Quantum-Safe
360 ALLIANCE

Digital Trust & Cybersecurity in the Era of Quantum Computing

Introducing the Quantum-Safe 360 Alliance

IBM Consulting
Antti Ropponen
Kevin Legge
Gregg Barrow

Thales
Blair Canavan
Rick Robinson
Jeff Miller

Keyfactor
Ted Shorter
Chris Hickman

Quantinuum
Nick VanDuyn
Roy Stephan

Executive Summary

We stand at the transformative frontier of quantum computing: unprecedented computational power that promises to revolutionize technology. It also poses a significant threat to today's encryption methods. It's time to transition to quantum-safe cryptographic protocols—an essential task that requires coordinated efforts, strategic foresight, and a commitment to collaboration across industries.

IBM Consulting

THALES

KEYFACTOR

QUANTINUUM

Enter the Quantum-Safe 360 Alliance:
a team of industry leaders with expertise spanning digital trust, cryptographic hardware and software, and cybersecurity best practices. Addressing the complex challenges posed by quantum computing is bigger than one enterprise, which is why the Alliance has pooled resources and knowledge to accelerate the development of a unified, collaborative, secure global transition to post-quantum cryptography (PQC).

Our mission is clear: to facilitate this global transition by promoting and empowering cryptographic agility. This foundational principle prepares organizations for a future in which threats evolve unpredictably and technological change is constant. Cryptographic agility—the ability to seamlessly adopt and integrate new encryption standards—is no longer a luxury, but a critical business imperative.

Why this collaborative approach?

Unparalleled expertise. Members bring deep proficiency in cryptographic design, development, deployment, and lifecycle management to guide partners through this transition.

Interoperable solutions. The Alliance fosters the development of cryptographic solutions that work cohesively across platforms and industries, easing implementation challenges.

Shared responsibility for a global problem. Addressing the risks posed by the future of quantum computing transcends individual organizations and sectors. A unified approach fosters trust, minimizes duplicative efforts, and accelerates the adoption of quantum-safe technologies.

The quantum era is not a distant future; it is rapidly approaching, and the time to act is now. Together, through collaboration and foresight, we can build a secure and resilient digital future.

The Quantum-Safe 360 Alliance brings together industry leaders with deep expertise in cryptography, quantum computing, and cybersecurity, each contributing unique strengths to the shared mission of facilitating the transition to quantum-safe cryptography.

IBM Consulting

IBM Consulting is a trusted, industry-recognized partner in post-quantum cryptography migration, empowering organizations to future-proof their operations through quantum-safe solutions, leveraging deep industry expertise, cutting-edge assets, and strong alliance connections.

IBM Consulting has extensive experience in cryptographic risk assessments and quantum-safe transformation that ensure secure and scalable solutions, protecting critical business operations and building customer trust.

IBM Consulting's advanced cryptographic discovery assets, hybrid solutions, and Gen AI-driven insights deliver accelerated transformation timelines and reduced operational risk.

IBM's collaboration with global standards bodies and industry alliances ensures alignment with emerging quantum-safe regulations and access to the latest advancements, benefiting customers with forward-looking solutions.

THALES

Thales is a data and application security leader who actively fosters a global, carefully vetted post-quantum cryptography ecosystem emphasizing interoperability and collaboration. Preparing for evolving threats is critical to providing trust, which is why at Thales, crypto-agility is at the heart of our quantum-ready solutions equipped with flexible, upgradeable technology.

Thales has actively collaborated on the design and review of PQC algorithms selected by NIST, reinforcing its commitment to shaping the future of secure cryptographic standards.

Thales Luna HSMs protect applications and cryptographic keys within a FIPS-validated, hardened, and tamper-resistant device.

The CipherTrust Data Security Platform further enhances cryptographic agility by centralizing policy management and enabling advanced techniques like data masking, tokenization, and encryption across multi-cloud environments.

KEYFACTOR

Keyfactor is a leader in public key infrastructure (PKI), certificate management, and code signing specializing in crypto-agility and post-quantum cryptography solutions.

Founded by expert practitioners as a PKI consultancy, Keyfactor has evolved into a comprehensive machine identity management platform.

Keyfactor Enterprise EJBCA supports modern PKI platforms by quickly scaling large volumes of certificates across various deployment models, while Keyfactor Command provides a centralized platform for machine identity management across the certificate landscape.

In 2024, Keyfactor **partnered with Quantinuum** to integrate their PKI platform with Quantum Origin to ensure high-quality keys using verified quantum entropy sources.

QUANTINUUM

Quantinuum is at the forefront of quantum computing innovation, building advanced quantum computers and leveraging their capabilities to counter quantum threats.

The company's Quantum Origin platform generates provable quantum randomness, enabling the strongest encryption possible by supporting the most advanced cryptographic algorithms.

This solution enhances cybersecurity systems through seamless integration across Windows, Linux, HSMs, cloud infrastructure, and IoT—all without requiring additional hardware or code changes. This enables rapid deployment and scaling within existing infrastructures.

Quantum Origin's proven quantum randomness strengthens key generation, setting new benchmarks for cryptographic security—as demonstrated through our integration with Thales Luna HSMs.

Together, the Quantum-Safe 360 Alliance exemplifies the power of collaboration by addressing a challenge too large for any single entity. We've combined our diverse capabilities to prepare our partners to navigate the quantum era with confidence and resilience.

The Quantum Threat: Why You Need Cryptographic Agility

It is not a question of if quantum computers capable of breaking encryption algorithms will arrive, but when. Projections suggest that such capabilities could emerge as soon as 2030, prompting leading bodies like NIST to establish 2030 as the deprecation deadline for widely used algorithms such as RSA and ECC.

This urgency is compounded by immediate "harvest now, decrypt later" (HNDL) attacks, where adversaries collect encrypted data today, waiting for quantum computers to break it tomorrow. Sensitive information—including personal, financial, and governmental data—is at risk without immediate action to secure it.

Quantum computing has the potential to quickly dismantle current encryption standards that are foundational to securing the digital world in which we work, putting everything from sensitive business data to personal privacy at risk. With quantum computers' ability to process vast amounts of data in parallel, they are capable of breaking current PKI standards by efficiently factoring the large prime numbers or solving the discrete logarithms that are the bedrock of modern cryptography systems.

The foundation of cryptographic security, randomness, is equally at risk. Weak or flawed randomness has already enabled devastating vulnerabilities, including Randstorm, Polynonce (leading to $25M in stolen Bitcoin), and Cisco ASA (exposing enterprise networks for nearly a decade). These weaknesses often persist undetected for years, compounding their impact.

Together, the risks of HNDL and randomness flaws demand immediate and proactive measures. Both are critical components of a quantum-safe future and must be addressed as part of any post-quantum cryptographic migration. Strengthening cryptographic agility—encompassing algorithms and randomness—is essential to secure sensitive data against these intertwined threats.

In this future state, relying on current cryptographic methods will no longer suffice. The only viable solution is cryptographic agility—the ability to swiftly adopt and implement quantum-safe cryptographic standards that can evolve and adapt to emerging challenges.

To prepare for the hurricane before it makes landfall, the transition to quantum-safe methods must begin now.

What is Crypto-Agility?

Crypto-agility is an organization's ability to adapt cryptographic solutions or algorithms quickly and efficiently in response to emerging threats and technological advances. It is both a measure of preparedness and a design principle for updating, replacing, and adapting cryptographic systems with minimal disruption to operations and architecture.

As defined by FS-ISAC, crypto-agility involves implementing, updating, and adapting cryptographic solutions and policies with no significant architectural changes, minimal operational disruption, and rapid transition times. This is essential in a world where quantum computing (and potentially other specialized computational threats) challenge the integrity of encryption.

Post-quantum cryptography (PQC) represents the next evolution of secure encryption. It combines cryptographic resilience through proven randomness, quantum-resilient algorithms, and flexibility. Quantinuum Senior Solutions Architect Roy Stephan says crypto-agility is the ability to respond to encryption threats quickly. "PQC is an example of just one type of threat," he says. "Solutions should be designed to withstand an unbounded attacker regardless of the mechanism they are currently using."

The Stakes of Inaction

If the 10-year shift from SHA-1 to SHA-2 is any indication, the migration to quantum-safe cryptography will be a multi-year process for most enterprises. And true quantum readiness is much more than just new algorithms—it encompasses agility in infrastructure, key management, and application design. Future threats could combine quantum computing and AI to break encryptions, making real-time responses indispensable.

It is clear to the Quantum-Safe 360 Alliance that organizations must embrace cryptographic agility to navigate the unknowns of the future. Prioritizing adaptability enables resilience both against quantum threats and an evolving landscape of cybersecurity challenges.

> Crypto-agility is the ability to respond to encryption threats quickly. PQC is an example of just one type of threat. Solutions should be designed to withstand an unbounded attacker regardless of the mechanism they are currently using.
>
> *- Quantinuum Senior Solutions Architect, Roy Stephan*

Frameworks: How To Think About Your PQC Journey

Preparing for a quantum-safe future requires a comprehensive framework, similar to the philosophical approach of zero trust. Post-Quantum Cryptography (PQC) is not a standalone product but a systematic approach to building and maintaining cryptographic resilience across an organization's infrastructure.

Insights gathered **from more than 200 global IT leaders** reveal that organizations are beginning to recognize the importance of a quantum-safe cryptographic infrastructure.

However, true preparedness requires a holistic approach: addressing every element of cryptographic implementation, from data ingress to storage.

Partially investing in PQC solutions but continuing to rely on outdated algorithms like RSA-protected cloud backups would leave critical gaps in security—and likely be exploited by quantum-capable computers.

Case Study: Building Quantum-Safe Operations

THE CHALLENGE

A multinational financial services company sought to proactively establish robust technical solutions to secure the data, systems, and applications relied upon by its customers.

Facing the challenges presented by legacy hardware, system-wide applications, and certificates from multiple vendors, the organization required a quantum-safe solution that could seamlessly integrate into its existing IT environment with minimal disruption.

Their goal: to develop a scalable, agile PQC approach to protect against data harvesting threats while maintaining enterprise-wide adaptability.

THE SOLUTION

Collaboration with Quantinuum and Thales empowered this company to implement a quantum-safe solution for secure key generation, management, and protection. Quantinuum's Quantum Origin solution provides a software quantum random number generator (QRNG) to generate unpredictable keys. Unlike today's random number generators that rely on statistical testing, Quantum Origin's mathematically verified processes ensure near-perfect randomness.

Thales Luna Hardware Security Models (HSMs) are used to protect these cryptographic keys both physically and logically, offering crypto-agile flexibility and designed for seamless deployment across diverse environments. With these HSMs, cryptographic keys never leave the device, providing robust protection and locating all cryptographic operations within the HSM.

For further fortification against quantum threats, Quantinuum's Quantum Origin seeds Quantum-enhanced entropy into the HSM's Deterministic Random Bit Generator (DRBG), empowering the Luna HSM to directly generate quantum-computing-hardened cryptographic keys.

In addition, PKI integrates these quantum-safe digital certificates and keys properly into the organization's overall security architecture. Issuing quantum-safe certificates for authentication, encryption, and data integrity protects the entire ecosystem from quantum decryption threats.

This is just one example of the value of holistic post-quantum preparation guided by the expertise and skills of the Quantum-Safe 360 Alliance members. Integrating advanced technologies with proven infrastructure empowers your organization to safeguard operations against emerging threats while maintaining operational continuity.

Beginning the Journey to Quantum Safety

The advancements of quantum computing promise to render our current cryptographic standards obsolete. The implications of this sea change are profound, with catastrophic ripple effects threatening the integrity of enterprise systems, critical infrastructure, and digital trust.

Addressing this challenge requires a monumental effort comparable to replacing all the rivets, nuts, bolts, and welds in a massive ship—a task essential to prevent the vessel from rusting apart. A similar transition to post-quantum cryptography is fundamental to maintaining secure and resilient operations.

A Roadmap to Agile Cryptographic Security

Transitioning to a crypto-agile posture is a complex endeavor, but with a structured approach, organizations can mitigate risk and prepare for a quantum-safe future. Here are our suggestions for enterprises wondering how to begin:

1. Discovery and Prioritization

The first step is understanding the scope of the quantum threat and your organization's assets. A thorough assessment includes:

Evaluating the threat landscape.

Quantify the risk quantum computing poses to your existing cryptographic systems and identify timelines for potential vulnerabilities.

Assess randomness sources.

Take stock of the sources of randomness your assets use to generate cryptographic keys. Evaluate legacy randomness sources that can be strengthened with proven entropy.

Asset inventory and risk valuation.

Map out all affected assets and prioritize them based on data sensitivity and lifecycle. For example, data that remains critical and sensitive beyond 2030 should be secured first, while data with shorter lifespans may not need immediate quantum-safe measures.

Lifecycle considerations.

Focus initial efforts on long-lived and high-value data, such as financial records, intellectual property, and personally identifiable information (PII) that could be exploited even years after being stolen.

2. Incremental Implementation

A gradual, phased approach is essential for transitioning to PQC without disrupting ongoing operations. Our suggestions for an incremental implementation process:

Testing and staging.

Begin with small-scale tests and pilot projects to validate PQC solutions in controlled environments, including opportunities to strengthen randomness and improve the cryptographic ecosystem. Use these learnings to refine implementation strategies, evaluating them for efficiency and effectiveness.

Iterative deployment.

Address known risks in stages, integrating PQC into existing IT processes while minimizing disruptions. Build flexibility and adaptability into the deployment by focusing on modular updates, improving with each iteration.

Continuous monitoring and improvement.

Regularly evaluate the effectiveness of deployed solutions and adjust strategies to respond to evolving threats and technological advancements.

3. Leverage Alliance Expertise for a Seamless Transition

The Quantum-Safe 360 Alliance brings together market-ready solutions and deep expertise to facilitate an agile and secure PQC transition. Equipped with combined tools and strategies designed to address the specific needs of diverse industries, alliance members can help your organization:

Implement quantum-safe cryptographic algorithms.

Securely manage and protect data throughout its lifecycle.

Maintain operational continuity while addressing emerging threats.

Case Study: Application Modernization with Cryptographic Agility

Thales supports a large financial services organization in leveraging existing application modernization workstreams to introduce a series of crypto-agile pilots. The organization recognizes that managing Post-Quantum Cryptography (PQC) risks requires cryptographic agility, particularly across an evolving application portfolio. They sought to ensure that cryptographic operations were abstracted from application logic, allowing algorithms to be changed and tested at scale for various reasons—such as security, performance, or compliance—with minimal cost and disruption.

The objectives for the pilot included establishing cryptographically agile application data protection and key management services that are both easy for DevOps to consume and easy for Security teams to govern.

Thales collaborated with both stakeholder groups to design and architect a catalog of highly scalable, API-driven microservices based on defined architecture patterns and application profiles. Additionally, the pilot services are required to meet the organization's stringent resiliency, performance, and regulatory requirements.

Key capabilities and technologies utilized included:

- Application data protection services using Thales CipherTrust RESTful Data Protection (CRDP) and Data Protection Gateway (DPG)
- Container level data protection and access controls services using CipherTrust Transparent Encryption for Kubernetes
- Key Lifecycle Management services using Thales CipherTrust and CipherTrust Cloud Key Manager
- Key Generation, Storage, and Cryptographic Operations using Thales Luna HSM
- Automation and Orchestration using Terraform and Ansible

Common Challenges to Organizational Buy-In for Cryptographic Agility

The truth is, you may be fully aware of the potential ramifications of ignoring or postponing your organization's transition to post-quantum cryptography. If you face challenges with internal buy-in for PQC, you're not alone. We've found a few common hurdles—many of which may be overcome by clearly communicating the stakes of imminent technology.

Awareness vs. Action

Many organizations are still grappling with foundational questions like, "How do I get started?" and, "When should I act?" This hesitation occurs despite the clear and present reality of "harvest now, decrypt later" attacks.

Threat actors are exploiting weak randomness and classic key attacks today, targeting data with long lifecycles (such as SSNs) that can be decrypted when quantum capabilities become viable. Delaying action only increases exposure to these risks.

Myths and Misconceptions

Misunderstandings about the quantum computing timeline and the nature of PQC can hinder progress, as well. Common myths:

- **"Q-Day is 2030, so we have time."** While 2030 is often cited as the quantum readiness deadline, organizations should not wait until the last minute to act. The complexity of transitioning to PQC demands years of preparation.
- **"The risks aren't so great; it'll all work out."** You don't want to be caught out when the zero-day for quantum comes. The shift to quantum-resilient cryptography is unavoidable. Quantum computing technology will significantly impact global standards and protocols. Early adoption is critical to risk mitigation and maintaining compliance as regulations evolve in kind.

Leadership Disconnect and Organizational Challenges

While CIOs and CISOs are becoming increasingly aware of PQC priorities, there is often a disconnect between technical teams and budgetary decision-makers. Reaching agreement between these stakeholders requires long-term commitment, as PQC preparation spans years and demands investments in hardware, software, and operational processes. Quantum-safe transformation is a strategic, organization-wide initiative that requires executive leadership to align strategy, enhance procurement practices, update governance, and foster agility to maintain business resilience and security in the face of future quantum risks.

Additionally, industries like finance, defense, government, and telecommunications are leading PQC adoption, while retail and local governments lag behind. Organizations in these slower-moving sectors face the challenge of catching up to avoid vulnerabilities.

Maintaining PQC Over Time

Sustainability is another key organizational concern. Gone are the days of a “set it and forget it” cryptographic solution; instead, PQC requires continuous monitoring, patching, and updates by a skilled workforce. Enterprises beginning their crypto-agility journey must approach PQC as an evolving process, similar to other contemporary security options (such as SOC tuning).

Operational and Technical Challenges

The technical complexity of transitioning to post-quantum cryptography presents significant hurdles. Lack of centralized visibility over current cryptographic assets makes it difficult for organizations to maintain a comprehensive inventory, hindering planning efforts or posing surprise problems during implementation.

Legacy systems, constrained Internet of Things (IoT) devices, and outdated hardware often struggle to support the computational demands of PQC—and the combination of larger key sizes and longer handshake times can introduce performance challenges for even the most advanced tech stack.

Strength Imperatives for Success

In the face of these challenges, our guidance is to build the road to crypto-agility one brick at a time. Follow these strategic imperatives:

1. **Start Now**

   Early adopters gain the opportunity to shape regulations, establish best practices, and lead their industries.

2. **Centralize Planning**

   Establish centers of excellence to coordinate PQC transition efforts. Leverage alliances like Quantum-Safe 360 to share resources, expertise, and scalable solutions.

3. **Build Expertise**

   Address the knowledge gap by investing in skilled practitioners and experienced leaders to drive PQC migration efforts.

4. **Plan Iterative Implementation**

   Itterative implementation is much more than a buzzword for strategy. Breaking the transition into manageable phases is essential to addressing the immediate risks first while planning for long-term adaptability.

Tackling these challenges head-on and committing to a structured transition makes it possible for organizations to build a secure, quantum-resilient future while minimizing disruptions to your current operations.

Tips and Tools for Starting Now

Viable quantum computing could arrive in less than five years, which means time is a precious commodity for security practitioners. When quantum computers achieve the ultimate cryptographic breakthrough, the resulting vulnerabilities could trigger unprecedented data theft risks and economic consequences, **potentially leading to the largest transfer of wealth in recorded history.**

Organizations must invest in foundational systems and practices to achieve cryptographic agility, according to Chris Hickman, Chief Security Officer at Keyfactor. "We have a responsibility to get it right the first time," he says. "The biggest risk is sitting around, waiting." To that end, the Quantum-Safe 360 Alliance offers market-ready solutions for enterprises at every stage of quantum resilience.

Strategy

IBM Consulting offers end-to-end consulting services to guide organizations through the entire quantum-safe transformation journey. From identifying quantum-related risks and conducting cryptographic discovery to designing roadmaps, implementing procurement and supply chain strategies, and embedding crypto-agility practices, our approach ensures secure, scalable, and sustainable transitions tailored to industry-specific needs. We also focus on organizational change management to embed quantum-safe principles across all levels of the business.

- Proprietary cryptographic discovery assets, such as IBM Quantum Safe Explorer, remediation playbooks, and Gen AI-powered analysis to accelerate risk assessments, pinpoint vulnerabilities, and tailor targeted solutions
- Frameworks and processes to ensure all new IT initiatives, vendor engagements, and software supply chains align with quantum-safe principles, preventing future risks
- End-to-end services, from technical migrations and remediation efforts to organizational change management, enabling long-term crypto-agility and quantum resilience.

PKI

As an industry leader for PKI solutions, Keyfactor emphasizes the importance of centralized certificate lifecycle management, encryption and key management, and crypto-agile development practices.

- Enterprises can explore the Keyfactor PQC Lab for tools and resources to visualize and test quantum-safe protocols before implementation.

Key Management

Paired with Thales' crypto agile solutions like CipherTrust, Luna HSMs, or High Speed Encryptors, organizations can become quantum ready with:

- Application Protection as an API-driven encryption microservice
- Centralized, automated Enterprise and Cloud Key Management with hybrid-certificate support
- Key generation and storage
- High performance data-in-motion encryption
- Thales offers the Post-Quantum Crypto-Agility Risk Assessment Tool for assessing PQC readiness and identifying vulnerabilities, enabling organizations to see what needs improvement first.

Randomness

Quantinuum is advancing the development of quantum-safe cryptographic solutions that integrate quantum technology to enhance security and resilience against emerging threats.

- Quantum Origin is the first quantum random number generator of its kind. Read the technical whitepaper for a comprehensive understanding of why unpredictable proven randomness enhances security.
- Quantinuum's solutions are designed to integrate into existing infrastructures and future-proof customer security systems in preparation for the quantum era.

These foundational investments create a resilient infrastructure capable of adapting to emerging cryptographic challenges, setting your organization up for success defending against new tools and tech.

Resourcing: The Investment in Quantum Safety

Achieving quantum safety doesn't have to overwhelm resources. A phased, incremental approach allows organizations to make manageable changes that compound over time to build agility. This layered strategy makes it possible to strengthen keys and algorithms for critical safety while steadily progressing towards a fully quantum-resilient infrastructure.

Resources like the **Open Quantum Safe** project offer affordable tools to identify assets, assess cryptographic agility, and plan effective remediation strategies, so your organization can begin their quantum-safe journey with low cost and reap the benefits of early adoption.

The members of the Quantum-Safe 360 Alliance stand ready to support organizations through this complex journey. We are dedicated to offering trusted partnerships—including staff augmentation to meet a tight quantum readiness timeline—and making the transition to PQC manageable, sharing responsibility and building cryptographic agility worldwide.

Leveraging the combined resources of the alliance empowers businesses like yours to secure critical assets and prepare for the post-quantum future with confidence.

A Quick Win

Driving vendor accountability is a critical step. Your organization's procurement power is a key tool for demanding quantum readiness from vendors, accelerating industry-wide adoption of quantum-safe tools and technology. Key questions to ask your data partners:

When will your solutions meet PQC standards?

How quickly can these solutions be deployed within our systems?

What quantum-safe practices do you currently use, if any?

Holding vendors to these expectations forces external partners to align with internal security goals, fostering a collaborative ecosystem for quantum resilience. After the considerable investment of time and resources into your own organization's crypto-agility, the last thing you need is a third-party lacking quantum-safe practices providing a revolving door for attackers.

Key Takeaways

The advent of quantum computing represents a pivotal moment in the evolution of technology and cybersecurity. Its unprecedented computational power heralds transformative potential—accompanied by profound risks for the cryptographic systems underpinning our digital world. **The urgency to act cannot be overstated: The time to begin preparing for quantum resilience is now.**

The Quantum-Safe 360 Alliance has emerged as a beacon of collaborative strength, bringing together industry leaders with unparalleled expertise to address this challenge. Our mission is to guide organizations to secure their data, infrastructure, and operations against the looming quantum threat by fostering cryptographic agility and leveraging cutting-edge technologies.

This collaborative approach is key—organizations do not need to navigate the complexities of transitioning to post-quantum cryptography alone.

Through structured methods, phased implementation, and incremental progress, your organization can embark on the journey to quantum safety without overwhelming resources. Investing in foundational systems, demanding vendor accountability, and leveraging the expertise of trusted partners are critical steps towards achieving a secure, agile, and resilient digital future.

There's no denying the stakes are high: **a quantum breakthrough could very well trigger a seismic shift in cybersecurity.** Understanding the problem is the first step. Now it's time to take decisive action to mitigate the risks of financial, operational, and reputational consequences—and position your business as a leader in the new quantum era.

Together, through foresight, collaboration, and innovation, we can build a future where digital trust thrives in the face of quantum advancements.

Let the journey to quantum safety begin.

Quantum-Safe
360 ALLIANCE