quantum safe technology

# managing risks and opportunities for quantum safe development

Version 1.0

Published on 31 January 2024


**Authors**

Dr Hoon Wei Lim, NCS
John Buselli, IBM

# Executive summary

In today's rapidly evolving digital landscape, the emergence of quantum computing presents both a challenge and an opportunity. Businesses that fail to prepare for quantum-safe security may face significant risks, including data breaches and a loss of competitive edge. This summary highlights the essential steps and benefits of transitioning to quantum-safe practices, ensuring your business remains secure, competitive, and future-proof.

Our world depends on digital infrastructure and digital communications – all of which inherently rely on cryptography to ensure trust. Cryptographic technologies are used throughout government and enterprises across a variety of industries to authenticate the source and protect the confidentiality and integrity of information that we communicate and store. Cryptographic technologies include a broad range of protocols, schemes, and infrastructures.

This trust is at risk as asymmetric cryptography is likely to be broken when a Cryptographically Relevant Quantum Computer (CRQC) becomes available. This risk extends to symmetric cryptography, which is not directly impacted, but will require new strategies for mitigation as well.  As quantum computing advances, organisations face the need to protect their sensitive data from potential vulnerabilities.

Developing quantum safe encryption capabilities is crucial to maintaining cybersecurity and integrity for critical applications and data. The quantum computing era will unfold over time, but the need for quantum-safe solutions is immediate. In fact, both the historic and current complexity of crypto systems—even pre-quantum computing—can require several years of strategic planning, preparation, and remediation. Business, technology, and security leaders face an urgent need to develop a quantum-safe strategy and quantum-computing roadmap now.

**The IT landscape has become increasingly complex over the years. This landscape is composed of many components including internally developed digital applications, IT capabilities inherited through acquisitions, third party software products, services consumed from cloud providers and consumption of SaaS capabilities. The scope of technology that organisations need to upgrade to become Quantum Safe or remediated to use Quantum Safe cryptography is significant. As a result, it is not unreasonable to anticipate several years of effort for an enterprise to become Quantum Safe.**

Developing quantum-safe cryptography capabilities is crucial to maintaining data security and integrity for critical applications. This includes developing and applying cryptographic agility approaches to switch between multiple cryptographic primitives without making any major changes to infrastructure and ensure a rapid response to any cryptographic threat.

Cryptographic agility requires more than just an inventory but by having the relevant information at the right time in the right place with the right governance. A programmatic and iterative Quantum Safe programme provides a structured approach to implement quantum-safe solutions while collaborating with stakeholders, adapting to emerging threats, and continuously improving security measures.

## Planning for quantum safe

The scope of what needs to be upgraded to be quantum safe or remediated to use post-quantum cryptography (PQC) is significant. This journey must be well planned and incrementally executed based on business and technical priorities and several other critical considerations. The following provides an overview of critical next steps to consider on the journey to quantum safe:

1. **Inventory cryptography usage:**
   The first step is to ensure that a comprehensive view of cryptography usage across the organisation is in place. This is achieved by developing an inventory of both the static and dynamic view of cryptography usage. Scanning of cryptography usage in custom applications used within an organisation provides a static view and scanning networks for cryptography calls provides a dynamic view of cryptography usage. This comprehensive inventory of cryptography usage is best represented in a standard form, such as, a Cryptography Bill of Material (CBOM).

2. **Identify and prioritise crown jewels:**
   Having a comprehensive inventory is necessary but not very useful from a planning perspective. It is critical that the crown jewels, i.e., the most critical data and assets of your organisation, are identified and safeguarded first. This is achieved by classifying the various assets within the organisation and using these as filters to prioritise and plan. This classification and selection must consider both technical and business perspectives. This prioritised view should be used to develop a transformation plan or roadmap.

3. **Develop a transformation roadmap:**
   It is not possible to transform all the applications and systems in one massive initiative. This must be broken into several phases with each phase building on the collective experiences and capabilities of the previous phase. Developing such an incremental transformation roadmap is a very important step and must be done with great thought and depth of understanding of the challenges involved. This is typically a transformation that should start small, learn from each iteration, build reusable components, establish comprehensive transformation approaches, and be executed diligently and over several years. The scope of the transformation must include systems within the control of the organisation as well as ensuring that appropriate external or third-party entities that integrate also complete their transformation.

4. **Begin transformation to become quantum safe:**
   Having developed an actionable transformation roadmap – beginning to execute to that plan is the next step. The transformation journey will typically take several years. Given this duration, it is important that the transformation roadmap be periodically validated with the learnings from the ongoing transformation as well as other environmental considerations and changes and adjusted accordingly. One key aspect of this

transformation step is ensuring that crypto agility is part of the transformation. Ensuring that future cryptography related changes do not require core changes to the application is what is typically referred to as crypto agility. This enables ease of transition from one post-quantum cryptography algorithm to another in the future – should the need arise. Therefore, activities must include enabling crypto agility as part of the transformation.

Another key aspect of the transformation step is to not assume that the effort is one of replacing old cryptography with the new post-quantum cryptography. While this is indeed one approach – it is not the most efficient or effective way. Identifying the appropriate remediation approach or pattern for transforming an application or system is important. It is very likely that organisations with a lot of applications typically can establish and use multiple patterns repeatedly across their IT landscape.

5. **Gain familiarity and expertise in the use of new algorithms:**
An activity that must be undertaken right from the start and be executed in parallel to the previously enumerated steps is to establish a credible level of competency in judicious application of post-quantum cryptography. The new post-quantum cryptography algorithms are quite complex and quite different from existing algorithms. Understanding the appropriate usage of the algorithms, their performance profile, resource consumption characteristics, etc. are very important.

   This is accomplished by establishing a center of excellence, identifying dedicated cryptographic engineers, security architects, etc. and providing them an environment and an opportunity to experiment and learn Having a sandbox to test the new algorithms in the organisation's context is very important.  Executing several targeted pilot projects to learn from is important.

# Recent developments in quantum computing

The world is on the cusp of another computer revolution. It will be driven by the convergence of powerful technologies: high-performance computing, AI, and quantum computing. Quantum computing is not simply a faster way of doing what today's computers do – it is a fundamentally different approach that promises to solve problems that classical computing can never realistically solve. It holds the promise to help humanity confront important challenges, from solving long-standing questions in science to overcoming obstacles in  improving industrial efficiency. Working in conjunction with classical computers and cloud-based architectures, quantum computers could even be the answer to problems we haven't yet dreamed of. The opportunities for society and the economy are potentially limitless.

In the case of quantum computing, the theme of the past few decades has been the emergence and establishment of this new technology. The community is focused on laying the groundwork: experimenting with quantum hardware, devising use cases, and educating people on how to use quantum computers, while running experiments benchmarking devices. IBM made quantum computing real.

Earlier this year, a new paper from IBM and UC Berkeley shows a path toward useful quantum computing. Read here for new insights into how we demonstrated that quantum computers could run circuits beyond the reach of brute-force classical simulations. For the first time, IBM has hardware and software capable of executing quantum circuits with no known a priori answer at a scale of 100 qubits and 3,000 gates. Quantum is now a computational tool, and what makes us most excited is that we can start to advance science in fields beyond quantum computing, itself.  It is clear that a heterogeneous computing architecture consisting of scalable and parallel circuit execution and advanced classical computation is required. This has culminated in IBM's vision for high-performance systems for the future: quantum-centric supercomputing: IBM Debuts Next-Generation Quantum Processor & IBM Quantum System Two, Extends Roadmap to Advance Era of Quantum Utility

# The quantum threat

The security of most standard algorithms relies on extremely difficult mathematical problems that take years to solve with current computers. Modern public-key encryption protocols are satisfactory for protecting against most technological tools at the disposal of today's threat actors. However, that won't last. Quantum computers will be capable of breaking these math-based systems in a matter of seconds. In addition, threat actors are now harvesting large quantities of encrypted data and storing it until they can break the encryption keys using quantum computing. Data that is encrypted today is vulnerable to decryption tomorrow.

> **"Quantum computers promise transformative powers for businesses and organisations across the globe and through a diverse range of industries. However, they also introduce significant risks to the current digital economy. In the near future, sufficiently powerful and commercially available quantum computers will undermine current cryptographic standards protecting most digital communications and vast amounts of sensitive data."**
>
> ***Quantum Readiness Toolkit: Building a Quantum-Secure Economy, World Economic Forum, 2023*** [1]

When large-scale quantum computers are built, they will be capable of breaking many of the current public-key cryptography systems. Global funding for quantum computing startups increased by 13.5% last year, to $1.1 billion. According to McKinsey China plans to invest $15.3 billion in the industry, and the European Union has set aside $7.2 billion for investment. Without significant preparation for moving to post-quantum cryptography, quantum computers in the wrong hands would significantly compromise the privacy and security of the digital communications which the world increasingly relies on.

To illustrate the quantum threat, imagine a vault with a lock that takes a conventional computer centuries to crack. Quantum computing, however, could unlock it in mere hours.

1 https://www3.weforum.org/docs/WEF_Quantum_Readiness_Toolkit_2023.pdf

# Why start preparing now?

The question of when cryptography will be broken by quantum computing is unfortunate, for it implicitly frames the threat to be sometime in the future. The threat is today. The impact is in the future. Data that is considered securely protected today is already lost to a future quantum adversary if stolen or harvested. All data, past, present, and future that is not protected using quantum-safe security will be at risk, and the longer we postpone the migration to quantum-safe standards, the more data there is that will be at risk.

Our experience makes it clear that there will not be a one-size-fits-all strategy when it comes to migrating to quantum safe schemes. Given the long-term nature of the threat and the dynamic environment surrounding quantum computing, it is also clear that a cryptographic strategy needs to consider multiple time frames and needs to deal with potential step improvements in quantum technology development. Governments have a role to play here too. To supplement the private industry's engagement in standards development, governments need to accelerate investments in, and promote the adoption of quantum-safe cryptographic schemes that can safeguard data now and long into the future.

The threat of Cryptographically Relevant Quantum Computers (CRQC) is significant, but the timeline for when this will happen is unknown. How can an organisation quantify the risk of a Cryptographically Relevant Quantum Computer (CRQC) when they don't yet exist? The immediate best practice suggests creating several scenarios on the risk a quantum threat to a specific asset, with some of these scenarios being "more likely" than others.

The argument for starting now, to address the threat that quantum computers will pose to existing security systems, is based on the following considerations:

- Cryptographic technologies are integrated into most of the digital products commonly used by organisations to run their daily operations.
- Some of the applications and systems used within energy, transportation, finance, and government infrastructures have product lifetimes of 15 - 30 years, and even longer requirements for data protection and privacy.
- The time needed to migrate installed cryptographic technologies (e.g., SHA1) to something newer can take many years.
- The number of cryptographic systems that organisations will need to migrate to use new "quantum-safe" cryptography will be large.
- Most organisations have no clear view of the cryptographic technologies used in IT operations and this will make it difficult to discover and then prioritise the systems to be upgraded to post-quantum cryptography.

# Guiding principles for preparing a quantum safe journey

The World Economic Forum (WEF) recently published a set of guiding principles to become quantum cyber-ready [WEF23]. These provide practical guidance for organisations to prepare for the quantum-secure economy. They also highlight the importance of a cohesive, global and cross-border approach to governing quantum risk involving business stakeholders and experts from business, government, regulators and academic institutions. However, organisations vary in size, industry, and maturity. There is no single approach or strategy that serves as a one-size-fits-all solution. We outline here five key guiding principles that any organisation may consider as they start preparing for their transition to quantum safe security.

## Look beyond quantum computing development timeframe

In contemplating the potential impact of quantum computing on our digital landscape, it is crucial to adopt a forward-thinking perspective that extends beyond its current developmental stage. Quantum computing holds transformative potential, yet remains an active area of research, with scientists exploring more reliable and scalable methods. Precisely predicting when quantum computers could break existing encryption proves challenging. Strategic preparation efforts should be decoupled from specific development timelines. Relying solely on projected quantum computing evolution can create a false sense of security. Instead, organisations must focus on building a robust cybersecurity foundation with quantum-resistant algorithms, irrespective of the uncertain quantum computer arrival. This approach involves developing cryptographic strategies resilient to time, embracing post-quantum cryptography (PQC), and enhancing security continually. By fostering adaptability and resilience, organisations can proactively secure digital assets in the face of evolving quantum computing landscapes.

## Understand where you are now

Preparing for the imminent era of quantum computing requires organisations to proactively strengthen their cybersecurity defences. A foundational step in this process is conducting a thorough cryptography inventory and assessment, especially crucial for entities safeguarding data requiring prolonged protection. Scrutinising cryptographic infrastructure allows organisations to identify vulnerabilities and bolster defences against quantum computing threats. The preparatory phase involves identifying assets and systems reliant on cryptography, emphasising vulnerable algorithms like RSA and ECC. Prioritisation is critical. Organisations should categorise systems based on data criticality to strategically allocate resources. Evaluating the potential impact of transitioning to quantum-resistant algorithms ensures a seamless integration without compromising operational efficiency, enhancing overall cyber resilience.  This proactive approach positions organisations to navigate the challenges posed by quantum computing effectively.

## Put in place a governance framework

Establishing quantum-safe security demands a meticulous approach and a robust governance structure, necessitating the active involvement of senior executives. A dedicated governance team oversees the entire process, ensuring alignment with organisational goals. This involves developing a quantum-safe roadmap, synchronised with

quantum risk assessments and the organisation's risk appetite. Moreover, integrating quantum risk into the existing cybersecurity operating model fortifies defences against emerging threats. Designating cryptographic champions within the organisation helps socialise the impact of quantum risk and drives the implementation of quantum security plans. In essence, effective governance forms the foundation for successful quantum security projects, instituting robust structures and mandates that ensure clear direction and accountability throughout the quantum-safe transition.

## Hybrid approach

In enhancing cybersecurity against the uncertainties introduced by quantum computing, a prudent and conservative approach is essential. We advocate for a strategy that embraces a hybrid approach, strategically combining classical and quantum-safe cryptographic algorithms. Nuanced strategy recognises that today's quantum-safe algorithms may encounter future challenges from computing advancements or unforeseen weaknesses as has often been the case throughout the history of cryptography.  By adopting a multi-layered defence mechanism through a hybrid approach, , not relying solely on the resilience of a single cryptographic algorithm, organisations aim to fortify their security posture.  This may involve combining classical and quantum-safe algorithms or integrating multiple quantum-safe algorithms with distinct properties. This forward-looking strategy emphasises adaptability and robustness in the evolving cybersecurity landscape, reflecting a commitment to proactive security measures with diversity and redundancy at its core.

## Continuous capability development

In the pursuit of quantum-safe security, continuous capability development is crucial for organisations aiming for a proactive and adaptive transition. This involves conducting small-scale pilots to validate PQC solutions in real-world scenarios, assessing performance, compatibility, and integration challenges. These pilots yield valuable data and feedback, informing and enhancing the overall migration strategy. Simultaneously, employee education plays a central role, raising awareness about quantum computing risks and the necessity for migration. Training programmes empower the workforce with knowledge and skills to securely use and manage quantum-safe systems, fostering a culture of cybersecurity awareness. Continuous monitoring of PQC implementations ensures ongoing identification of vulnerabilities and performance issues, crucial for staying ahead of the evolving quantum threat landscape. The governance team remains agile, adapting security measures based on emerging challenges and insights gained through ongoing monitoring. Regular tracking of standardisation efforts by organisations like NIST and ETSI solidifies the organisation's commitment to quantum-safe security, aligning with industry best practices and standards. Through these multifaceted efforts, organisations fortify their capabilities and readiness to navigate the quantum era with resilience and foresight.

Adopting quantum-safe practices isn't just about security; it's a strategic business move. In this subsection, we translate technical principles into business strategies, showing how being quantum-safe can be a unique selling point and enhance customer trust.

# Risk management

Consider a business that overlooks quantum threats and finds its encrypted data compromised overnight. This case study explores such a scenario, highlighting the importance of the risk management strategies we outline, ensuring your business remains secure and resilient.

## Strategy and preparation

Our experience indicates the journey to quantum safe must be well planned and incrementally executed based on business and technical priorities, as well as several other critical considerations. An effective Quantum Safe approach combines technology with first-step guidance to prioritise quantum-safe initiatives to assess organisational risk, IT strategy, supply-chain dependences, and ecosystem operations. Core to this approach is the creation of cryptographic inventories as well as corresponding risk and governance plans. Quantum Safe migration is a multi-step process requiring both operations and cryptographic experience. Alignment with broader business transformation efforts is another dimension for effective planning across this multi-year initiative. External factors involving regulatory agencies, standards bodies and ecosystem partners must also be considered.

## IBM Quantum Safe approach

The IBM Quantum Safe approach combines first-step guidance to prioritise with IBM quantum-safe technology tailored to meet client objectives to assess organisational risk, IT strategy, supply-chain dependences, and ecosystem operations. The IBM Quantum Safe offering extends to include capabilities designed understand application and network operations and their implications. The overall approach supports a Quantum Safe change programme through the creation of cryptographic inventories and corresponding risk and governance plans. There are two (2) main elements:

**Strategy –** Services designed to enable clients to initiate a quantum safe transformation programme and prepare to fund and scale this across the organization. The IBM Quantum Safe programme establishes an approach to assess the requirements to transition to Quantum Safe cryptography and creates a plan for adoption. The approach includes clear phases and outcomes with agile information collection methods with delivery dependencies and parallel activities.

**Technology –** Designed to guide our clients through initial pilots to demonstrate the ability to accelerate the transition to Quantum Safe cryptography, accelerate the remediation of applications within their enterprise, and establish a programme for full-scale deployment.

IBM Quantum Safe technology offers a comprehensive set of capabilities, and approaches combined with deep expertise to help plan and execute a migration to quantum-safe cryptography. Building quantum cyber-resilience is performed in three phases—Discover, Observe, and Transform—each powered by IBM Quantum Safe technology:

- **IBM Quantum Safe Explorer** can enable organisations to scan source and object code to locate cryptographic assets, dependencies, vulnerabilities and to build a CBOM. This allows teams to view and aggregate potential risks into one central location.

- **IBM Quantum Safe Advisor** allows the creation of a dynamic or operational view of cryptographic inventory to guide remediation and analyses cryptographic posture and compliance to prioritise risks. Quantum Safe Advisor performs an enterprise-wide analysis of your cryptography and builds a comprehensive cryptographic inventory that details the types and locations of your cryptographic instances, the relationships between assets and data flows, and potential vulnerabilities to quantum technology.

- **IBM Quantum Safe Remediator** enables organisations to deploy and test best practice-based quantum-safe remediation patterns to understand the potential impacts on systems and assets as they prepare to deploy quantum-safe solutions. Remediator helps you to create an architecture for seamlessly upgrading your cryptographic infrastructure to be Quantum Safe.

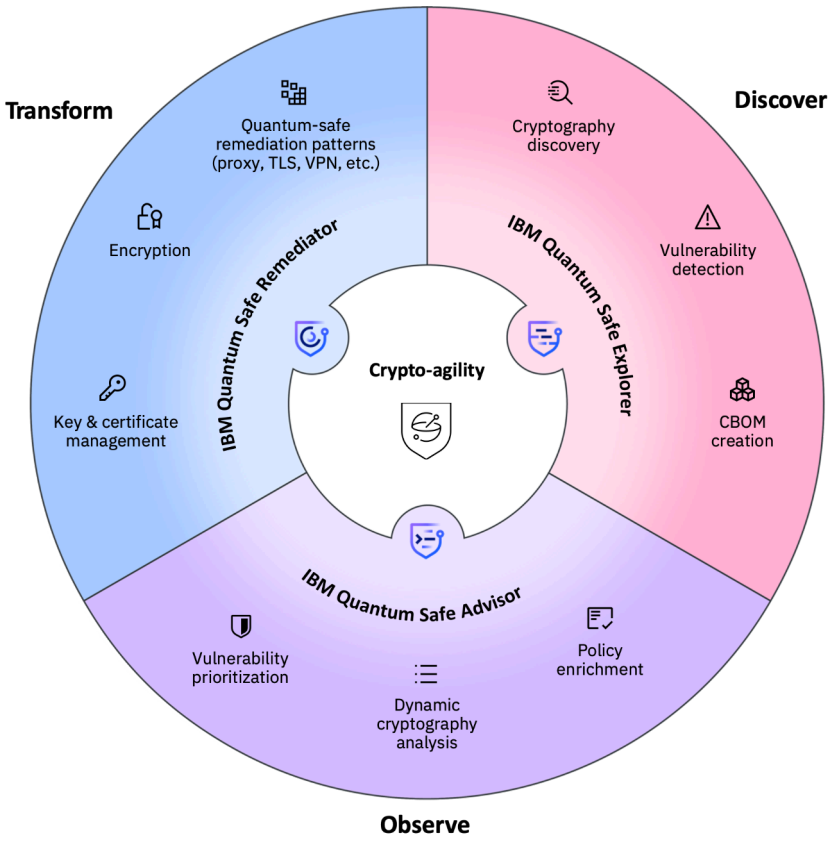


Figure 1. IBM Quantum Safe Technology Approach

## Cybersecurity and data protection guidelines

There are multiple existing cybersecurity risk management guidelines and frameworks that have been widely adopted by organisations, such as the following:

- **NIST Special Publication 800-37:** Risk Management Framework (RFM) for Information Systems and Organisations A System Life Cycle Approach for Security and Privacy [RMF18].

- **NIST Cybersecurity Framework (CSF)** for Improving Critical Infrastructure Cybersecurity [CSF18].

- **ISO/IEC 27001:** Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems [ISO22a].

- **ISO/IEC 27005:** Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks [ISO22b].

These standards share a common focus on effective risk management in information security, emphasising a systematic approach to identify, assess, and manage risks comprehensively. They advocate for continuous monitoring, assessment, and improvement to address evolving cybersecurity threats, considering technical aspects, governance, processes, and human factors.

In Singapore, the Personal Data Protection Act (PDPA) aims to protect individuals' personal data by establishing guidelines for its collection, use, and disclosure. Organisations must implement reasonable security arrangements to safeguard personal data from unauthorised access, disclosure, alteration, or destruction. Cryptography plays a crucial role in cybersecurity risk management, ensuring data confidentiality, integrity, and authenticity. For example, encryption is used to secure data at rest, in transit, and during processing, mitigating the risk of data breaches and unauthorised disclosures, aligning with PDPA requirements.

Despite the prevalent adoption of current risk management frameworks, they lack provisions for quantum-safe security, revealing gaps that must be addressed. Consideration of quantum risks should be integrated into existing risk assessment processes. Organisations must focus on evaluating the longevity of data supporting critical applications. For prolonged data protection, there is a pressing need to introduce additional mitigating controls. Quantum threats pose risks to sensitive health and financial data, compromise the confidentiality of communications, challenge the integrity of digital documents, and threaten cryptocurrencies.

The emergence of “harvest now, decrypt later” tactics underscores the urgency for organisations to fortify their cybersecurity measures against quantum advancements. Proactive adjustments to risk management strategies are crucial to navigate evolving threats and ensure the resilience of information security frameworks in the face of quantum challenges.

## Quantum risk assessment

In what follows, we give an overview of two examples of quantum risk assessment frameworks which have been published within the quantum safe community: Mosca’s Quantum Risk Assessment (QRA) [MM23] and Crypto Agility Risk Assessment Framework (CARAF) [Ma21]. Moreover, we highlight their limitations.

**Mosca’s QRA** uses a time-based approach to define risk, dependent on when migration to a quantum-safe state begins and considers “harvest now decrypt later” attacks. Its methodology is adapted from the six stages for conducting a risk assessment in the NIST Cybersecurity Framework [CSF18].

Mosca’s “x, y, z” quantum risk model focuses on the dimensions of the impact of quantum computing. The “x” parameter represents the lifetime of assets (how many years we need our encryption to be secure?). The “y” parameter indicates the time required to migrate a quantum-safe state (how many years it will take us to make our IT infrastructure quantum-safe). The “z” parameter considers the time until current cyber defences collapse in the face of threat actors with access to quantum technology (how many years before a large-scale

quantum computer will be built?). By examining these dimensions, organisations can assess the urgency and potential consequences of quantum threats, guiding them in developing strategic and timely responses to ensure the security of their cryptographic systems.

**CARAF** builds on Mosca's QRA by specifically addressing cryptographic agility. Cryptographic agility involves the swift replacement of vulnerable cryptographic primitives, algorithms, and protocols with more secure alternatives. The conventional process of transitioning from one cryptographic solution to another can be time-consuming, potentially leaving organisations exposed to security risks during this period.

The CARAF framework aims to systematically analyse and assess the risks arising from the absence of cryptographic agility. By leveraging CARAF, organisations can thoroughly evaluate their cryptographic systems' agility, identifying potential vulnerabilities and assessing the associated risks. This analysis facilitates the development of a mitigation strategy that aligns with the organisation's risk tolerance. Essentially, CARAF provides a structured approach for organisations to navigate the challenges of crypto agility, enabling them to make informed decisions about their cryptographic infrastructure and security posture in the face of evolving threats and technological advancements. Further details on CARAF and Mosca's QRA, and their comparison can be found in [FS-ISAC23a].

**Cautionary notes:** Mosca's methodology often results in assigning a low-risk classification when "z", representing the time to compromise, ranges from 15 to 20 years. This approach tends to prioritise items with extended security shelf-lives over high-impact areas that may not require a prolonged security shelf-life. The emphasis is on identifying sensitive or critical data that could be vulnerable to future threats, including scenarios like a "store now and decrypt later" attack. The risk determination process categories assets into either at risk or not at risk without considering nuanced risk levels for effective prioritisation. This means that items with significant impact, like the telecommunication control plane, might have lower "x" or "y" values but should not be labelled as having low or no risk, emphasising the need for a more nuanced risk assessment [GSMA23].

## Perspectives on quantum risk management

The National Institute of Standards and Technology (NIST) projected in 2016 that a quantum computer capable of breaking 2000-bit RSA encryption could be built by 2030 for about a billion dollars [Chen16]. However, various research institutes and tech firms have offered different timelines, ranging from less than 10 to up to 30 years. Relying on a speculative quantum timeline for risk assessment poses its own risks, potentially leading organisations to adopt a passive "wait-and-see" approach. Organisations run the risk of being caught off guard, or left with insufficient time to take mitigation measures if there is a breakthrough in the advancement of quantum computing in the near future. This risk is extended if there is a new discovery or design flaws in current crypto systems already running in existing environments.

In our approach, we move away from relying on a specific quantum timeline and instead focuses on strengthening the overall cyber risk management framework. Rather than adopting an entirely new framework, quantum risk management integrates into existing cybersecurity practices. The process is continuous, adapting to dynamic threats, emerging vulnerabilities, and evolving regulatory environments. Key factors for managing quantum risk within an organisation are outlined below, emphasising the importance of constant vigilance and adaptability in the ever-changing landscape of cybersecurity.

# Get the basics right

Addressing the quantum threat requires organisations to proactively assess their readiness, understanding both known challenges and potential unknown implications. The first step involves cataloguing all instances of cryptography usage, encompassing encryption keys, algorithms, applications, and associated business processes. This comprehensive inventory empowers organisations to achieve crypto agility, enabling strategic planning and adaptability in the evolving quantum-safe security landscape.

Effective monitoring of potential impacts requires careful consideration and maintenance of critical elements. At a minimum, these elements should encompass the following aspects [FS-ISAC23a]:

- **Applications:** Organisations should assess both in-house and vendor applications, examining their utilisation of cryptographic algorithms. An inventory of critical and high-availability applications, along with an overview of internal and external application connections, is vital for a thorough understanding of the cryptographic landscape.

- **Third-party vendors:** Evaluate vendor roadmaps to ascertain their support for post-quantum cryptography. Procurement considerations should align with the organisation's commitment to PQC, ensuring that vendors comply with evolving security standards.

- **Data:** It is crucial for organisations to determine the duration for which data assets need protection. Classifying datasets based on sensitivity and criticality aids in developing a targeted security strategy. Additionally, organisations must assess the risk of a “harvest now, decrypt later” attack scenario, especially for highly sensitive information.

- **Regulations:** Organisations should be prepared to respond to potential queries from regulators, ensuring compliance with industry standards and guidelines. Addressing questions promptly and transparently is essential to maintain regulatory compliance.

- **Location of data:** Data residency introduces another layer of complexity, as different regions may have varying timelines for adopting post-quantum cryptographic measures. Organisations must align their strategies with regional timelines to ensure a cohesive and effective implementation of security measures. By systematically addressing these considerations, organisations can proactively navigate the challenges posed by the evolving quantum threat landscape.

By systematically evaluating these aspects, organisations can enhance their quantum readiness and strategically plan for the future, ensuring robust security measures in the face of emerging quantum threats.

## Start small, start now

The complexity of transitioning to PQC is accentuated by its deep integration into enterprises, intricately woven into physically remote systems. According to the World Economic Forum's Global Future Council on Quantum Computing, a staggering 20 billion digital devices are projected to require upgrading or replacement with PQC within the next two decades [WEF20]. This shift is not a mere switch-out or patch; it profoundly transforms numerous devices and systems, spanning ATMs, TV set-top boxes, smartphones, and more. Algorithm replacement, a key aspect, is disruptive and time-intensive, often spanning years. Urgency is paramount, emphasising the need for organisations to plan and adopt a posture of crypto agility.

Commencing this transformative journey is not just recommended; it's a strategic imperative. Organisations are advised to adopt a pragmatic and phased approach, with key plans and objectives serving as a foundational framework for the migration process:

- **Identify critical business processes:** Identify key processes heavily reliant on critical data to understand specific areas demanding immediate attention.
- **Conduct comprehensive risk assessment:** Undertake a thorough risk assessment against critical business processes to evaluate vulnerabilities and potential threats, creating a risk register for structured mitigation.
- **Establish risk tolerance and crypto agility:** Define risk tolerance levels and embrace crypto agility principles, prioritising remediation efforts based on asset value or risk. Understand quantum technology capabilities and challenges, assessing the business impact of quantum computing advancements for informed decision-making in the quantum era.

A phased approach allows gradual adaptation, focusing on higher-value or higher-risk assets, aligning strategies with the evolving quantum technology landscape.

## Continuous learning and monitoring

Following the identification of cryptography uses for key business processes and an initial risk assessment, organisations must adopt a vigilant and adaptive strategy in the dynamic realm of quantum computing and its corresponding quantum-resistant security. Continuous development and monitoring are imperative:

- **Monitor quantum computing development:** Stay informed about ongoing developments, breakthroughs, and potential quantum applications that could impact existing cryptographic systems.
- **Understand vulnerabilities in crypto systems:** Develop a comprehensive understanding of both known and emerging cryptographic vulnerabilities associated with quantum threats through continuous research and awareness initiatives.
- **Adhere to standards and regulatory requirements:** Align with emerging standards and regulatory requirements set by national cybersecurity institutions, such as the winners of the NIST PQC competition transitioning into Federal Information Processing Standards (FIPS).
- **Evaluate vendor readiness:** Assess the readiness of third-party vendors and solution providers in the quantum realm, including technologies based on PQC, quantum key distribution (QKD), and quantum random number generators (QRNG).
- **Enhance crypto agility:** Strive to efficiently update cryptographic algorithms, parameters, processes, and technologies to respond adeptly to new protocols, standards, and security threats posed by quantum computing. Consider factors such as data and cryptographic assets, cryptographic keys, and infrastructure limitations.

Furthermore, organisations should consider hybrid solutions integrating classical and quantum-ready approaches. This strategic approach overlays existing security measures with robust post-quantum cryptography algorithms, providing assurance during the transition to quantum-safe security.

By adopting these ongoing measures, organisations establish a resilient posture in the face of quantum computing advancements. This continuous development and monitoring strategy fortify cryptographic systems, enabling organisations to navigate the complexities of the evolving quantum landscape with agility and preparedness.

# Next steps

Forward-leaning companies and governments are preparing for a quantum computing future and positioning themselves ready to capture the many benefits of this technology. Yet, more can and should be done. Collaboration is key: governments, researchers, academics, and industry will need to work together on policies to accelerate the adoption of new educational curricula, fund R&D, create new talent pipelines, and more.

Migrating to quantum-safe security requires a multi-pronged approach that combines proactive action, strategic planning, and continuous adaptation. In what follows, we summarise key next steps and considerations:

- **Inventory & assessment:** Start by identifying all assets and systems relying on cryptography, especially those using vulnerable algorithms like RSA and ECC. Prioritise these based on their importance and the sensitivity of the data they handle. Evaluate how the adoption of quantum-resistant algorithms might impact their performance and compatibility.

- **Pilot & testing:** Engage in pilot projects to test chosen PQC solutions in real-world scenarios. Assess their impact on performance, check for compatibility issues, and identify potential challenges in integration. Gather valuable data and feedback from these pilot projects to refine and enhance the overall migration strategy for the future.

- **Planning & strategy:** Develop a comprehensive migration strategy for adopting PQC algorithms. Evaluate and select PQC algorithms that align with specific security needs and requirements. Prioritise systems holding high-value data and critical infrastructure. Factor in costs, resources, and training considerations for each phase of the migration.

- **Deployment & rollout:** Implement PQC solutions in a phased manner, starting with high-risk or critical systems and data. Establish robust key management and lifecycle practices specifically designed for PQC keys to ensure their secure and effective use.

- **Awareness & training:** Educate employees on the risks associated with quantum computing and emphasise the necessity for migration. Provide training to equip them with the knowledge and skills required to securely use and manage quantum-safe systems. Foster a culture of cybersecurity awareness and vigilance across the organization.

- **Monitoring & maintenance:** Continuously monitor implemented PQC solutions for vulnerabilities and performance. Stay informed about the evolving quantum threat landscape and adapt security measures. Keep a close eye on standardisation efforts by organisations like NIST and ETSI.

This above ensures a thorough and proactive transition to quantum-safe security while keeping the organisation resilient and prepared for the challenges posed by quantum computing.

# IBM-NCS value propositions

## Why IBM-NCS partnership?

The partnership between IBM and NCS is driven by the shared commitment in ensuring quantum-safe security for organisations in Singapore and beyond. IBM, a global leader in quantum computing development, has not only been at the forefront of quantum technology but has also played a crucial role in creating quantum-safe technologies showcased in the NIST post-quantum cryptography competition. Three out of four finalists in the competition were developed by IBM in collaboration with industry and academic partners.

NCS stands out as a prominent digital and technology service provider in the Asia-Pacific region, particularly known for its role as a trusted system integrator for government agencies in Singapore for over four decades. With a strong track record in successfully executing large-scale projects, NCS Cyber complements its core capabilities in application, engineering, and infrastructure with security solutions and services. This collaboration allows NCS to leverage IBM's expertise in quantum safe security, ensuring that clients receive top-notch consultancy services.

The IBM-NCS partnership offers more than just advanced security. We bring practical benefits to your business, such as ensuring compliance, gaining a competitive edge, and building customer trust in an era of quantum computing.

Recognising the major implications quantum-safe security will have on both legacy systems and new deployments dealing with sensitive data, the partnership aims to prepare clients for a quantum-safe future through the combined knowledge and experience of IBM and NCS.

## Specialised domain knowledge and capabilities

The collaboration between NCS and IBM brings together a wealth of specialised resources, including Ph.D.-trained personnel, qualified consultants, and skilled engineers. These resources each possess in-depth knowledge of the evolving quantum-safe technology landscape. This expertise spans the intricacies of cryptographic algorithms, their applications, and the systems and infrastructure where these algorithms find deployment.

This partnership transcends the conventional supplier-client relationship by offering more than just technology solutions. It extends to delivering a comprehensive package encompassing expert advisory, processes, and experiences. Clients stand to benefit not only from cutting-edge technological advancements but also from the collective expertise and proficiency of a team well-versed in navigating the complexities of quantum-safe implementations. As a result, the collaboration ensures a holistic approach to addressing the challenges posed by quantum threats.

## Localisation

NCS boasts a profound understanding of prevalent cyber risk management and data protection frameworks, intricately navigating the guidelines and best practices stipulated by local authorities. This encompasses a comprehensive grasp of regulatory standards such as the Personal Data Protection Act (PDPA), IM8, CCoP 2.0, as well as sector-specific guidelines for banking and healthcare. Leveraging this extensive expertise, the collaborative efforts of IBM and NCS in the realm of quantum risk assessment and management are uniquely poised to align with local requirements. The joint offerings through IBM and NCS are designed complement existing risk assessment frameworks, ensuring a seamless integration that addresses the specific needs and intricacies of the local regulatory landscape. This approach underscores the commitment to delivering quantum-safe solutions that not only meet global standards but also resonate with the nuanced requirements of the communities they serve.

## References


[WEF23] Quantum Readiness Toolkit: Building a Quantum-Secure Economy. World Economic Forum, Jun 2023.

[Ma21] C. Ma et. al., CARAF: Crypto Agility Risk Assessment Framework, Journal of Cybersecurity, pages 1-11, 2021.

[MM23] M. Mosca and J. Mulholland, A Methodology for Quantum Risk Assessment. Global Risk Institute, 2023.

[Chen16] L. Chen et. al., Report on Post-Quantum Cryptography, Vol. 12. US Department of Commerce, National Institute of Standards and Technology, 2016.

[GSMA23] GSMA, Guidelines for Quantum Risk Management for Telco version 1.0, 22 September 2023.

[RMF18] NIST Special Publication 800-37 - Risk Management Framework (RFM) for Information Systems and Organisations A System Life Cycle Approach for Security and Privacy, Revision 2, December 2018.

[CSF18] NIST Cybersecurity Framework (CSF): Framework for Improving Critical Infrastructure Cybersecurity version 1.1, April 2018.

[KM20] NIST Special Publication 800-57 - Recommendation for Key Management: Part 1 - General. Revision 5, May 2020.

[ISO22a] ISO/IEC 27001: Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems, 2022.

[ISO22b] ISO/IEC 27005: Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks, 2022.

[FS-ISAC23a] FS-ISAC: Risk Model Technical Paper, Post-Quantum Cryptography (PQC) Working Group, 2023.

[WEF20] WEF: Global Future Council on Quantum Computing, June 2020. https://www3.weforum.org/docs/WEF_Global_Future_Council_on_Quantum_Computing.pdf.


ncs.co