertise needed to evaluate quantum-safe cryptographic algorithms, assess their suitability for specific use cases, and implement them effectively within existing infrastructure. Without internal expertise capable of translating technical trade-offs into business implications, organizations struggle to make informed choices about alternative approaches, timeline options, and resource allocation strategies.

QSCs invest about two times the resources compared to their peers. And they're proficient, with 69% of them reporting they're highly effective at obtaining talent via internal skills development, attracting talent from adjacent STEM fields, partnering with academic institutions and research labs and internship programs, compared to just 6% of those early in their quantum-safe journey.

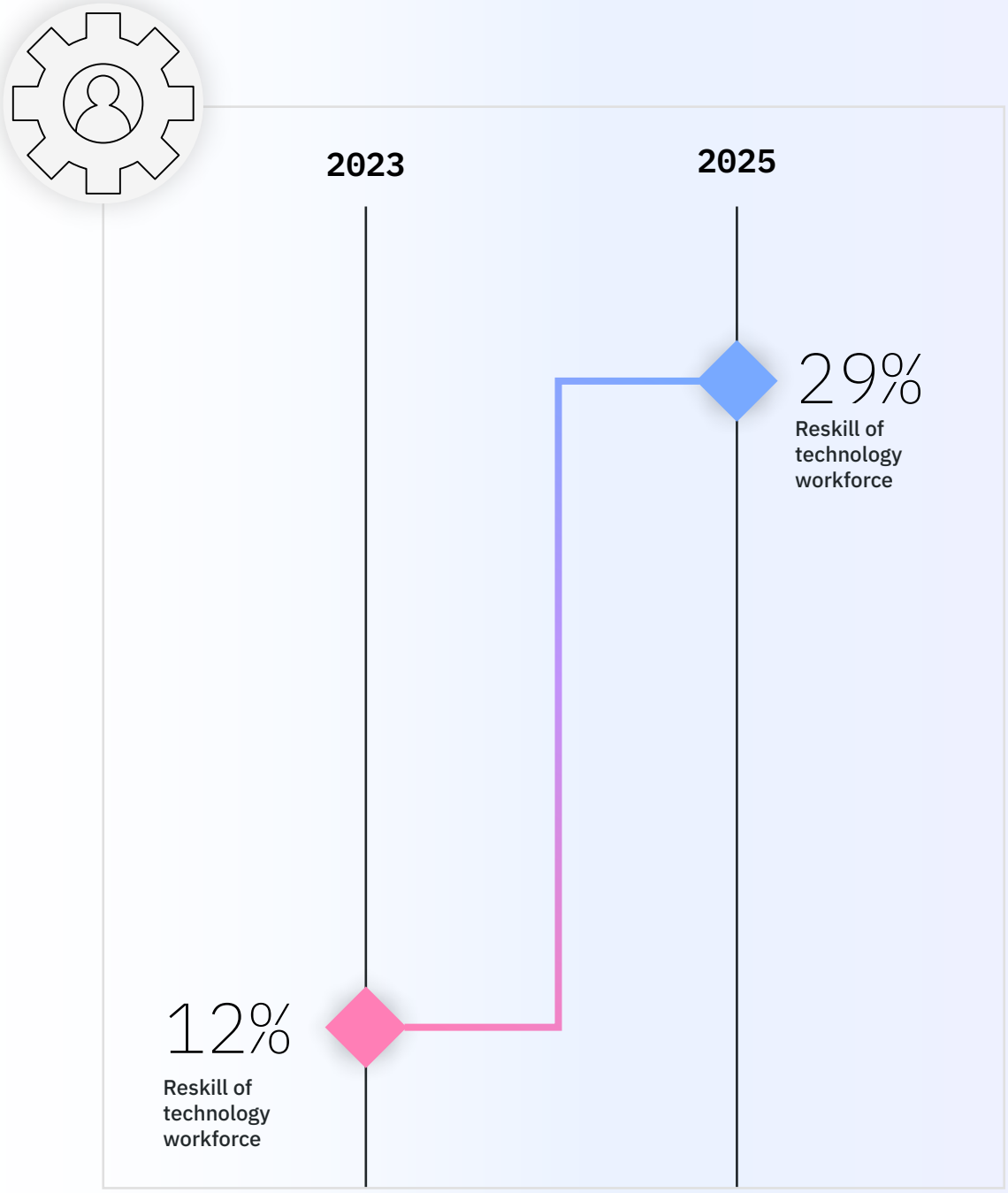
Reskilling emerges as the most powerful driver of quantum-safe readiness, outperforming both external recruitment and vendor partnerships in its impact on organizational preparedness.

Why? Internal teams have valuable perspective on both institutional infrastructure and cultural norms. By developing core competencies in-house, leaders create sustainable capabilities that evolve with changing technologies and threats. And indeed, these are the core characteristics of "cryptographic agility" (crypto-agility for short). Leaders should also push vendors to create tools that simplify and automate remediation, enabling resources to handle key tasks efficiently.

According to organizations we surveyed, they're operating with only about two-thirds of the quantum-safe cryptography expertise necessary for quantum-safe protocol implementation, leaving a critical 36% skills gap.

Figure 6

The reskilling imperative
A steep climb in the need to develop quantum-safe knowledge



Q. What proportion of your technology workforce will need to reskill to support the quantum-driven needs of your organization over the next three years?

Specifically, crypto-agility means rapidly adapting cryptographic mechanisms in response to changing threats and technological advances. In practice, it's not just about transitioning to quantum-safe cryptography or updating algorithms. Instead, organizations must continuously evolve their cryptographic architecture, automation, and governance to enable greater control and flexibility while adopting a posture that allows them to adapt to evolving cyber and crypto threats with minimal disruption.[8]

The effectiveness of internal skill development also reflects the interdisciplinary nature of quantum-safe transformation. A successful outcome requires not just cryptographic expertise but also understanding of business processes, regulatory requirements, risk and governance practices, and change management techniques. Internal teams are best positioned to develop and maintain these multifaceted capabilities.

Section 3

From risk to reward

Quantum-safe risk takes on new complexities the closer we move to implementation.

One area where deployment challenges are likely to emerge is in how the organization supports data encryption for both classical and quantum-safe workloads. This can require the ability to support multiple security certificates, yet many legacy applications and services might not be able to adopt this approach. So, deployment teams may need extra time to develop wrapper-services or new trust authority (TA) and certificate authority (CA) frameworks.

Classical and post-quantum encryption regimes must coexist seamlessly. This dynamic data landscape increases potential attack surfaces and complicates protection strategies.

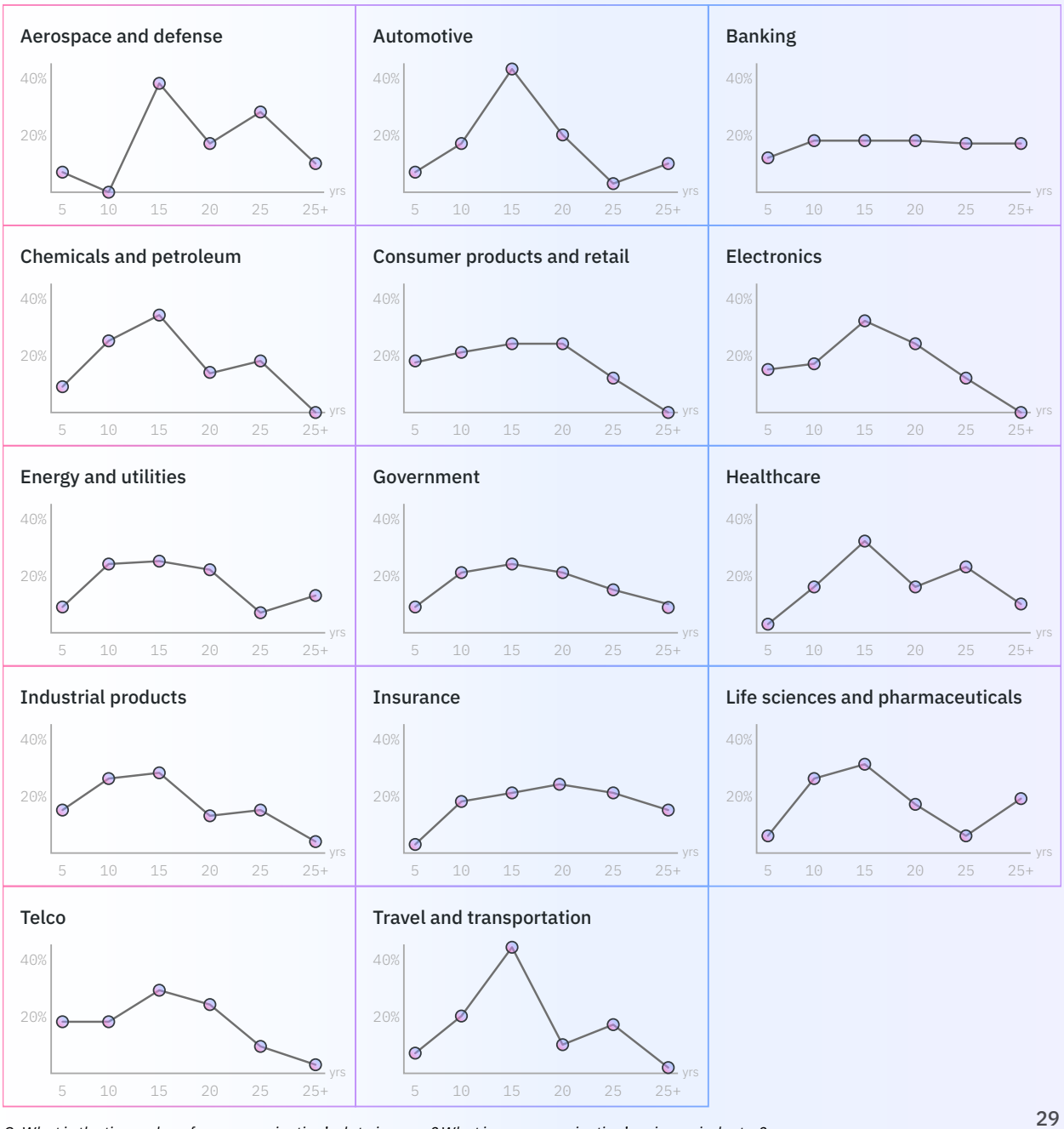
The other key consideration is the operational lifecycle of data, which dictates the timeframe for which it needs protection (see Figure 7). Only 10% of organizations consider their data valuable for five years or less. 68% of organizations consider their data valuable for somewhere between 10–20 years. For QSCs, data retains value even longer, with a third of QSCs considering their data valuable for 25 or more years.

"We advocate a hybrid cryptography approach—co-deploying classical and PQC algorithms to ensure continuity and gradual migration to PQC."

Kamal Kumar Agarwal, Deputy Director General (Quantum Technology), Telecommunication Engineering Centre, Department of Telecommunications, India

Figure 7

How long does data need protecting?
Y-axis represents percentage of industry respondents. X-axis represents respondents' assessments of how long data must be secure for their industry.



Q. What is the time value of your organization's data in years? What is your organization's primary industry?

Linking risk, response, and readiness

While the Quantum-Safe Readiness Index (QSRI) quantifies preparedness on a 100-point scale across discovery, observability, and transformation, the quantum-safe landscape reveals an underlying paradox.

Organizations with similar risk profiles often demonstrate wildly different levels of response preparedness, while those with comparable response capabilities face vastly different threat environments (see Figure 8). This divergence suggests that an effective quantum-safe strategy requires a nuanced understanding of how organizational risk intersects with response capacity. Different organizations can encounter distinct preparation challenges that demand tailored approaches.

Organizational risk in the quantum context emerges from the intersection of three critical factors:

- *Exposure*—How much quantum-vulnerable infrastructure an organization depends upon
- *Vulnerability*—How quickly and severely quantum attacks by bad actors could damage operations
- *Impact*—The business consequences of cryptographic compromise

Meanwhile, organizational response capacity combines:

- *Strategic preparedness*—The quality of planning and governance structures
- *Resource commitment*—The human and financial capital devoted to quantum-safe initiatives

When these dimensions are mapped against each other, four distinct organizational risk-response approaches emerge, each presenting unique challenges and opportunities for quantum-safe solutioning.

Figure 8

The four risk-response quadrants
And key characteristics for each

Linking risk, response, and readiness (continued)

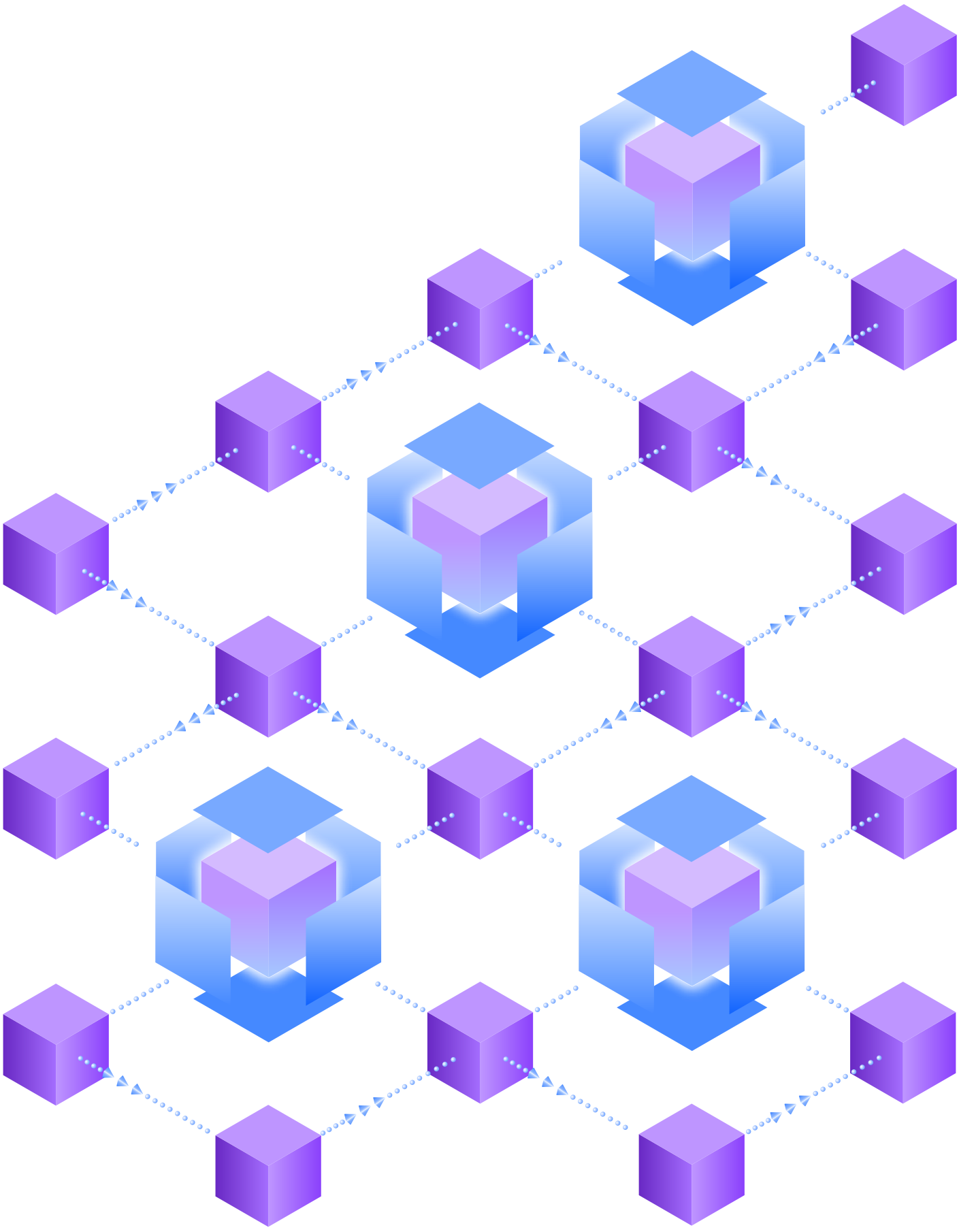
Low-risk, low-response organizations (21% of all organizations)
Efficient and stable, these organizations feel little urgency to change course. With a median revenue of $5.2 billion and the highest budget growth over the past three years (10%), they focus on efficiency over uncertain expansion. They devote the smallest IT budget share and are least likely to name cybersecurity as a top challenge. Moderately attentive to quantum risks, they struggle to justify quantum-safe investments within ROI models. High confidence—64% believe they outperform competitors in IT resiliency—can hinder change before disruption hits.

Low-risk, high-response organizations (29% of all organizations)
This group best understands the quantum-safe challenge, often linking quantum computing and AI in a shared view of emerging-tech disruption. They allocate the most budget to IT and R&D. Talent is their top challenge (41%), yet they continue their quantum investments. Among active investors, 89% express strong confidence in crypto-agility programs. Still, sustaining funding for future-oriented quantum-safe security remains difficult.

High-risk, low-response organizations (29% of all organizations)
In the most precarious position, these organizations cite cybersecurity as the top challenge (43%), with 49% rating their performance below competitors. They post the lowest budget growth and often underperform peers in efficiency and profitability. Awareness of quantum risks is high, but perceived complexity, lack of urgency, and organizational paralysis stall action, leaving them exposed.

High-risk, high-response organizations (21% of all organizations)
The largest players, with median revenue of $7.25 billion, forecast the strongest 2025 budget growth. They expect the highest quantum investment return by 2030 (475%) and show strong readiness commitment. Yet lack of executive urgency (64%) and the need to reskill 33% of the technical workforce for quantum technologies create friction. High cybersecurity concern and capability gaps fuel tension between ambition and vulnerability.

74% of QSCs are high-response organizations.

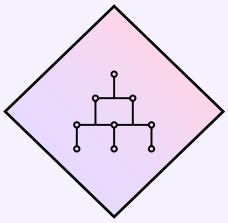


Action guide

Cryptographic risks from quantum computing, first demonstrated 30 years ago, are now materializing.[9] Leaders must shift from strategic planning to active discovery, governance, and remediation. Quantum risk transcends IT boundaries, requiring clear executive ownership and dismantling departmental silos.

Given our reliance on secure encryption, this operational risk impacts every business function—legal, compliance, finance, supply chain, and customer relations. Approached creatively, quantum safety can become a vehicle for driving business transformation, not merely a technology modernization effort.

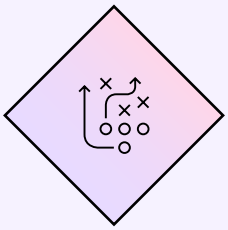
The framework below provides a structured approach for quantum-safe transformation programs, aligning with existing capabilities and risk exposures.



Low-risk, low-response organizations

Focus on building a strong foundation.

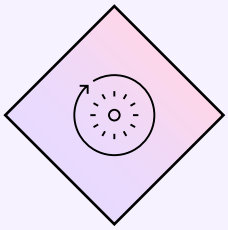
- Inventory critical business applications, documenting cryptographic assets and dependencies.
- Assess future cryptography needs using tools to compare current versus desired posture.
- Create an initial CBOM for key applications.
- Build basic quantum-risk literacy for C-suite and technical leaders.
- Integrate quantum safety and crypto-agility into digital transformation.
- Plan PQC adoption and phase out classical algorithms.
- Update procurement to prioritize quantum-safe vendors.
- Join an industry-aligned quantum-safe working group.



Low-risk, high-response organizations

Refine your strategy to stay ahead.

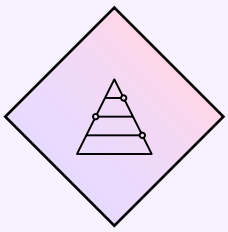
- Model quantum risk exposure through scenarios.
- Identify and prioritize critical applications.
- Focus remediation by risk and criticality.
- Establish cryptographic standards and quantum-safe design guidelines.
- Formalize governance, policies, and controls.
- Create a reference cryptographic architecture.
- Automate CBOM generation and integrate into development pipelines.
- Deploy cryptographic lifecycle management tools.
- Embed quantum-safe principles into innovation programs.
- Establish a quantum-safe Center of Excellence.



High-risk, low-response organizations

Re-assess and drive urgency.

- Form a quantum-safe steering committee with senior sponsorship.
- Build cross-functional literacy and allocate funding.
- Protect data vulnerable to “harvest now, decrypt later” attacks.
- Deploy automated discovery to catalog assets and dependencies.
- Map cryptographic dependencies to better understand your specific risk exposure.
- Implement crypto-monitoring tools.
- Pilot migrations of key applications to assess remediation complexity.
- Join a quantum-safe working group for best practices.



High-risk, high-response organizations

Lead with top-down action.

- Create a C-level quantum-safety council.
- Quantify cryptographic risks in financial terms and define high-impact business cases.
- Invest R&D in quantum-safe technologies aligned to risk exposure and growth.
- Map all business applications and dependencies.
- Update your operating model to support continuous cryptographic awareness.
- Set performance benchmarks and enable real-time posture monitoring via dashboards.
- Partner with strategic vendors to create baseline capabilities.
- Pilot third-party integrations and hybrid crypto solutions.
- Implement automated discovery and remediation tools.
- Leverage early adoption as a competitive advantage.

Research methodology

Survey scope and participant profile

To assess global enterprise preparedness for quantum-enabled risks, the IBM Institute for Business Value (IBV), in partnership with Phronesis Partners, conducted a comprehensive survey of 750 executives across 28 countries and 14 industries. All participants represented organizations with annual revenues of at least $250 million.

The cohort was designed to capture a balanced perspective, comprising 60% security and technology leaders and 40% business strategy and operations leaders.

- *Security and technology leaders* included CISOs/BISOs, CIOs/Heads of IT, CTOs/Heads of Technology Strategy, Chief Data Officers/Heads of Analytics, Chief Risk Officers, and VPs of R&D.
- *Business strategy and operations leaders* included CEOs, COOs/CSCOs/Heads of Operations, Chief Strategy Officers, Chief Innovation Officers, and business unit leaders.

The surveyed organizations were predominantly publicly owned (86%) and represented major sectors such as banking (10%), energy & utilities (9%), and industrial products (9%). The average annual revenue was $12.9 billion, with an average IT budget of 4% of revenue and an R&D budget of 1.5%.

How we derived the Quantum-Safe Readiness Index (QSRI)

To provide a more granular view of technical progression, a Quantum-Safe Readiness Index (QSRI) was calculated based on self-reported activity across the migration lifecycle.

The score measures an organization's self-assessed progress through three critical phases of a quantum-safe migration, based on 14 specific activities:

- *Discover.* In-depth analysis and planning activities, including performing analysis of cryptographic dependencies, establishing service levels, identifying foundational technologies, determining the extent of exposed data, working with aligned vendors, and taking inventory of applications and data.
- *Observe. O*ngoing governance activities, covering deploying telemetry solutions, using AI-based rules for decisioning, developing program-wide visibility, and implementing common governance mechanisms.
- *Transform.* Active transition activities, such as creating a transition plan, identifying supporting solutions, validating new products, and testing new NIST algorithms.

Methodological approach for readiness score

Responses for each activity on the 5-point scale were recoded to a 0-2.5 scale (1=0, 2=1, 3=1.5, 4=2, 5=2.5). This non-linear transformation served two primary purposes. First, it accurately established the "Not started" state as a true zero point, creating a meaningful baseline that denies credit for inactivity. Second, it intentionally models the increasing marginal effort required to advance through the later stages of the migration lifecycle. The smaller incremental gain between the scores for "Mostly

complete" (4=2) and "Fully complete" (5=2.5) reflects the greater effort and complexity inherent in the final stages of testing, validation, and optimization, compared to the foundational work of initial planning.

Following this recoding, the phase scores were calculated through a weighted aggregation process. Conversely, the scores for the Discover, Transform, and Observe phases were calculated as weighted components of the final composite score. The Discover score was derived by summing its six recoded variables divided by the maximum scores, then applying a weight of 0.5. The Observe score followed the same division for its four variables but carried a higher weight of 0.33, while the Transform score was the sum of its four variables divided by the maximum score then weighted at 0.17.

The overall Quantum Security Readiness Final score is the sum of the weighted Discover, Observe, and Transform scores, multiplied by 100, providing a percentage-based measure of an organization's progression through the technical migration journey.

Analytical framework: Quantum risk and response matrix

The core objective of this analysis was to develop a robust quantitative framework for assessing organizational postures towards quantum computing-enabled risks based on this global dataset. This was achieved by constructing two distinct composite indices: a Quantum Risk Exposure Metric, which quantifies an organization's susceptibility to quantum-related risks, and a Quantum Response Score, which measures its strategic and financial commitment to achieving quantum-safe security.

Prior to index construction, all raw variables underwent a standardized preprocessing phase to ensure methodological consistency. Key ordinal variables were reverse-coded so that a higher value consistently signifies a more negative outcome. This was applied to metrics where a high original score indicated strong performance or agreement, such as an organization's performance in IT resiliency and business continuity and cybersecurity compared to competitors, as well as agreement with the statement, "We have a crypto-agility program to transition to quantum-safe systems." After reverse coding, stronger disagreement or worse performance now yields a higher risk score. Furthermore, the annual revenue variable was transformed using the natural logarithm to correct for its skewed distribution and to model the diminishing marginal impact of organizational size. All continuous and Likert-scale variables were then converted to z-scores to place them on a common, unit-less scale for aggregation.

The **Quantum Risk Exposure Metric** was built as an additive composite of three standardized pillars, reflecting the cumulative nature of risk factors:

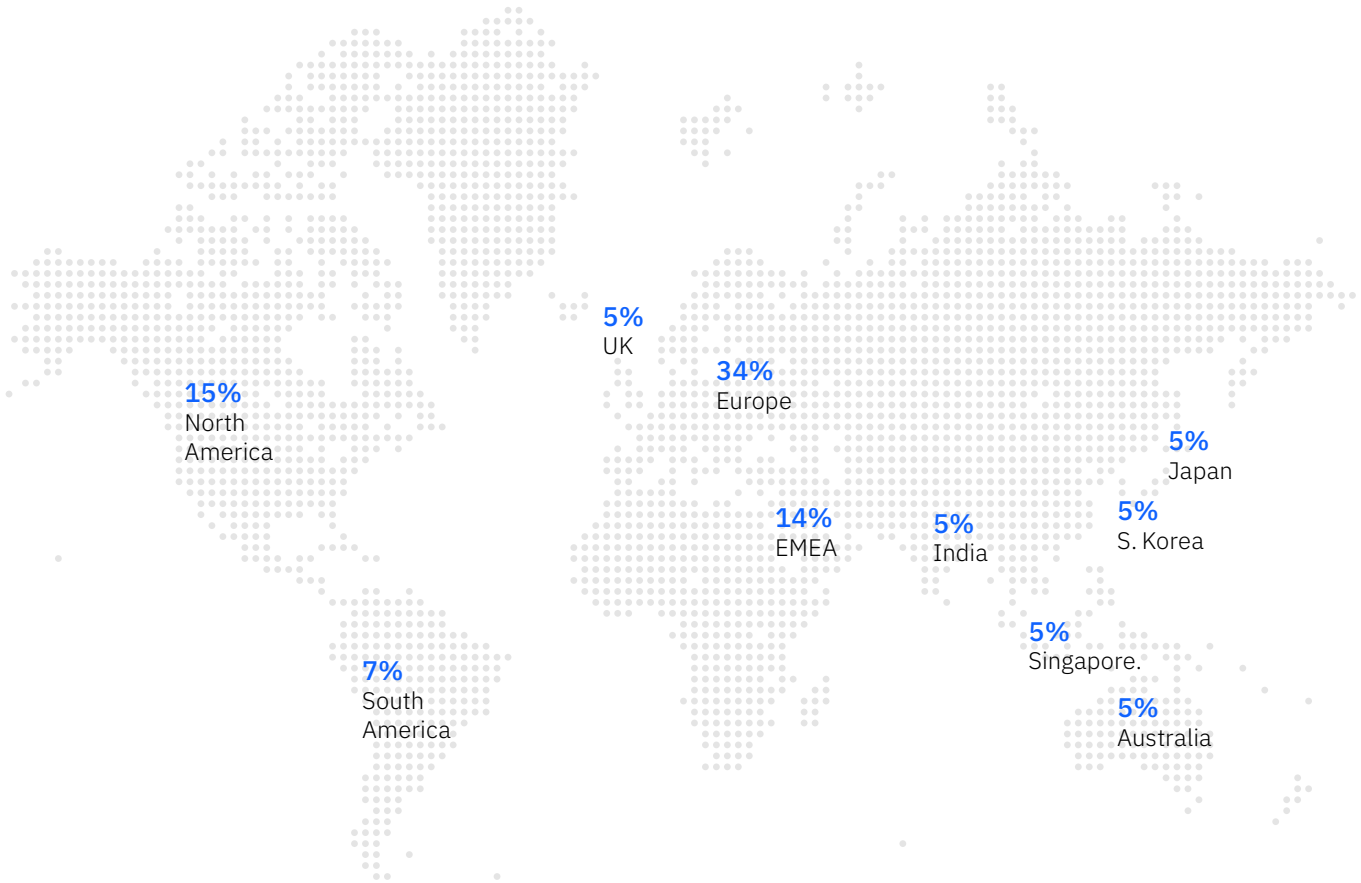
- *Exposure*. Combines a direct metric of quantum risk of data lifespan with reversed organizational performance in IT resiliency and business continuity.
- *Vulnerability*. Aggregates a measure of low investment (reverse-coded), a lack of a crypto-agility program, and the barrier posed by a "Lack of executive awareness or urgency."
- *Impact*. Combines the log-transformed revenue—where larger organizations face a greater potential impact—with reversed performance in cybersecurity and the current business challenge posed by cybersecurity.

The **Quantum Response Score**, in contrast, is calculated as the mean of two sub-indices, reflecting the necessity for a balanced approach between strategy and resources:

- *Strategy preparedness*. This sub-index averages four standardized variables that capture strategic maturity, including the proportion of the technology workforce needing reskilling, the resilience of legacy platforms and devices, an active crypto-agility program, and consortia fostering collaboration.
- *Resource commitment*. This sub-index is the mean of three financial commitment variables: the annual budget for IT, for Research and Development (both as a percentage of revenue), and the specific investment in quantum-safe transformation as a percentage of the cybersecurity budget.

For the core analysis, the cohort was refined to include only respondents actively engaged in quantum-safe planning. Within this group, a strategic typology was created by performing a median split on the two indices, classifying organizations into four distinct quadrants: Low Response/Low Risk, Low Response/High Risk, High Response/Low Risk, and High Response/High Risk. This grouping is designed to facilitate the identification of patterns and strategic needs specific to each segment.

Global representation



750	28	14
Senior executives	Countries	Industries

About the authors

Ray Harishankar

IBM Fellow & Vice President
linkedin.com/in/rayharishankar/
harishan@us.ibm.com

Ray is responsible for driving the overall strategy for IBM Quantum Safe product strategy and product engineering. Ray leverages the deep technical expertise of IBM in security services and post-quantum cryptography and pragmatically applies it with clients across insurance, banking, telecommunications, and government. Ray was nominated as an IBM Fellow in 2006 and holds 23 patents.

Gregg Barrow

Vice President & Global Offering Leader
Quantum Safe Transformation & Growth
linkedin.com/in/greggbarrow/
gbarrow@us.ibm.com

Gregg leads IBM's Quantum Safe transformation strategy, helping clients prepare applications and infrastructure for quantum computing's cybersecurity challenges. Previously, he managed IBM's Americas Security consulting and delivery services and built the Global Data and Application Security competency. Before IBM, he held senior roles at GE Capital, Cigna, Protiviti, and Citibank, with expertise in security, risk management, and leading global teams.

Antti Ropponen

Executive Partner, Quantum Safe Transformation and Cyber Defend Services Leader
IBM Consulting
linkedin.com/in/antti-ropponen/
Antti.Ropponen@ibm.com

In his current role, Antti drives cybersecurity strategy across data security, cryptography, and cloud protection. Since 2019, he has pioneered quantum-safe transformations, partnering with executives to implement cutting-edge solutions, scale global offerings, and help ensure organizational resilience against emerging threats. He has validated successes through dozens of quantum-safe programs across banking, telecommunications, insurance, and government sectors.

Veena Pureswaran

Research Director and Quantum Computing Leader
Senior Quantum Ambassador
IBM Institute for Business Value
linkedin.com/in/veenapureswaran/
vpures@us.ibm.com

In addition to her role with the IBM Institute for Business Value, Veena serves as a Senior Quantum Ambassador for IBM. Her research findings have influenced over 50 clients in industries ranging from electronics to financial services and she has presented at over 40 major conferences in Asia, Europe, and North America.

Gerald Parham

Global Research Leader, Security and CIO
IBM Institute for Business Value
linkedin.com/in/gerryparham
gparham@us.ibm.com

As a Global Research Leader at the IBM Institute for Business Value, Gerry's research spans quantum-safe cybersecurity, AI transformation, cyber risk management, and supply chain security. His research insights have appeared in publications such as *The Wall Street Journal, Forbes, CIO, Cyber,* and *Infosecurity Magazine*. Gerry's papers have been recognized as among the leading examples of thought leadership in the world.

Related reports

The quantum clock is ticking
The quantum clock is ticking: How quantum safe is your organization? IBM Institute for Business Value. May 2024.
ibm.co/quantum-safe

The Quantum Decade
The Quantum Decade: A playbook for achieving awareness, readiness, and advantage. Fourth edition. IBM Institute for Business Value. December 2023.
ibm.co/quantum-decade

Make quantum readiness real
Make quantum readiness real: Driving business utility with ecosystems, innovation, and talent. IBM Institute for Business Value.
December 2023.
ibm.co/quantum-readiness

Contributors

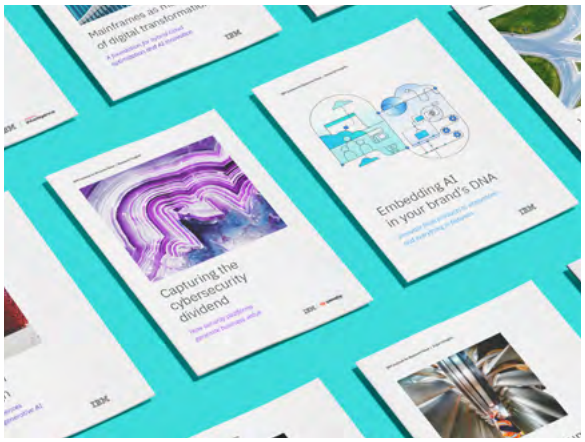
Jai Arun, Head of Product Management & Strategy, IBM Quantum Safe and Crypto-Agility Products, IBM Software; John Buselli, Offering Management, IBM Research; Kiran Subba Rao, Program Director, Product Marketing, Data Security Software, IBM Software; Zygmunt Lozinski, Senior Technical Staff, Quantum Safe Networks, IBM Research; Mark Hughes, Global Managing Partner Cybersecurity Services, IBM Consulting, Cybersecurity Services; Dimple Ahluwalia, Global Offering Leader, CyberDefend, IBM Consulting, Cybersecurity Services; Tim Van den Heede, Vice President Global Security Services Sales, IBM Consulting, Cybersecurity Services; Dinesh Nagarajan, Partner & Offering Leader—Data & AI, Quantum Safe, Application Security Services, IBM Consulting, Cybersecurity Services.

Chris Nay, IBM Quantum Communications Lead, IBM; Ray Shieh, Senior Product Marketing Manager—Quantum Safe, IBM; Jen Mack, Global Program Director, Quantum Safe Transformation Services, IBM Consulting.

Marisa Conway, Corporate Communications, IBM; Christine Selph, VP, Eminence, Thought-Leadership and Client Stories, IBM.

Jim Reavis, Co-founder and Chief Executive Officer, Cloud Security Alliance; Illena Armstrong, President, Cloud Security Alliance; Eileen Sciarra, Executive Vice President, Growth, Cloud Security Alliance.

And from the IBV IBV: Sara Aboulhosn, Associate Creative Director; Namit Agrawal, Managing Consultant; Heba Nashaat, Data and Content Management Manager; Lucy Sieger, Editorial Lead; Andrew Womack, Creative Director.



Subscribe to our IdeaWatch newsletter

Just the insights. At your fingertips. Delivered monthly.

Brought to you by the IBM Institute for Business Value, ranked #1 in thought leadership quality by Source Global Research for the second consecutive year.

Research-based thought leadership insights, data, and analysis to help you make smarter business decisions and more informed technology investments.

Subscribe now: ibm.co/ideawatch

Notes and sources

1. Soutar, Colin, Itan Barmes, and Filipe Beato. "Why the new NIST standards mean quantum cryptography may just have come of age." World Economic Forum. October 22, 2024. https://www.weforum.org/stories/2024/10/quantum-cryptography-nist-standards/

2. *Assured Cyber Security Consultancy for the Post-Quantum Cryptography Pilot Offering Standard.* UK National Cyber Security Centre. May 2025. https://www.ncsc.gov.uk/files/acsc-pqc-standard-v1-0.pdf

3. "Post-Quantum Cryptography Migration Blueprint for ASEAN CISOs." World Quantum Summit. July 26, 2025. https://wqs.events/post-quantum-cryptography-migration-blueprint-for-asean-cisos/

4. Harishankar, Ray, Dinesh Nagarajan, Dr. Walid Rjaibi, Gerald Parham, and Veena Pureswaran. *The quantum clock is ticking: How quantum safe is your organization?* IBM Institute for Business Value in partnership with GSMA. May 2024. https://ibm.co/quantum-safe

5. Ibid.

6. Ricci, Sara, Patrik Dobias, Lukas Malina, Jan Hajny, Petr Jedlicka, et al. "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography." IEEE Access. February 8, 2024. https://ieeexplore.ieee.org/document/10430098

7. Arun, Jai, Sukanta Bhattacharjee, Kyle Brown, James McGugan, and Biswajit Roy. "Empowering CIOs to accelerate crypto-agility with IBM Quantum Safe Explorer: IBM as client zero." August 18, 2025. https://www.ibm.com/new/product-blog/empowering-cios-to-accelerate-crypto-agility-with-ibm-quantum-safe-explorer

8. Harishankar, Ray, Michael Osborne, Jai S. Arun, John Buselli, and Jennifer Janechek. "Crypto-agility and quantum-safe readiness." IBM Quantum Research Blog. June 19, 2024. https://www.ibm.com/quantum/blog/crypto-agility

9. Susnjara, Stephanie and Ian Smalley. "What is quantum-safe cryptography?" IBM Think blog. September 4, 2024. https://www.ibm.com/think/topics/quantum-safe-cryptography

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | October 2025

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

Examples presented are illustrative only. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided.

1443d5f5af4f5316-USEN-02