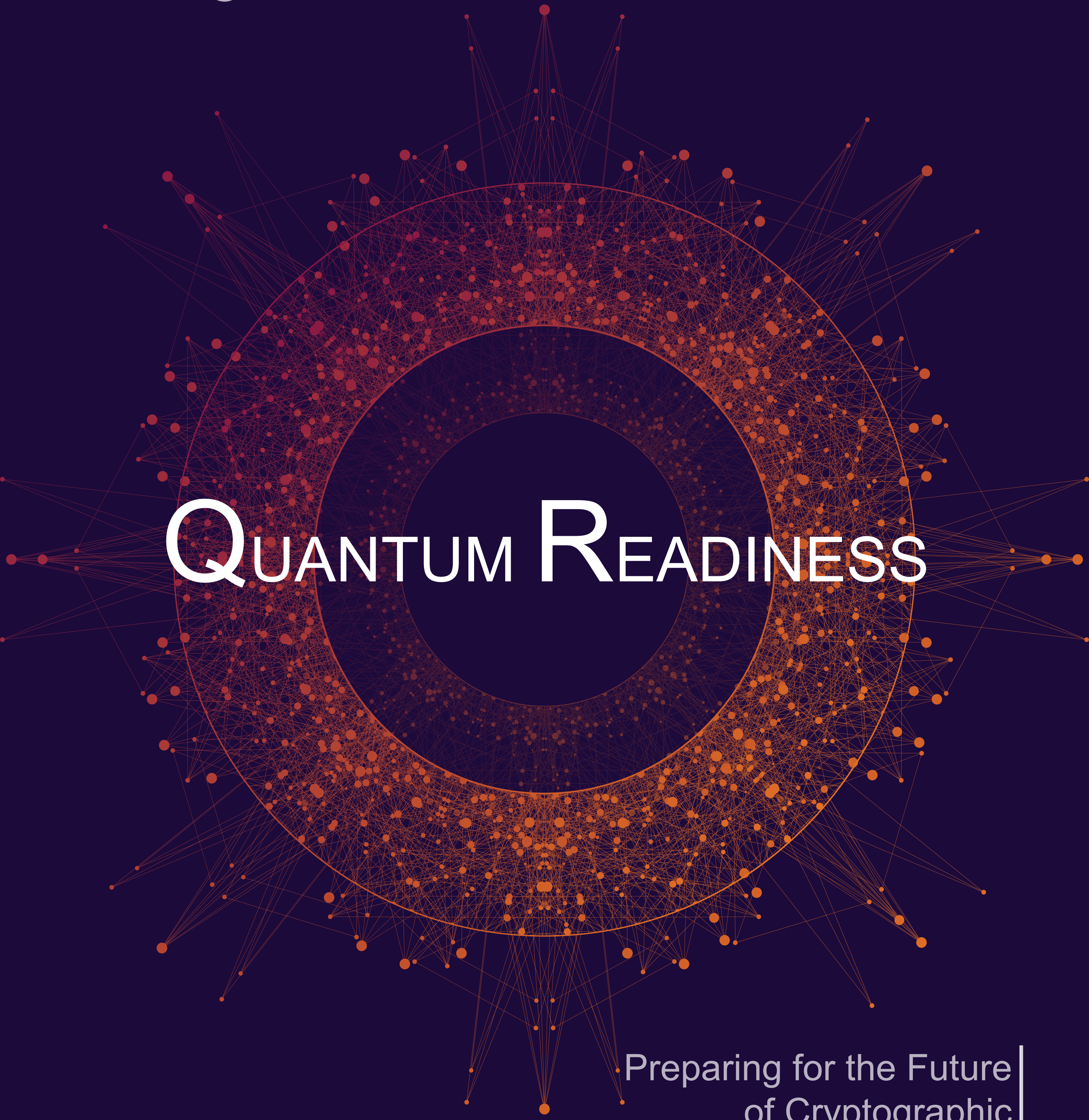
CyberAlberta's



Quantum Readiness

Preparing for the Future
of Cryptographic
Security

Classification: Public | Disclaimer

CYBER ALBERTA

Table of Contents

List of Abbreviations

CCCS	Canadian Center for Cyber Security
CFDIR	Canadian Forum for Digital Infrastructure Resilience
CISA	Cybersecurity and Infrastructure Security Agency
CRQC	Cryptographically Relevant Quantum Computer
DH	Diffie-Hellman
NIST	National Institute of Standards and Technology
PQC	Post-Quantum Cryptography
RSA	Rivest-Shamir-Adleman
SNDL	Store Now, Decrypt Later
WEF	World Economic Forum

Executive Summary

"Quantum Readiness: Preparing for the Future of Cryptographic Security" analyzes the potential impact of quantum computing on cryptographic security and provides a summary of common approaches to becoming quantum ready. The primary threat quantum computing poses is the threat to current encryption systems that organizations rely on to keep their data secure, especially for data in transit. Efforts to protect against quantum algorithms have already been put forward, with the National Institute of Standards and Technologies (NIST) working on a set of post-quantum cryptographic standards.

In the landscape of quantum, organizations are advised to start thinking about a quantum readiness strategy to keep their data secure. Organizations are recommended to understand their technical environment and build a plan to develop strategies to protect against quantum threats. Organizations should place a high level of importance on quantum readiness activities such as: inventorying cryptographic algorithms in use, creating a long-term plan to ensure preparedness for the security challenges posed by quantum computing, perform risk management activities, leverage NIST's recommendations, and establish effective communication strategies. This document emphasizes the need for organizations to start preparing now and provides recommendations to address the quantum threat.

Introduction

Assuming you are reading this document online, the probability that a cryptosystem is being used to secure your data and identity in the background is nearly absolute. Cryptographic systems have become essential pillars of our global digital communication infrastructure, embedding themselves deeply due to their unparalleled efficacy in safeguarding sensitive data. Their widespread presence highlights their essential role in maintaining secure communication channels. The security of these systems relies on the complexity of well-known mathematical problems; however, in the early 1990's, researchers discovered that these problems could be solved using quantum computers. This revelation sparked concerns about the potential downfall of modern cryptosystems. At the time the threat was purely theoretical as a quantum computer had yet to be built.

Quantum computers capable of cracking cryptographic systems, also known as cryptographically relevant quantum computers (CRQC), are steadily becoming a reality. Contemporary views on CRQC and the threat they pose to modern cryptography remain debatable. For this reason, the National Institute of Standards and Technology (NIST) has drafted and selected post-quantum cryptographic standards (Chen, et al., 2016) . NIST and other industry experts have legitimized the threat, but the quantum paradigm shift appears to be forever just around the corner. This ongoing uncertainty leaves organizations questioning when the threat will materialize, how quickly they need to act, what steps to take, and even what a quantum computer truly is.

We aim for this document to serve as a guide for organizations to prepare for the quantum era. It provides an overview of quantum computing, assesses its potential impact on business operations, and outlines a strategic roadmap for quantum readiness. Whether you are just starting your quantum security journey or looking to refine your strategy, we hope this document will be a valuable resource in navigating quantum challenges.

1981

Physicists Richard Feynman conceptualized the first quantum computer in a now famous article titled "Simulating Physics with Computers" (Feynman , 1982).

1994

Mathematician Peter Shor developed a series of infamous quantum algorithms known as "Shor's algorithm" (Shor, 1997).

1996

Computer scientist Lov Grover develops Grover's algorithm (Grover, 1996).

1998

The first two qubit quantum computer was created (Holton, 2025).

2016

NIST announces a competition to update their standards to a post-quantum state (NIST, 2016).

2020

IBM announced their quantum roadmap, outlining their plan to have 4,000 qubit systems by 2025 (IBM, 2022).

2022

In 2022, after several rounds NIST announces selected candidates for PQS standard (The NIST PQC Team, 2022).

?

Threat Manifestation...

Demystifying Cryptography

A cryptographic algorithm is considered secure if it is resistant to all known attacks. This inherently means that this classification is subject to change. Thus, algorithms we consider secure today may not be considered secure tomorrow.

Cryptography, on the other hand, is the practice of hiding secrets so that only the person the message was intended for can read them. It has been around for thousands of years, but archaic cryptography hardly resembles what we rely on today. Old cryptographic systems relied on system secrecy, so to break a cipher you simply needed to know the process used to create it. In contrast, modern cryptographic systems rely on the difficulty of certain—well known—mathematical problems and the secrecy of a key.

The three broad categories of cryptographic algorithms are asymmetric key cryptography, symmetric key cryptography, and cryptographic hashing algorithms. A CRQC poses a material threat to the security, in terms of confidentiality and integrity, of standard asymmetric and symmetric cryptographic algorithms widely in use today.

A cryptographic algorithm retains a secure classification if:

1. The system itself remains unbroken; and
2. The secret key is sufficiently strong, in terms of bits of security strength.

Depending on the category of an algorithm, a CRQC generally only threatens one of these two items.

Symmetric key algorithms rely on a single key for all functionality, such as encryption/decryption and signatures. The current best known quantum approach to breaking these is through Grover's algorithm, which provides a quadratic speedup in deriving the shared secret key. Thus, the solution to securing against Grover's is simple and familiar: utilize a symmetric key algorithm with a sufficiently large key strength, such as AES256 for encryption over AES128.

The threat of a CRQC to asymmetric cryptographic algorithms is far more substantial than that of symmetric algorithms, because the system itself is lost. Modern public key infrastructure is vulnerable due to their reliance on well-known and specific mathematical problems, which are currently known to be greatly simplified by CRQCs. These include the discrete logarithm problem for the Diffie-Hellman (DH) algorithm, and prime factorization for the Rivest-Shamir-Alderman (RSA) algorithm. Asymmetric cryptography can be fundamentally broken by a CRQC using Shor's algorithm, which provides an exponential speedup in deriving the private (secret) key.

Therefore, the solution for quantum-readiness is significantly more difficult for asymmetric cryptographic algorithms, as it requires an entirely new cryptographic system and, in some cases, infrastructure to mitigate the known quantum threats.

Cryptogrpahic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric	Encryption	Debated; prefer AES256
SHA-2, SHA-3	Hashing	Various cryptographic algorithms, data integrity, data masking	Debated; prefer SHA2 or SHA3, specifically SHA2/3 384 or SHA2/3 512
RSA	Asymmetric	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Asymmetric	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Asymmetric	Signatures, key exchange	No longer secure

Table 1: Impact of Quantum Computing on Cryptographic Algorithms [(Chen, et al., 2016), Tab.1]

Post-Quantum Algorithms

NIST has released its list of the first four post-quantum algorithms that will become the new standards for encryption. These algorithms are based on math problems that would be challenging for both conventional and quantum computers to solve (NIST, 2024).

NIST identified two purposes for these algorithms. The first primary purpose involves improving the establishment of post-quantum secure connections to protect critical information (e.g., passwords, financial information) being transmitted over the internet. The second purpose stated by NIST, is for digital signatures used for identity authentication (NIST, 2024).

For key establishment, used in creating secure connections, CRYSTALS-Kyber was selected and adapted into ML-KEM. For digital signatures, CRYTALS-Dilithium, FALCON and SPHINCS+ were selected (Boutin, 2022). The first three mentioned algorithms are based on structured lattices and SPHINCS+ is based on hash functions (NIST, 2024).

NIST post-quantum standards will replace many current cryptography standards in the post-quantum world, and many are already being implemented across popular systems, services, and applications. Certain products, such as popular web browsers and web servers, are already incorporating some of these post-quantum algorithms (e.g., X25519MLKEM768; a derivative of CRYSTALS-Kyber).

For more information on the NIST standards visit the NIST website.

When Will the Quantum Threat Manifest?

There is no consensus as to when this threat will manifest, only that it eventually will. The urgency with which one should act is determined by their risk tolerance.

Forecasting when a CRQC will be created has proven to be a difficult problem. The answer to this is usually presented as a function of two inversely accelerating rates, whose convergence marks the point at which the quantum threat will manifest. These rates are as follows:

1. The number of qubits required to break modern encryption decreases over time as qubits improve.
2. The number of qubits in the largest circuit model quantum computer, which increases over time with improvements in the field.

No one knows when this intersection will occur and there is much debate, as simply increasing system complexity is only one piece of the puzzle. Qubits represent extremely sensitive quantum systems. For this reason, quantum computers are shielded from the world and cooled to near absolute zero, as any external forces could result in error. Because of this sensitivity and the probabilistic nature of quantum computations, these systems are also prone to error even when proper precautions are taken, and thus error correcting qubits are required to monitor the logical qubits.

Building a CRQC takes immense resources and is a multidisciplinary problem that is on the edge of our current capabilities. Despite this, experts are certain that a CRQC will be built, but there is no consensus as to when. Therefore, it is recommended that organizations start preparing now to be prepared for emerging quantum threats. According to The Global Risk Institute, the urgency with which an organization should act is gauged by their risk tolerance and the following three factors:

- **The shelf-life time:** how many years your data must remain secure for.
- **The migration time:** how many years it will take to securely migrate systems protecting that data.
- **The threat timeline:** the estimated timeline until potential adversaries gain access to a CRQC.

A notable threat is “Store Now, Decrypt Later” (SNDL), wherein threat actors store encrypted information with the anticipation that the encryption scheme will be feasibly breakable in the future. An attacker can simply capture encrypted packets now, store them, and decrypt them at an arbitrary time in the future when they have access to a CRQC. Fundamentally speaking, cryptography should be applied such that the anticipated time to break the encryption far exceeds the shelf-life of the data. This is especially concerning for data with long shelf life (e.g., Social Insurance Numbers), as encrypted traffic containing this sensitive information may be decrypted decades down the line and utilized for subsequent attacks (e.g., ransom, fraud, intrusion, etc.). Needless to say, this risk is exacerbated by the quantum threat, as the vast majority of web-based traffic is susceptible to attack due to its dependence on asymmetric cryptography algorithms.

Preparing for Quantum

Failure to become quantum aware and ready may lead to the inability to keep up with the cybersecurity trends and landscape, therefore putting organizational systems and information at risk for an attack.

Quantum computing is a revolutionary technology that will impact organizations and cybersecurity practices. Since it is unknown when the threat will manifest, organizations should proactively consider quantum readiness practices when developing and adapting their organizational cybersecurity strategies.

Preparing for the quantum threat is not new. In the last few years, various industry leaders have been advising the need to become cryptographically agile. However, becoming quantum ready is an extensive process that will require multiple phases and years (Quantum-Readiness Working Group (QRWG), 2023). A key part of readiness will be to set forth a solid and realistic plan on how the organization will prepare and respond to quantum threats. However, such a plan can only be successful if there is a clear understanding of the organization's assets and information. The possible threats that quantum poses will vary for each organization, depending on their environment and systems, making quantum readiness a unique process for each.

The following timeline is an example of a quantum readiness roadmap. The dates and activities are examples and recommendations based on the best practices and recommendations from CFDIR (Quantum-Readiness Working Group (QRWG), 2023), NIST (Cybersecurity and Infrastructure Security Agency [CISA], 2023), and WEF (World Economic Forum, 2023).

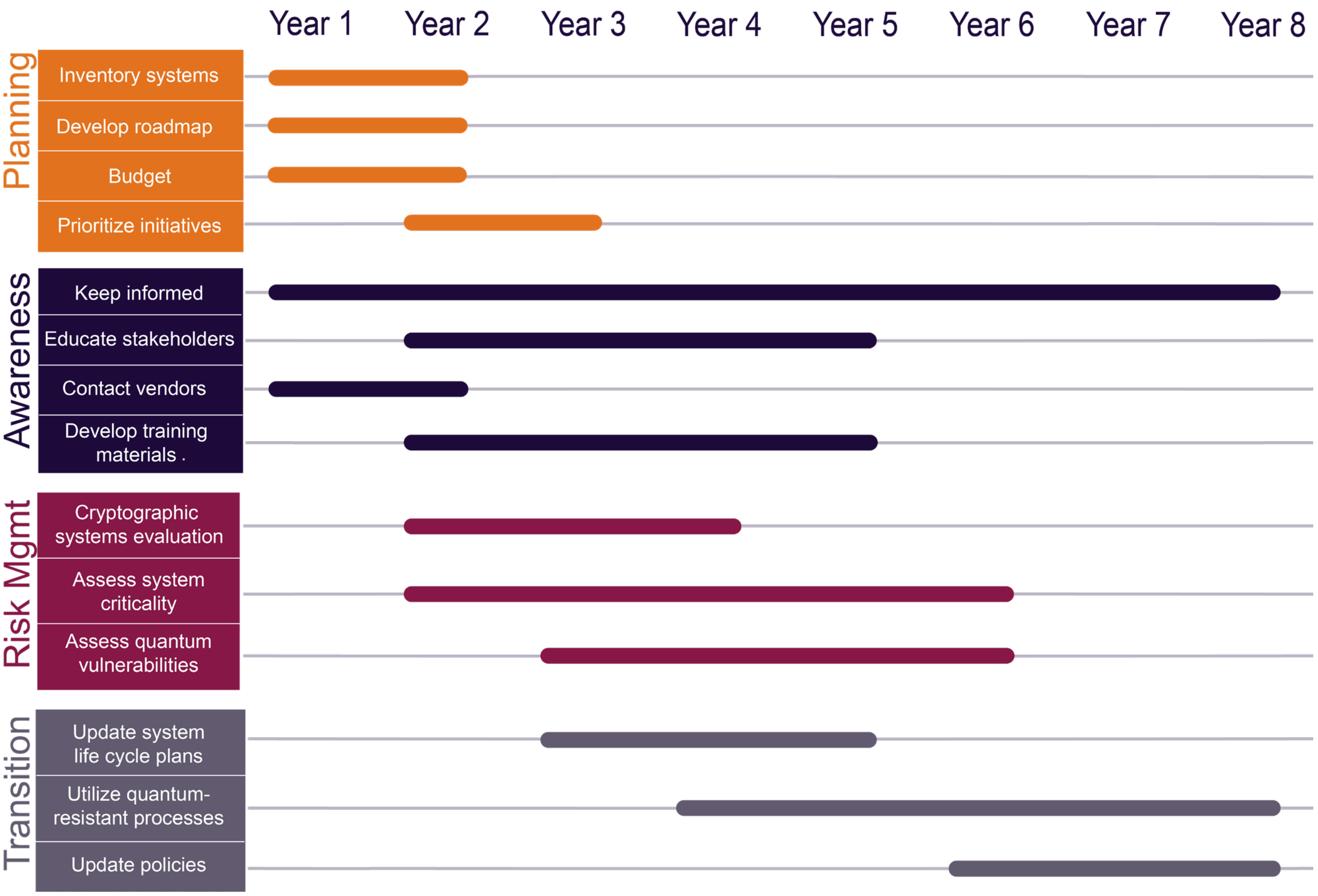


Figure 1. Example quantum ready roadmap activities and timeline

Quantum Readiness Strategies

Quantum Readiness Planning

Organizations should begin planning their quantum strategy as soon as possible. Planning is one of the first steps for quantum-readiness and should be done as an organizational strategy to protect information and systems. During the planning phase, the inventorying of systems, devices, databases etc., should be performed to better the planning strategies and activities. Post-quantum efforts will require detailed plans and considerations that will be different for each organization. The following are activities that should be considered and performed as a part of quantum planning.

Inventory cryptographic systems by identifying all systems and applications using current cryptography methods. Having an inventory will aid in prioritization and overall organization of systems, helping to understand how cryptography is leveraged in IT and OT systems, and what is at risk (Cybersecurity and Infrastructure Security Agency [CISA], 2023).

Develop a roadmap to establish both a clear action plan and an actionable timeline (Cybersecurity and Infrastructure Security Agency [CISA], 2023). A quantum readiness roadmap should be tailored to each organization and their specific IT environment. It is important that this quantum roadmap is developed and integrated into the organizational operations and budget.

Budget for potential updates and system replacements, it will be important to establish a budget early in the planning phase to ensure that the quantum readiness plan can be implemented (Canadian Center for Cyber Security, 2025).

Prioritize activities and initiatives during the planning and roadmap creation process. These prioritizations should be done after the organization has performed some risk management activities and understands the threats to their systems and organization.

Becoming Quantum Aware

Organizations should communicate the progress and changes being implemented throughout their quantum readiness timeline. Communication and awareness ensure that the necessary stakeholders are aware of the current state of the organization and potential risks.

Keep informed on the existing and emerging threats of quantum and post-quantum cryptography to the business. All levels of an organization and its stakeholders should be informed on the quantum threats to ensure strategy is communicated to mitigate quantum threats and there is full support from the business for post-quantum efforts. Various organizations have dedicated teams put forth to study and release information on quantum. Said organizations include NIST, CISA, CCCS, WEF, and GRI. Furthermore, reputable consulting firms provide valuable resources for good practices regarding quantum security and readiness.

Contact vendors and partners to understand their strategies on quantum readiness. It is important to understand the timelines that they have set, especially if any of the services and/or technology impacts your organization (Cybersecurity and Infrastructure Security Agency [CISA], 2023).

Proper training procedures and practices will ensure that employees are well equipped with the best cybersecurity tools and knowledge for quantum threats. Additionally, educating employees about the risks of quantum and proactive measures can reduce the resistance to change when quantum becomes a larger threat.

Undergoing Risk Management Activities

Evaluate existing cryptographic systems prior to implementing post-quantum controls. Leverage the inventory of cryptographic systems (see above) and evaluate based on system criticality and priority. It is important to determine which systems are at risk of post-quantum cryptographic threats and the impact of a potential attack on the organization's systems (Quantum-Readiness Working Group (QRWG), 2023). Another reason for evaluating systems is to understand the difficulty/ ease of upgrading the controls and the budgets required for becoming quantum ready.

Assess the criticality of cryptographic systems within the organization. Understanding the criticality of the systems and information within the organization's IT environment is necessary to develop the correct strategies. Organizations will be able to better prioritize upgrades and initiatives.

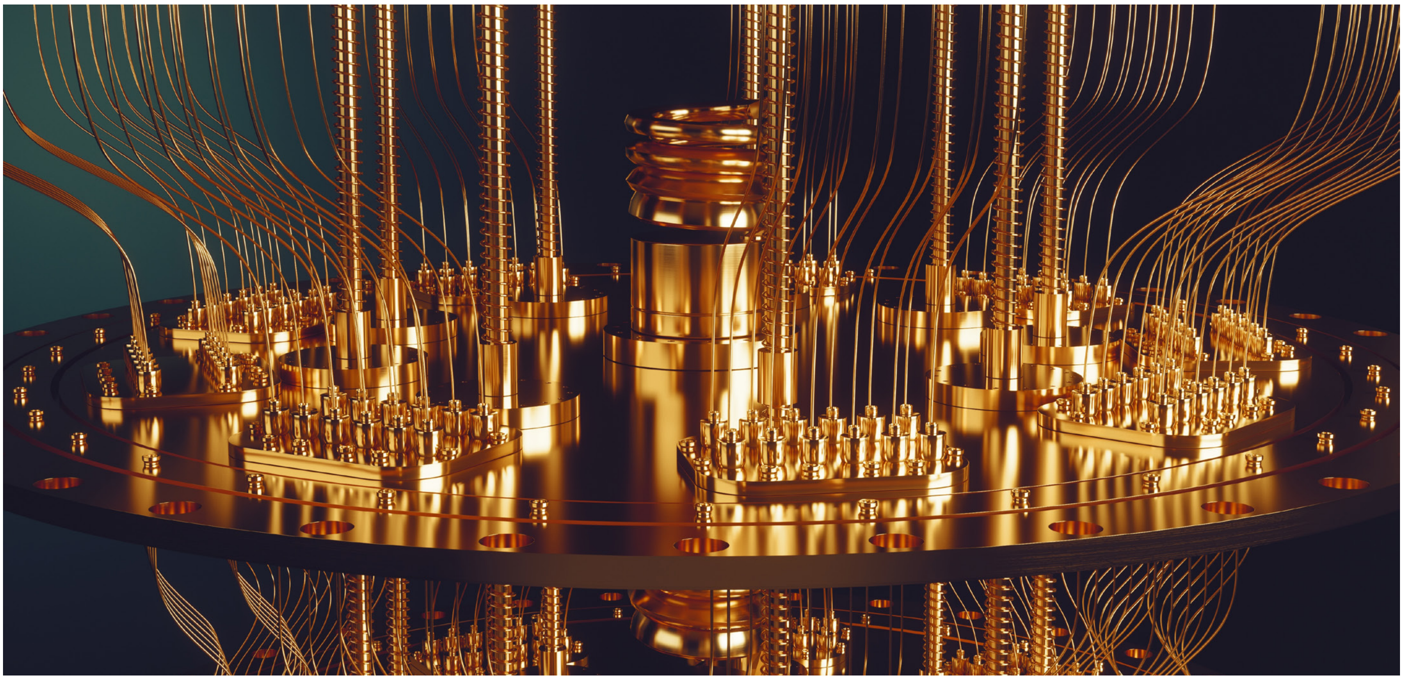
Understand the vulnerabilities with current cryptographic controls. There should be an understanding of how impactful a quantum related cyberattack can be on an organization's systems (Quantum-Readiness Working Group (QRWG), 2023). It is important to understand the various vulnerabilities and risks that are in scope for an attack, and which organizational systems fall into each category.

Transitioning to a Quantum Resistant Environment

Integrate quantum-resistant processes into the IT environment. Critical cryptographic systems should be prepared to implement quantum-resistant algorithms, to reduce the risk and impact of a quantum powered cyberattack (Soutar, Knackstedt, & Kaiser, 2023).

Review and update policies to address cryptographic quantum threats. We recommend referencing NIST's post-quantum cryptography standards. Data classification schemes should be reassessed to address long terms decryption risks. Addressing policy sooner rather than later will help organizations adapt quicker and more effectively to quantum threats.

Update system life cycle plans to address the quantum threat. Addressing the quantum threat within system life cycles will ensure that the technical needs of the systems to counter quantum threats are addressed (Canadian Center for Cyber Security, 2025).



References

Boutin, C. (2022, July 5). NIST Announces First Four Quantum-Resistant Cryptographic Algorithms. Retrieved from NIST: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Canadian Center for Cyber Security. (2025, February). Preparing your organization for the quantum threat to cryptography (ITSAP.00.017). Retrieved from Government of Canada: https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016, April). Report on Post-Quantum Cryptography. Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf

Cybersecurity and Infrastructure Security Agency [CISA], N. S. (2023, August 17). QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY. Retrieved from Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf

Feynman , R. P. (1982). Simulating physics with computers. In R. P. Feynman, International Journal of Theoretical Physics (pp. vol. 21, no. 6–7, pp. 467–488). https://doi.org/10.1007/BF02650179.

Grover, L. K. (1996, May 29). A fast quantum mechanical algorithm for database search. Retrieved from Cornell University: https://arxiv.org/abs/quant-ph/9605043

Holton, W. C. (2025, February 16). quantum computer. Retrieved from Britannica: https://www.britannica.com/technology/quantum-computer

IBM. (2022, November 9). IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two. Retrieved from IBM Newsroom: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

NIST. (2016, December 20). Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. Retrieved from Federal Register: https://www.federalregister.gov/documents/2016/12/20/2016-30615/announcing-request-for-nominations-for-public-key-post-quantum-cryptographic-algorithms

NIST. (2024, August 13). What Is Post-Quantum Cryptography? Retrieved from NIST: https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

Quantum-Readiness Working Group (QRWG). (2023, June 12). Canadian National Quantum-Readiness BEST PRACTICES AND GUIDELINES. Retrieved from Canadian Forum for Digital Infrastructure Resilience (CFDIR): https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/cfdir-quantum-readiness-best-practices-v03.pdf

Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. In P. W. Shor, SIAM Journal on Computing (pp. vol. 26, no. 5, pp. 1484–1509). https://doi.org/10.1137/S0097539795293172.

Soutar, C., Knackstedt, C., & Kaiser, R. (2023). Quantum Cyber Readiness: Achieve resiliency in the Quantum Era. Retrieved from Deloitte: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/5x5%20Quantum%20Cyber%20Readiness1.pdf

The NIST PQC Team. (2022, March 24). PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates. Retrieved from NIST: https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

World Economic Forum. (2023, June 29). Quantum Readiness Toolkit: Building a Quantum-Secure Economy. Retrieved from World Economic Forum: https://www.weforum.org/publications/quantum-readiness-toolkit-building-a-quantum-secure-economy/