Canadian National Quantum-Readiness

BEST PRACTICES AND GUIDELINES

Version 01 – July 7, 2021

AUTHORED BY:

Quantum-Readiness Working Group (QRWG)
of the Canadian Forum for Digital Infrastructure Resilience (CFDIR)

TLP:WHITE

The contents of this document are **TLP:WHITE**

CONTENTS

FOREWORD

The Bank of Canada is committed to working with its public- and private-sector partners to promote and strengthen the resilience of Canada's financial sector in the face of risks to business operations, including cyber incidents.

That's why we were pleased to take part in the Quantum-Readiness Working Group (QRWG) launched in 2020 by the Canadian Forum for Digital Infrastructure Resilience (CFDIR). A team of subject matter experts from organizations responsible for core elements of Canada's financial critical infrastructure has been studying what it will take to make Canada "quantum ready" in the years ahead.

The key message I want to leave you with is that we all need to start preparing now. The encryption technologies that are securing Canada's financial systems today will one day become obsolete. If we do nothing, the financial data that underpins Canada's economy will inevitably become more vulnerable to cyber criminals.

While some still see quantum as a long way off—given that this advanced encryption technology is not yet available—we also know that it will take time to develop and implement the quantum-safe encryption systems to replace those we have now.

The information and recommendations you see in this document were assembled and developed by people who are responsible for making these kinds of changes in their own institutions. The concepts are fundamental—with application to both small and large organizations, in both the public and private sector settings.

It starts with assessing the potential impact of quantum on your own organization. In addition to risks, quantum may also present opportunities. But no matter what, we all need to prepare for this transition—including in my own organization, the Bank of Canada. The resilience of Canada's financial system depends on it.

We would like to thank our colleagues who took part in this initial pilot project. There is a long road ahead, and the Bank of Canada will be there alongside our partners as the quantum issue unfolds.

Hisham El-Bihbety

CISO – Bank of Canada

ACKNOWLEDGEMENTS

The contents of this document were developed during the course of CFDIR Quantum-Readiness Working Group meetings between July 2020 and June 2021.

The information and recommendations contained herein were informed by the active participation and engagement of subject matter experts from the following organizations (listed alphabetically):

CFDIR MEMBERS:

BlackBerry, CCCS, CIRA, Google, IBM Canada, ISED, Microsoft Canada, Quantum-Safe Canada

QUANTUM-READINESS PILOT PROJECT PARTICIPANTS:

Bank of Canada, BMO, CIBC, Desjardins, Manulife, RBC, Scotiabank, 2Keys

QUANTUM-SAFE ECOSYSTEM STAKEHOLDERS:

Crypto4A, Entrust, evolutionQ, InfoSec Global, ISARA

A FEW WORDS ON CRYPTOGRAPHY

Throughout this document, the terms “cryptography” and “crypto” mean the practice of cryptography, which includes constructs such as encryption, digital signatures, hashing, and more. In particular, the term “crypto” does not refer to cryptocurrency, which is a form of unregulated digital currency that utilizes cryptography and often blockchain technologies.

REVISION HISTORY

The following table describes the dates of the major changes to this document.

Authors	Date / Version	Notes
CFDIR QRWG Participants, (July 2020 – June 2021)	July 7, 2021 / v.01	Initial version of recommended Best Practices developed from the QRWG's pilot project with members of Canada's Finance CI sector.

1. INTRODUCTION

Cryptographic technologies are used throughout government and industry 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. [1]

> ***Quantum computers will break currently deployed public-key cryptography, and significantly weaken symmetric key cryptography, which are pillars of modern-day cybersecurity. Thus, before large-scale quantum computers are built, we need to migrate our systems and practices to ones that cannot be broken by quantum computers. For systems that aim to provide long-term confidentiality, this migration should happen even sooner.***
>
> Cybersecurity in an era with quantum computers: will we be ready?
> *Michele Mosca, November 2015*

Canadians rely on cryptographic systems to secure their applications and websites, and to protect the confidentiality and integrity of their data from domestic and global cyber threat actors. Quantum computers, when used by malicious actors, will be able to break many of today's cryptographic systems. To counter this threat, digital systems that process, store, or transmit sensitive or confidential information will need to be upgraded to use new "quantum-safe" Post-Quantum Cryptography (PQC).

Unfortunately, quantum-resistant solutions are not yet available. The U.S. National Institute of Standards and Technology (NIST) began work on new standards for PQC in 2015, and hopes to release draft standards for public comments in 2022-2023.

> ***If your organization stores or communicates sensitive information, the use of post-quantum cryptography will be an inevitability in the next few years. To make this transition as smooth as possible, there are practical steps you can and should be taking to ensure your sensitive information remains secure both now and in the future.***
>
> Forbes magazine, *January 8, 2021*

The good news is there should be enough time for Canadian businesses and other organizations, including Critical Infrastructure (CI) owners and operators, to plan an orderly and cost-effective transition to quantum-safe cryptography over the next few years, using the recommended practices and guidelines in this document.

[1] Migration to Post-Quantum Cryptography U.S. National Institute of Standards and Technology (NIST), June 2021

1.1 OBJECTIVE

The goal of this document is to provide a set of recommended practices and guidelines:

- that Canadian Critical Infrastructure sector stakeholders and others can use now, to plan and prepare for how they will transition their digital systems to use new quantum-resistant cryptographic technologies and solutions; and
- to shorten learning curves by offering tangible advice and examples that illustrate "how to" undertake the recommendations made herein, so as to reduce the need for organizations to "start from scratch".

This document will be updated annually, to reflect industry feedback from implementing the best practices presented herein, and to provide additional examples of "how to" operationalize more of the strategic recommendations described in Section 3.

1.2 THE QUANTUM THREAT

Asymmetric cryptography, or public-key cryptography, provides confidentiality and integrity for sensitive information. It is used extensively by the Government of Canada (GC) and by private sector organizations to secure and protect communications networks, cryptographic keys during their distribution, data at rest, and more. Most organizations currently rely on public-key cryptography to secure:

- **digital signatures**: used to provide source authentication and integrity authentication as well as support the non-repudiation of messages, documents, or stored data;
- **identity authentication processes**: to establish an authenticated communication session or authorization to perform a particular action;
- **key transport of symmetric keys** (e.g., key-wrapping, data encryption, and message authentication keys) and other keying material (e.g., initialization vectors); and
- **privilege authorization processes**.

Security implications of quantum computing:

Current encryption protocols, such as Secure Socket Layer (SSL) and Transport Layer Security (TLS), based on existing public-key algorithms, are capable of protecting network communications from attacks by classical computers.

A fault-tolerant quantum computer, however, could break the mathematical challenges that underlie these and other protocols in a matter of hours or even seconds.

Deloitte Insights, April 2021

Asymmetric cryptography is based on the premise that two or more parties exchange public keys to establish a shared secret key to encrypt data. Symmetric cryptography on the other hand is based on the premise that all parties have already shared the exact same key prior to communicating.

Once developed, quantum computers will be able to use quantum physics to efficiently process information and solve problems that are impractical to solve using current computing technologies. Quantum computers will be able to compromise the algorithms used in asymmetric cryptography. This means that all classified, sensitive, and/or confidential information and communications that were protected using public-key cryptography, especially those having a medium to long-term intelligence value or commensurate need for long-term confidentiality, will be vulnerable to decryption by adversaries or business competitors that have quantum computers.[2]

1.3 WHY START PREPARING NOW?

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

a) cryptographic technologies are integrated into most of the digital products commonly used by organizations to run their daily operations; [3]

b) 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;

c) fault-tolerant quantum computers, capable of breaking existing encryption algorithms and cryptographic systems (e.g., public-key infrastructures), are widely expected to be available within the above timeline;

d) the time needed to migrate installed cryptographic technologies (e.g., SHA1) to something newer can take many years; [4]

e) the number of cryptographic systems that organizations will need to migrate to use new "quantum-safe" cryptography will be large; and

---

2 Mandatory GC Quantum Computing Threat Mitigation (ITSB-127) - Canadian Centre for Cyber Security, May 2019

3 Using Encryption to Keep Your Sensitive Data Secure (ITSAP.40.016) - Canadian Centre for Cyber Security, May 2021

4 The SHA1 hash function is now completely unsafe | Computerworld, February 2017

f) most organizations have no clear view of the cryptographic technologies used by their existing Information Management (IM), Information Technology (IT) and Operational Technology (OT) systems; this will make it difficult to discover and then prioritize the systems to be upgraded to post-quantum cryptography. [5]

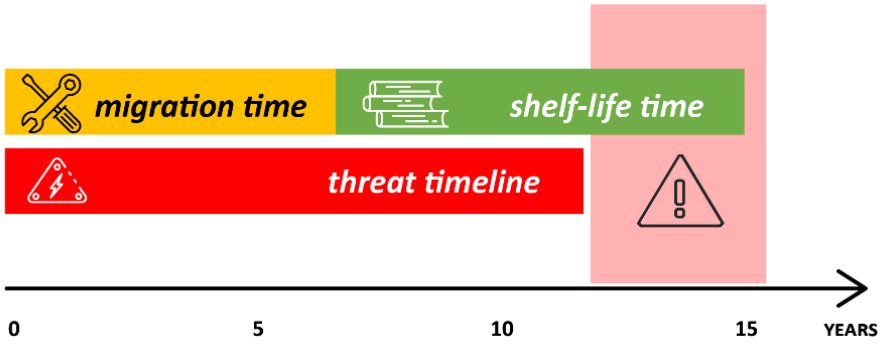
Business owners and systems operators will need time to determine the effort that will be needed to migrate their existing cryptographic systems to use new, post-quantum cryptography. Migrating an organization's cryptographic systems to PQC will require significant effort. Organizations should begin planning now given that:

- the effort and time needed (e.g., to investigate, analyse, plan, procure, migrate, and validate new PQC) will not be small, and it will be different for every organization, and
- the amount of time remaining (until threat actors can access sufficiently powerful quantum computers to break existing cryptography) will decrease every day.

1.4 HOW MUCH TIME IS AVAILABLE?

The amount of time that an organization will have to transition its systems to use new quantum-safe cryptography (QSC) depends on three factors:

- the ***migration time***: the number of years the organization will need to migrate all of the systems that handle its important data to new quantum-safe cryptography;
- the ***shelf-life time***: the number of years that the organization's important, high-value information needs to be protected; and
- the ***threat timeline***: the number of years before relevant threat actors will be able to break the organization's existing, quantum-vulnerable, cryptography. [6]



[5] Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms (nist.gov), April 28, 2021

[6] Quantum Threat Timeline Report for 2020, Global Risk Institute, January 27, 2021

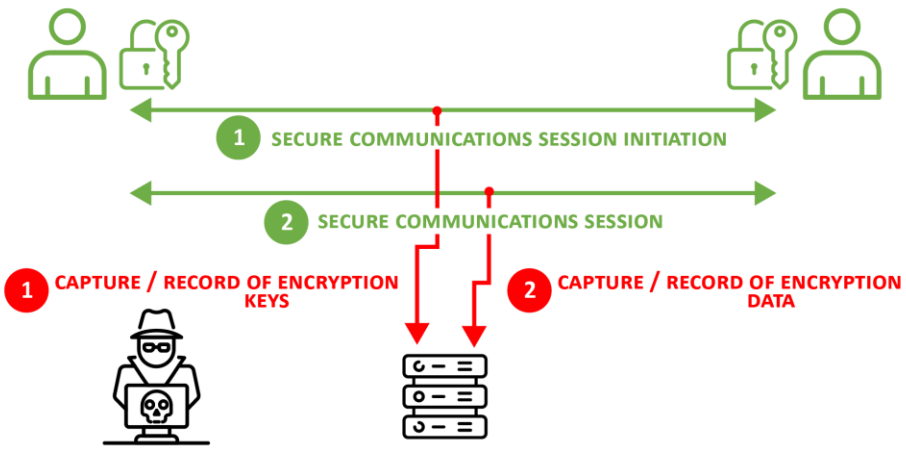
As illustrated above:

- organizations may need many years to migrate to QSC; and
- many organizations have important information (e.g., trade secrets, customer data, business plans) that they wish to keep confidential for a long time.

In the worst case, a threat actor will be able to use a quantum computer to break the encryption protecting important information before that data is protected by QSC.

Some threat actors (e.g., nation state level adversaries) are known to be harvesting copies of encrypted information today, and storing it for decryption in the future. Thus, any information that needs to be kept confidential for a long time (e.g., more than 10 years) may already be at risk of "harvest now, decrypt later" attacks. It must be noted that the shelf-life time for critical data and information such as trade secrets can be over 50 years.

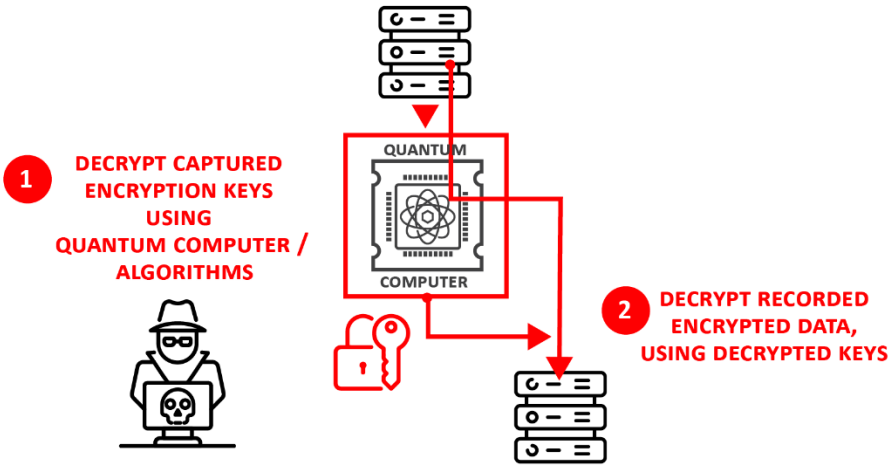
Today



	Users	Threat Actor
1	Secure communications session initiation includes crypto key exchanges	Capture / Record Encryption Keys
2	Encrypted session	Capture / Record encrypted data

Risk Mitigation Actions
Leverage information security and cyber security best practices and controls to help reduce current risks

In the best case, organizations that begin to assess their quantum-readiness now will have time to migrate their most important systems to use quantum-resistant cryptography before threat actors (and business competitors) obtain quantum computers.

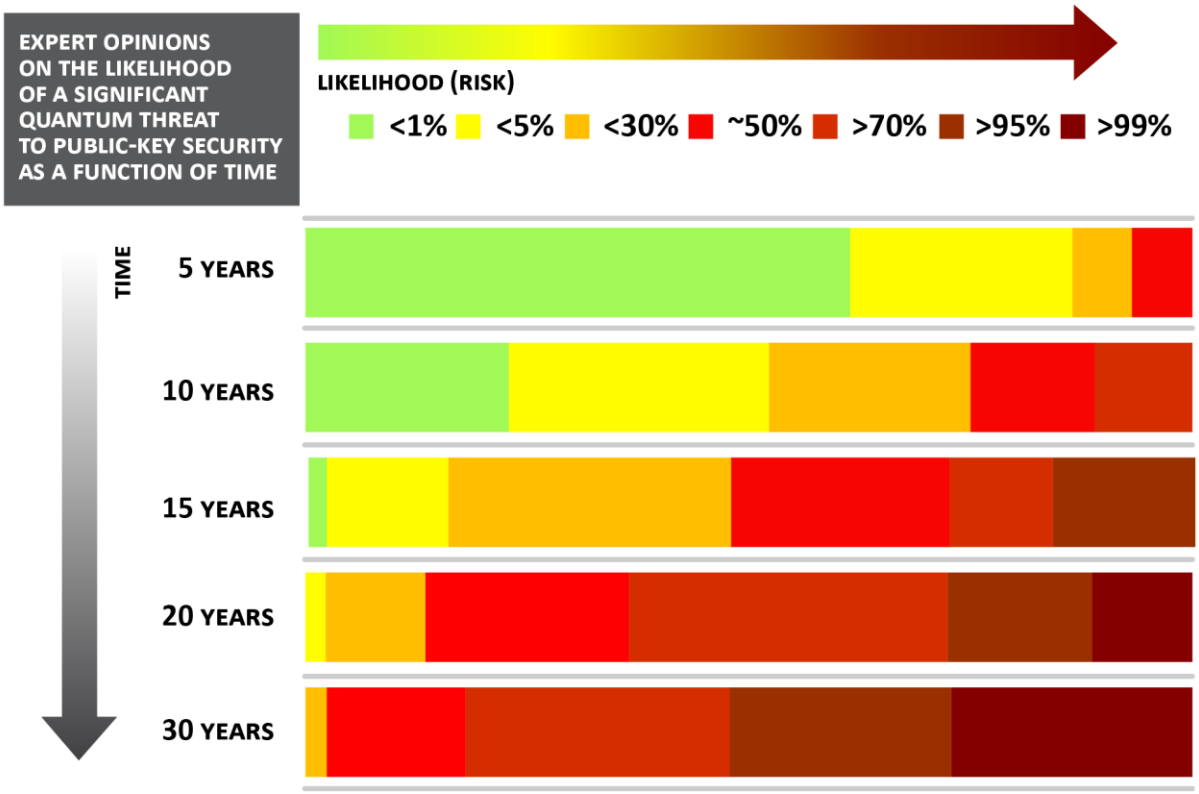
Future


	Threat Actor
1	Captured encryption keys are decrypted using large scale quantum computers and quantum algorithms
2	Decrypted keys enable the decryption of captured encrypted data

Risk Mitigation Actions

Immediate start of Quantum Readiness planning and actions to prepare for future quantum threats

With respect to the threat timeline, the figure below summarizes the latest opinions of 44 global quantum experts. Every organization will need to review information such as this, and then decide on how much time they have, based on their own risk tolerance.



Numbers reflect how many experts (out of 44) assigned a certain probability range.

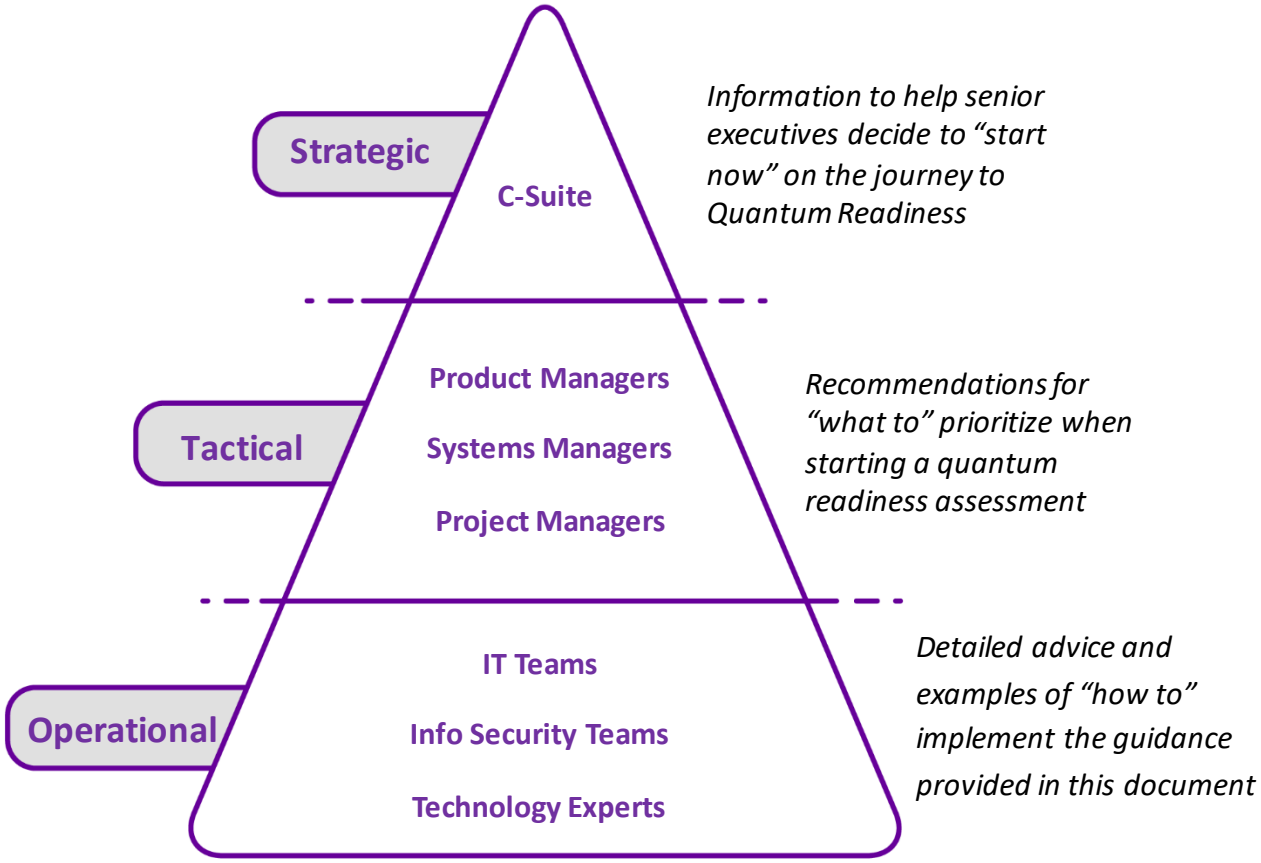
Quantum Threat Timeline Report 2020,
Global Risk Institute, January 7, 2021

1.5 ABOUT THIS DOCUMENT

In June 2020, the Canadian Forum for Digital Infrastructure Resilience (CFDIR) chartered its Quantum-Readiness Working Group (QRWG) to conduct a one-year "quantum readiness" pilot project with stakeholders from Canada's Finance CI sector. That project included discussions, discoveries and in-depth examination of many of the key considerations that C-suite executives, their direct reports, and their IM, IT, and OT staff will need to address to evolve their existing cryptographic systems to be "quantum-ready" (i.e., quantum-safe) in the coming years.

This document, and its suite of companion slide decks, provide foundational building-block information and material that can be used and adapted by organizations as needed to raise awareness and to inform business and technology decision makers on why and how to begin their Quantum-Readiness journey.

The contents of this document include strategic, and tactical recommendations (in Sections 3 – 5) and operational advice (e.g., sample "how to" guides in its Annexes).



2. SOURCES OF INFORMATION

The sources of information used to formulate the practices and guidelines recommended in this document have been drawn from an extensive variety of sources in the public domain, and from discussions and deliberations within the CFDIR QRWG.

Primary sources include:

- Canadian Centre for Cyber Security (CCCS) Publications;
- U.S. National Institute of Standards and Technology (NIST) Computer Security Resource Center Publications on Post-Quantum Security;
- European Telecommunications Standards Institute (ETSI) Quantum-Safe Cryptography working group documents; and
- Internet Engineering Task Force (IETF) Request For Comments (RFCs) as appropriate.

Where appropriate in later sections of this document, links to specific publications from the above sources may be identified as "normative references". Normative documents are publications that must be read to understand or to implement the guidance being provided.

In contrast, some of the other sources highlighted in this document are referred to as "informative references". Informative documents help the reader to develop a better understanding of a particular subject area.

Informative sources cited in this document include:

- Open source magazine articles, peer-reviewed papers and conference proceedings;
- International Monetary Fund (IMF) and Global Risk Institute papers;
- Archived webcasts of expert panel discussions and presentations from relevant conferences; and
- Open source content (e.g., white papers, case studies, application notes) from private sector CFDIR member companies as well as other members of the ICT supply chain for "Quantum-safe" solutions.

3. RECOMMENDED QUANTUM-READINESS BEST PRACTICES

Executives are encouraged to ask their organizations to start work now:

- to understand and then manage the risks associated with quantum computing advancements; and
- to plan how they will transition to quantum-resistant cryptography.

Recommended actions that can be started now include: [7]

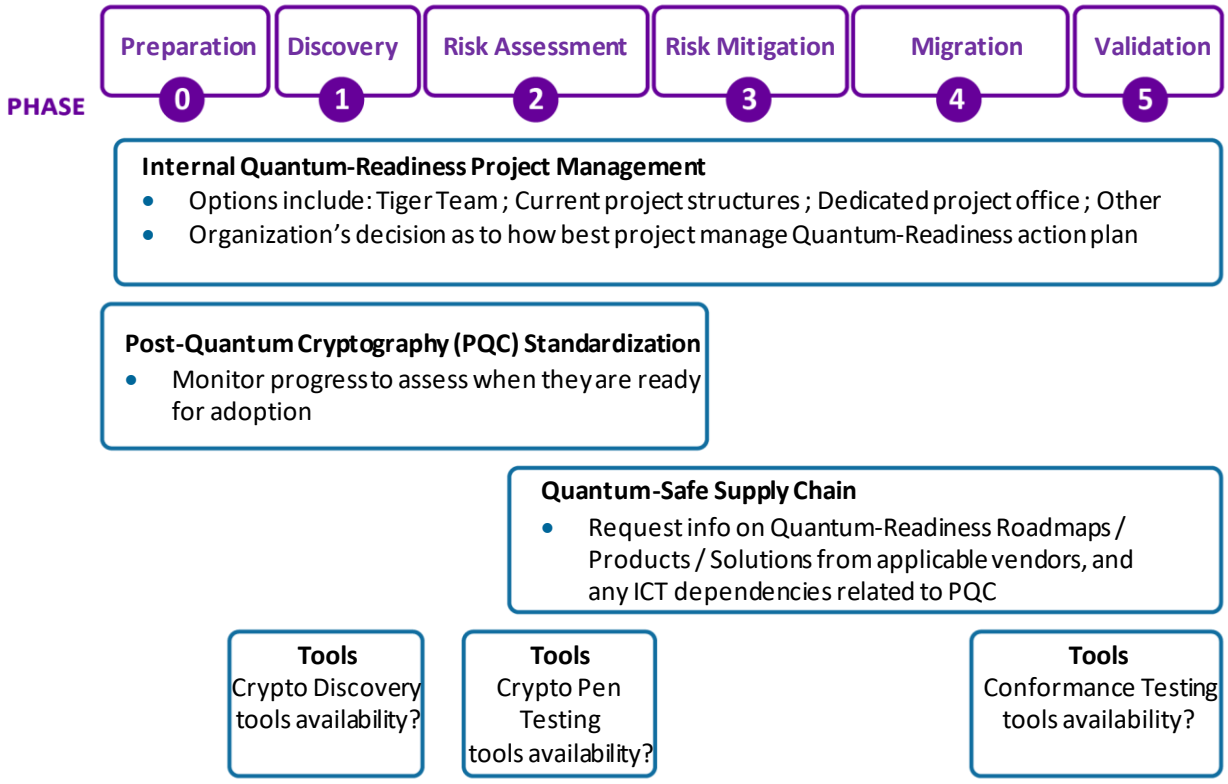
1. Updating and patching your Information Management (IM), Information Technology (IT) and Operational Technology (OT) systems frequently.
2. Ensuring that your vendors use standardized, validated cryptography (e.g., Federal Information Processing Standards [FIPS]).
3. Evaluating the sensitivity of your organization's information and determining its lifespan to identify information that may be at risk (e.g. as part of ongoing risk assessment processes)
4. Educating your teams on the emerging quantum threat to existing cryptography, as well as future quantum technologies.
5. Asking your vendors about their plans to implement quantum-safe cryptography (e.g. do your vendors plan to include quantum-safe cryptography in future updates, or will you need to acquire new hardware or software?).
6. Budgeting for potentially significant software and hardware updates, as the timeframe for necessary replacement approaches.
7. Updating your IM, IT, and OT life-cycle management plans to explicitly describe how and when your organization will implement post-quantum cryptographic algorithms to protect your most important data and systems starting 2024-2025, or when validated cryptographic modules become available (e.g., a year later).

[7] Preparing Your Organization for The Quantum Threat to Cryptography (ITSAP.00.017) - Canadian Centre for Cyber Security, February 2021

With respect to organizing the recommended actions into a Quantum-Readiness program, a multi-year and multi-phase timeline is recommended, as described below.

Quantum-Readiness Program Elements

Some Conceptual Building Blocks



While recognizing that every business is unique and that no one size fits all, each organization's unique Quantum-Readiness work plan should progress through the following project ***Stages*** and ***Phases***:

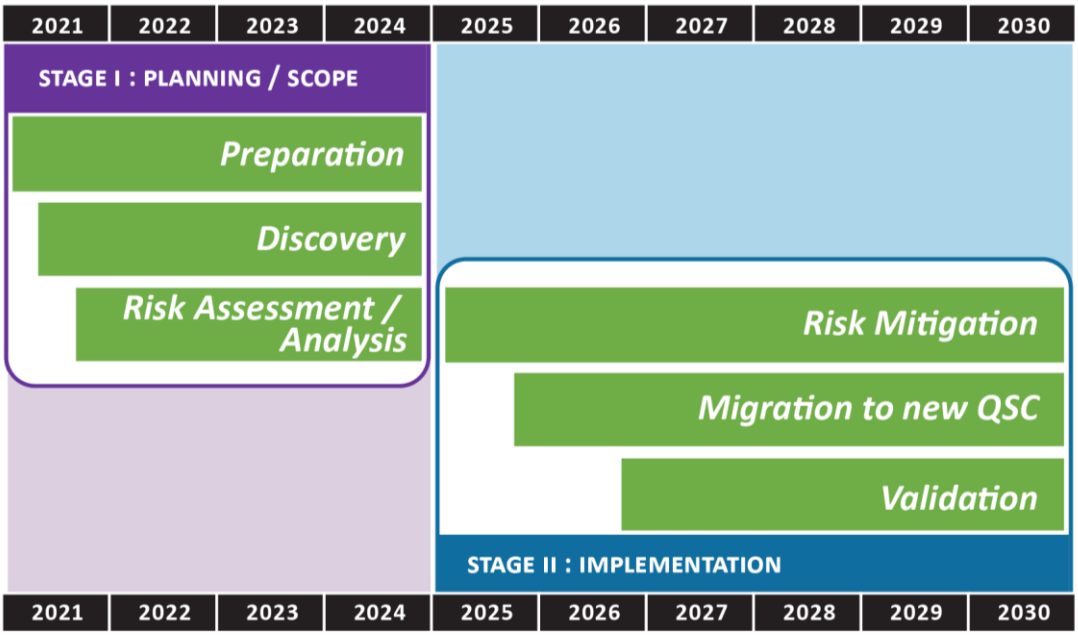
- **Stage I: Initial Planning & Scoping**, managed as three distinct project phases that should all be well underway before the standards for new Post-Quantum Cryptography (PQC) are completed in 2024:
    0. Preparation
    1. Discovery
    2. Quantum Risk Assessment

- **Stage II: Implementation,** starting in 2025, also consisting of three distinct phases:
    3. Quantum Risk Mitigation
    4. Migration to new QSC
    5. Validation

The participants in the CFDIR QRWG's initial pilot project recommend the following timeline be used to set expectations with respect to the amount of time that will be needed to achieve full quantum-readiness.

Quantum-Readiness Program Timeline

Initial Recommendations as of June 2021



The anticipated duration (in years) for each Stage and Phase shown above is the consensus view of the participants in the CFDIR QRWG's initial pilot project with members of Canada's Finance CI sector from July 2020 to June 2021.

Sections 3.0 to 3.2 of this document recommend ***Planning and Scoping*** actions and best practices for the first three phases. They describe what an organization needs to do to start preparing their IM, IT, and OT systems for new quantum-safe technologies between now and 2024.

Future versions of this document will offer additional guidance and recommended best practices for the post-2024 ***Implementation*** phases.

3.0 STAGE I - PREPARATION (PHASE 0)

(RECOMMENDATIONS FOR C-SUITE EXECUTIVES)

1. Develop an understanding of the threats that quantum computing will pose for your ICT infrastructure in the coming years. Request a briefing within 6 months.

   Normative references:

   - **CCCS**: ITSE.00.017 – Addressing the Quantum Computing Threat to Cryptography
     May 2020, 1 page
   - **NIST**: Cybersecurity White Paper - Getting Ready for PQC April 2021, 10 pages

   Informative references:

   - U.S. NCCoE: Post-Quantum Cryptography Challenges From a Customer Point of View
     September 2020, 18 minute webinar
   - U.S. NCCoE: The Long and Agile Transition - How Industry Needs to Prepare
     September 2020, 14 minute webinar

2. Ask one (or more) of your staff to form a team to investigate the scope of the effort that will be needed for your organization to start using new "quantum-resistant" cryptography in the coming years, and to identify which of your IM, IT and/or OT systems may need be remediated first.

   Normative references:

   - **CCCS**: ITSAP.00.017 – Preparing Your Organization for the Quantum Threat to Cryptography February 2021, 2 pages
   - **ETSI**: TR 103 619 - V1.1.1 - CYBER; Migration strategies and recommendations to Quantum Safe schemes (etsi.org) July 2020, 21 pages

   Informative references:

   - CCCS: ITSB-127 Quantum Threat Mitigation (cyber.gc.ca) May 2019, 4 pages
   - ETSI, IQC: Quantum readiness and resilience of the digital economy | TelecomTV
     October 2020, 27 minute panelled webinar

3. Request periodic reporting on the progress of #2 (e.g., quarterly) and decide when to advance to Phase 1 (Discovery), as described in Section 3.1 of this document.

   Informative references:

   - Internet Society: Cryptography: CEO Questions for CTOs March 2018, 15 pages

4. Email the CFDIR Secretariat with any questions on the above.

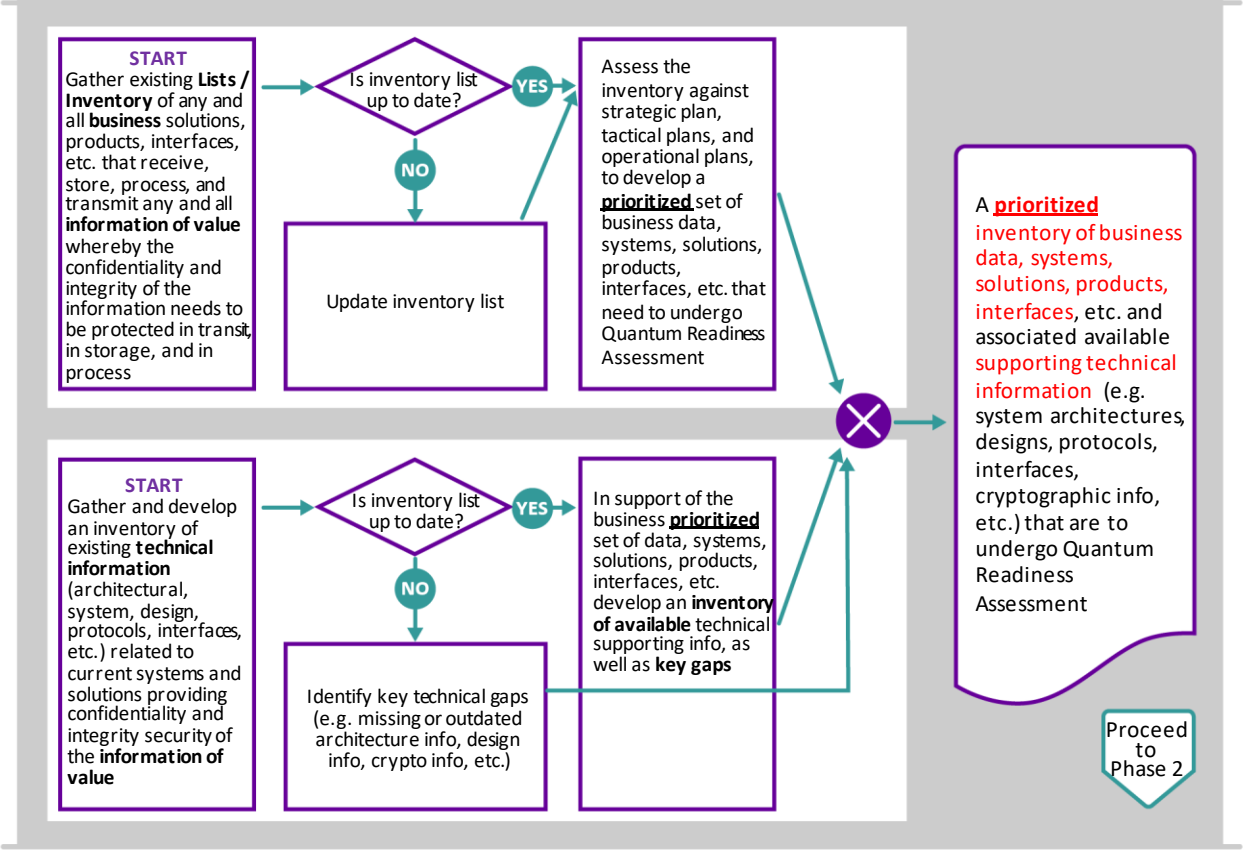
3.1 STAGE I - DISCOVERY (PHASE 1)

(RECOMMENDATIONS FOR C-SUITE EXECUTIVES AND THEIR DIRECT REPORTS)

5. Review the information to be collected during this phase, as illustrated in the diagram below.

   - The goal is discover where and how cryptographic products, algorithms and protocols are used by your organization to protect the confidentiality and integrity of your organization's important data and digital systems.
   - The information collected during this phase will be needed to assess your organization's quantum risks in Phase 2.

Phase 1 : Flow Chart : DISCOVERY



6. Appoint and empower someone to plan and execute a detailed discovery of where and how public-key cryptography is used by your organization.

   Informative reference:

   - Forbes Technology Council: Three Practical Steps To Prepare Your Business For The Quantum Threat January 8, 2021, 5 pages

7. Investigate whether using automated tools would facilitate your crypto discovery. Organizations should balance their security needs with their needs for usability and availability when considering such automated tools.

   Informative references:

   - NIST: Migration to Post-Quantum Cryptography - Project Description June 2021, Pages 4-5
   - NIST: Guide to Enterprise Patch Management Technologies July 2013, 26 pages
   - Forbes Technology Council: Building a Strong Cryptography Strategy (Part I): Securing Your Data Assets April 20, 2021, 3 pages

8. Build an inventory of where and how your organization uses public-key cryptography to protect its most important data and IM, IT and OT systems. Also identify any legacy cryptographic systems being used.

   Normative reference:

   - **ETSI**: TR 103 619 – V1.1.1 – CYBER; Migration strategies and recommendations to Quantum Safe schemes July 2020, pages 7-10

   Informative references:

   - Cryptosense Blog: What is Cryptographic Inventory? August 2, 2019
   - Cryptosense Blog: Cryptographic Inventory – Best Practice Tips June 3, 2020

9. Identify the important factors in which public-key cryptography affects the operation and security of your systems and applications (e.g., key sizes, latency and throughput limits, current key establishment protocols, how each cryptographic process is invoked, dependencies).

   Normative references:

   - **CFDIR QRWG**: Content Needed to Describe an Organization's Uses of Crypto, Annex C of this document
   - **CFDIR QRWG**: Using Kerberos for Authentication, Annex D of this document
   - **CFDIR QRWG**: PKI/CAs, Annex E of this document
   - **CFDIR QRWG**: sFTP, Annex F of this document

   Informative reference:

   - NIST: Getting Ready for Post-Quantum Cryptography Cybersecurity White Paper, April 28, 2021, Page 5

10. Analyze the findings from #8 and #9 to develop a prioritized list of your organization's most important quantum-vulnerable systems that must be protected.

    Informative references:

    - CCCS: ITSAP.00.017 – Preparing Your Organization for the Quantum Threat to Cryptography February 2021, 2 pages

3.2 STAGE 1 – QUANTUM RISK ASSESSMENT (PHASE 2)

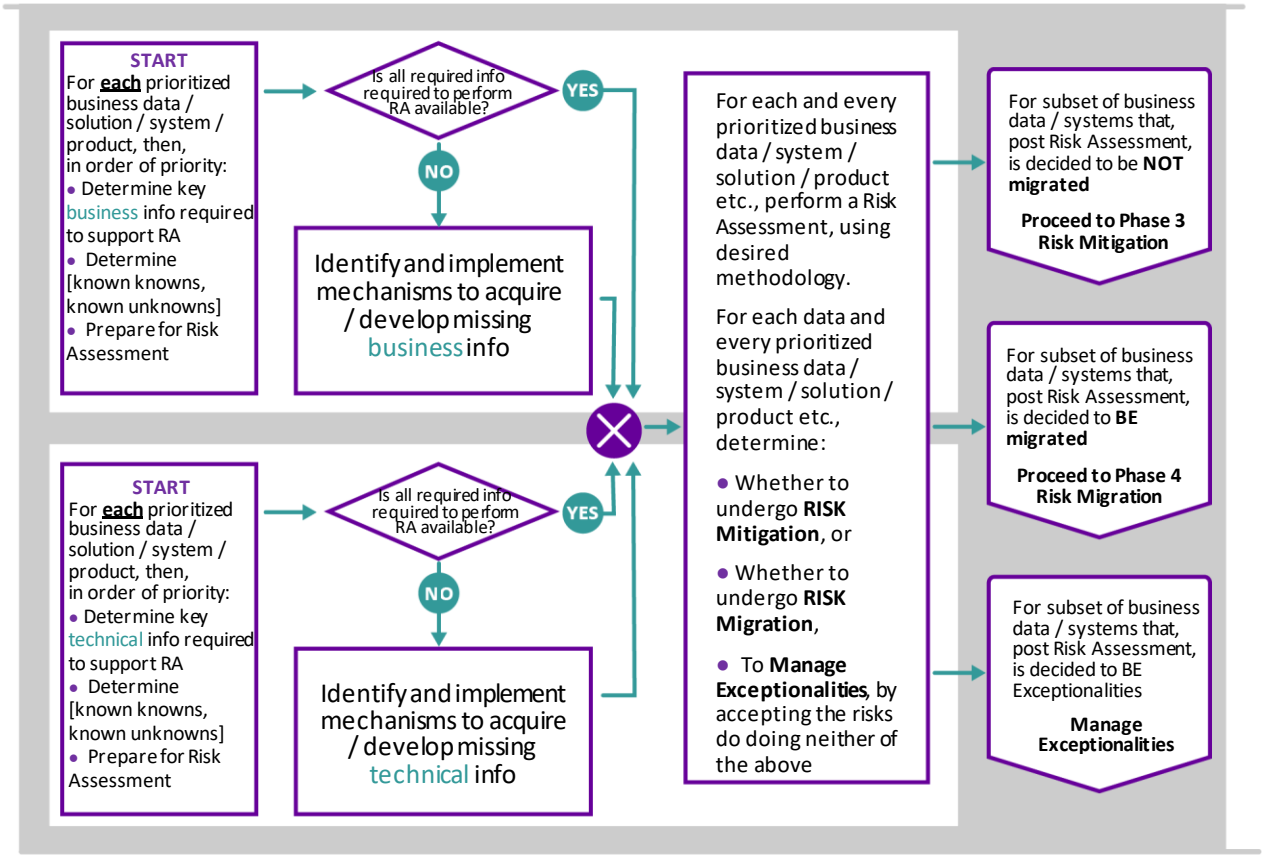
(RECOMMENDATIONS FOR IM, IT, OT MANAGERS AND THEIR DIRECT REPORTS)

11. Review the objectives of this Phase, as illustrated in the diagram below.

The objectives include:

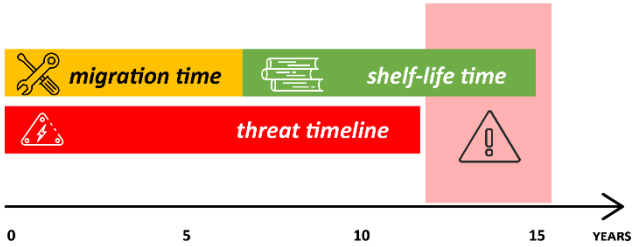
- Evaluating the sensitivity of your organization's information and determining its lifespan to identify the information that may be at risk (e.g. as part of ongoing risk assessment processes).
- Educating yourself and your teams on the threats that quantum computing will pose to your existing uses of cryptography.
- Asking your IM, IT and OT vendors and suppliers about their plans and timetables to implement quantum-resistant cryptography and crypto-agility, to understand any new hardware or software that will be needed.
- Reviewing your IT lifecycle management plans and budgeting for potentially significant software and hardware updates.

Phase 2 : Flow Chart : RISK ASSESSMENT (RA)



12. Start your Quantum Risk Assessment by reviewing the quantum risk equation introduced in Section 1.4, and the inventory of information discovered in Phase 1. That information is needed to determine the following variables for each of the digital systems that handle or store your organization's most sensitive information:

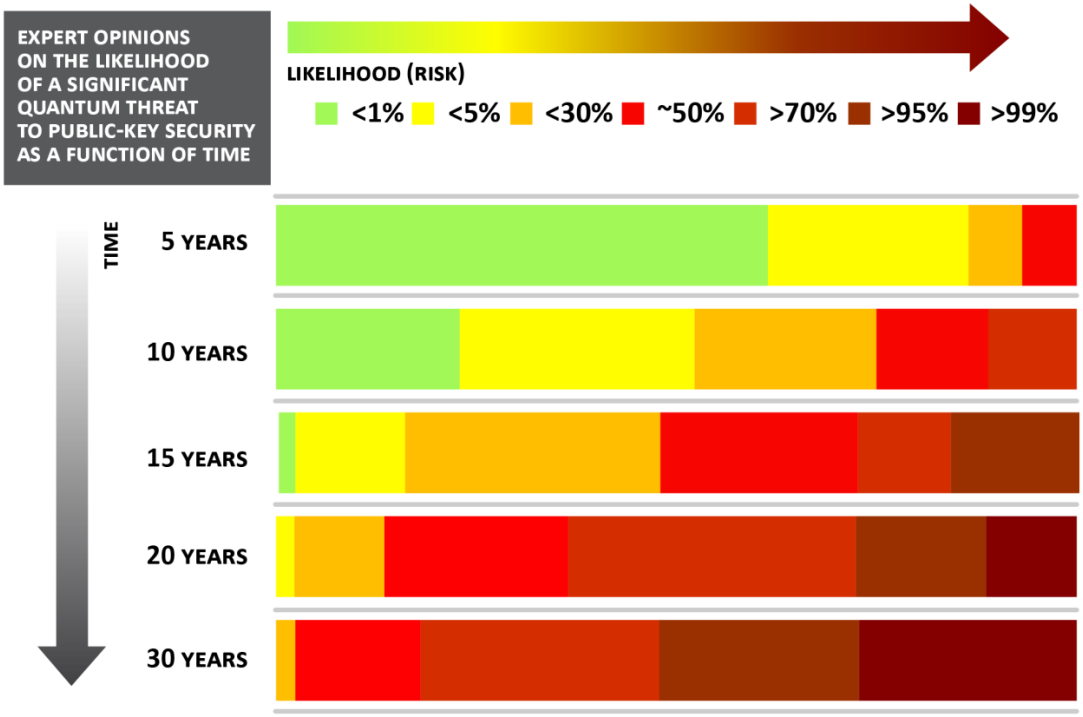
    - the ***shelf-life time*** (measured in years) that your most important data must be protected; and
    - the ***migration time*** *(measured in years)* that your organization will need to upgrade the systems, to be quantum-safe, that handle your longest shelf-life data.



Normative reference:

- **evolutionQ**: Managing the quantum risk to cybersecurity
  11 April 2016, pages 16-20

13. Decide how the currently anticipated quantum ***threat timeline*** affects your organization's risk posture. To do this, review open source information such as the following, and then determine your threat timeline based on your risk tolerance.



Numbers reflect how many experts (out of 44) assigned a certain probability range.

Normative reference:

- **Global Risk Institute**: Quantum Threat Timeline Report 2020 January 2021, 52 pages

14. Evaluate the sensitivity of your organization's information and determine its lifespan (i.e., the ***shelf-life time*** that your most important data must be protected) to identify information that may be at risk.

Normative reference:

- **CCCS**: ITSAP.00.017 – Preparing Your Organization for the Quantum Threat to Cryptography February 2021, Page 2

15. Review your technology lifecycle management plans for each of the quantum-vulnerable systems identified in step #10 of Phase 1. Ask your IM, IT and OT vendors if their product development roadmaps include supporting crypto-agility and/or quantum-resistant cryptography in future updates. If yes, ask when those capabilities will be available.

Normative reference:

- **CCCS**: ITSAP.00.017 – Preparing Your Organization for the Quantum Threat to Cryptography February 2021, Page 2

16. Using the information from #15, estimate the ***migration time*** *(measured in years)* that your organization will need to migrate each of the systems that handle your longest shelf-life data.

Informative reference:

- NIST: Migration to Post-Quantum Cryptography - Project Description June 2021, Page 6, Lines 197-216

17. Prioritize the systems that will need the most urgent attention, by listing all of the systems that handle important data for which:

$$\text{Migration Time} + \text{Shelf-life Time} > \text{Threat Timeline}$$

Informative reference:

- Journal of Cybersecurity: Crypto Agility Risk Assessment Framework 30 April 2021, Pages 5-9

18. For each dataset, product, system, or solution flagged in #17, determine:

- whether to undergo risk mitigation (per Phase 3), or
- whether to start migration to PQC (per Phase 4), or
- to manage exceptionalities, by accepting the quantum risk and doing neither of the above.

Informative references:

- **Boston Consulting Group**: Ensuring Online Security in a Quantum Future March 2021, 11 pages
- NIST: Migration to Post-Quantum Cryptography - Project Description June 2021, Lines 130-155

19. Also determine if your staff will need new training or additional resources (e.g., tools) to migrate your systems to use quantum-safe, post-quantum cryptography. If yes, the time needed to obtain those tools and/or training should be factored into the per-system migration time estimates developed in #16.

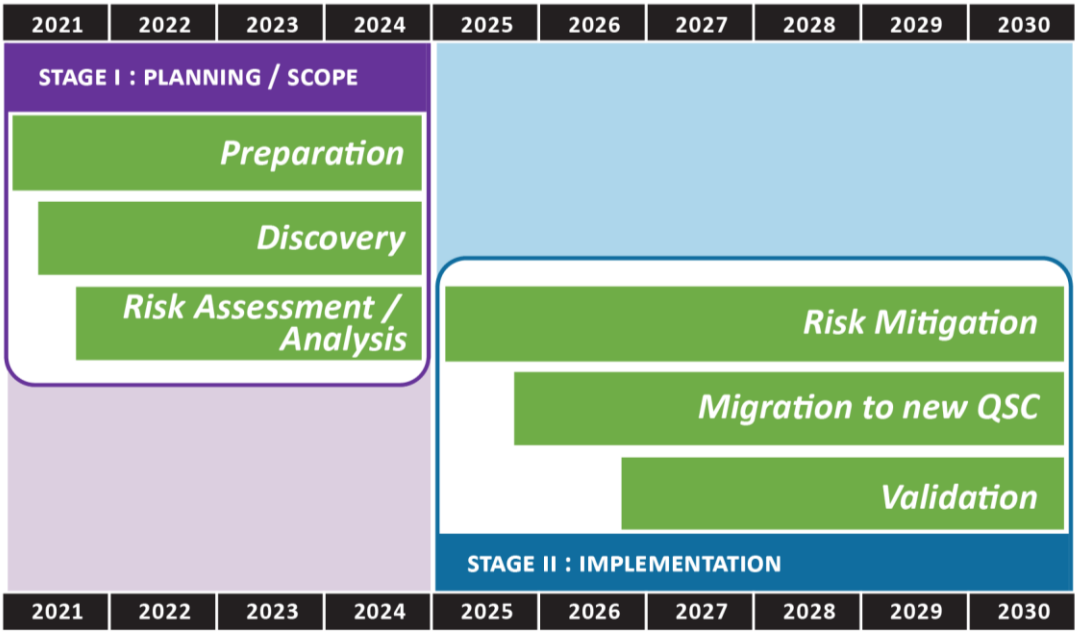
3.3 STAGE II – IMPLEMENTATION PHASES 3, 4 AND 5

Future versions of this document will offer guidance and best practice recommendations for the three post-2024 ***Implementation*** phases, namely:

- Quantum Risk Mitigation (Phase 3)
- Migration to new Quantum-Safe Cryptography (Phase 4)
- Validation (Phase 5)

Quantum-Readiness Program Timeline

Initial Recommendations as of June 2021



The CFDIR QRWG's second 12-month project from July 2021 to June 2022 will inform the above, as will relevant initiatives in other jurisdictions. For example, during June 2021, the U.S. National Cybersecurity Center of Excellence (NCCoE) within NIST invited public comments on a draft project description for ***Migration to Post-Quantum Cryptography***. [8] See Appendix C for more information.

[8] Migration to Post-Quantum Cryptography - Project Description NIST, June 4, 2021, 16 Pages

Other work that will be considered in the next release of this document include publications from the European Union Agency for Cybersecurity (ENISA) and the Internet Engineering Task Force (IETF).

In May 2021, ENISA updated its report on ***Post-Quantum Cryptography – Current state and quantum mitigation*** [9] to introduce two near-term options for Quantum Mitigation:

> ***If you encrypt data that needs to be kept confidential for more than 10 years and an attacker could gain access to the ciphertext you need to take action now to protect your data.***
>
> ***The first option is to already migrate to so called hybrid implementations that use a combination of pre-quantum and post-quantum schemes.***
>
> ***The second option is to employ the conceptionally easy, but organizationally complicated measure of mixing pre-shared keys into all keys established via public-key cryptography.***

In April 2021, the IETF agreed to recharter one of its working groups because *recent progress in the development of quantum computers pose a threat to wide deployed public key algorithms.* [10]

One of the Internet-Drafts being developed within the IETF's LAMPS working group is particularly relevant:

> ***During the transition to post-quantum cryptography, there will be uncertainty as to the strength of cryptographic algorithms; we will no longer fully trust traditional cryptography such as RSA, Diffie- Hellman, DSA and their elliptic curve variants, but we will also not fully trust their post-quantum replacements until they have had sufficient scrutiny.***
>
> ***Unlike previous cryptographic algorithm migrations, the choice of when to migrate and which algorithms to migrate to, is not so clear. Even after the migration period, it may be advantageous for an entity's cryptographic identity to be composed of multiple public-key algorithms.***
>
> *Composite Keys and Signatures for Use In Internet PKI*
> *IETF LAMPS working group, January 2021*

[9] https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation/at_download/fullReport , May 2021, pages 25-27.

[10] IETF LAMPS WG Charter, v.06, May 2021, Section 5

4. AWARENESS AND SKILLS DEVELOPMENT

Creating an effective quantum risk awareness program will be important for every organization that uses cryptography, large or small, in the coming years.

The CFDIR QRWG developed a suite of slide decks to provide foundational building-block information and materials that can be used and adapted by organizations as needed to raise awareness and to inform decision makers and staff on why and how to begin their Quantum-Readiness journey. These decks may be obtained by emailing the CFDIR Secretariat.

	Contents & Focus	Pages	File Name	Version & Date
1	**Introduction & Context**	5	Quantum-Readiness-WG-Overview-v01	Version 01 July 7, 2021
2	**Master Chart Deck**	62	Quantum-Readiness-Best-Practices-Guidelines-v01	Version 01 July 7, 2021
3	Subset of Master Chart Deck Example #1 – **Executive Primer**	2	EX-01-Quantum-Readiness-Exec-Primer-v01	Version 01 July 7, 2021
4	Subset of Master Chart Deck Example #2 – **Executive Overview**	8	EX-02-Quantum-Readiness-Exec-Overview-v01	Version 01 July 7, 2021
5	Subset Example #3 – **Executive Overview with backup slides**	34	EX-03-Quantum-Readiness-Exec-Overview-with-Backup-v01	Version 01 July 7, 2021
6	Subset Example #4 – **Detailed Overview for Managers**	32	EX-04-Quantum-Readiness-Mgmt-Overview-v01	Version 01 July 7, 2021
7	Subset Example #5 – **Detailed Overview for Managers with Backup slides**	60	EX-05-Quantum-Readiness-Mgmt-Overview-with-Backup-v01	Version 01 July 7, 2021
8	Subset Example #6 – **Detailed Overview for Implementors**	56	EX-06-Quantum-Readiness-Implementors-Overview-v01	Version 01 July 7, 2021

5. VENDOR ENGAGEMENT

Future versions of this document will offer guidance and best practices for the sub-sections listed below.

5.1 RECOMMENDED QUESTIONS FOR QSC VENDOR ENGAGEMENT

5.2 QSC PROCUREMENT CLAUSES FOR RFI'S AND RFP'S

6. CONCLUSION / KEY TAKEAWAYS

- Canadian businesses, organizations, and Critical Infrastructure owners and operators are advised to take action now, using the recommended practices and guidelines offered in this document, to begin planning an orderly and cost-effective transition to quantum-safe cryptography over the next few years to manage the risks that Quantum computers will pose to them.

Risks	
Cyber attack threat	• **Capture Now ; Replay and decrypt later ;** • **Data at Rest ; Data in Motion ;**
Key data at risk	• **Encryption keys ; PII ; Business "crown jewels" ; Intellectual Property**
Risk scope	• **Organization ; Customers ; Supply Chain ; Ecosystems ; Dependencies/Interdependencies**
Perform Organizational Quantum-Readiness Risk Assessment to determine risk	

- Given that every organization is unique, there can be no "one-size-fits-all" approach.

- Quantum-Readiness planning should be started now because migrating an organization's quantum-vulnerable systems to use new quantum-safe PQC will be a multi-year process.

Cryptography	
Discovery	• **Quantum-Readiness Best Practices Guidelines**
Quantum-Readiness	• **Canadian Centre for Cyber Security**
Crypto-Agility	• **Canadian Supply Chain for cryptographic products/services**
Organizations must prepare to upgrade / replace all cryptographic functions to standards-approved Post-Quantum Cryptography	

- Backward compatibility and interoperability between current and new cryptographic platforms, systems and solutions will be essential during the multi-year transition to QSC.

- Organizations should leverage all available information resources for the above, including but not limited to:
  - the recommendations presented in this document;
  - internal business and technical experts;
  - open source information; and
  - private sector Canadian and multi-national expertise and/or companies with experience and skills or products related to Quantum-Readiness.

Resources	
CFDIR Quantum-Readiness WG	• **Quantum-Readiness Best Practices and Guidelines**
Canadian Centre for Cyber Security	• **Open-source publications, including cryptographic guidance**
Canadian crypto supply chain	• **Canadian supply chain for cryptographic products/services**

Canadian as well as global resources available to help guide organizations prepare for Quantum-Readiness

ANNEX A: GLOSSARY

- CA - Certificate Authority
- CCCS - Canadian Centre for Cyber Security
- CFDIR - Canadian Forum for Digital Infrastructure Resilience
- CI - Critical Infrastructure
- DECT - Digital Enhanced Cordless Telecommunications
- ENISA - European Union agency for Cybersecurity
- FIPS - (U.S.) Federal Information Processing Standards
- HSM - Hardware Security Module
- IETF - Internet Engineering Task Force
- IKE - Internet Key Exchange
- IM - Information Management
- IPsec - Internet Protocol Security
- IoT - Internet of Things
- ISO - International Organization for Standardization
- IT - Information Technology
- Kerberos - Computer network authentication protocol to allow server communication over a non-secure network
- LDAPS - Lightweight Directory Access Protocol
- MFA - Multi-Factor Authentication
- mTLS - Mutual Transport Layer Security authentication
- NCCoE - (U.S.) National Cybersecurity Center of Excellence
- NIST - (U.S.) National Institute of Standards and Technology
- OAuth - Open standard for access delegation
- OT - Operational Technology
- PGP - Pretty Good Privacy
- PII - Personally Identifiable Information
- PKI - Public-Key Infrastructure
- PQC - Post-Quantum Cryptography
- QRWG - Quantum-Readiness Working Group
- QSC - Quantum-Safe Cryptography
- S/MIME - Secure/Multipurpose Internet Mail Extensions
- SAML - Security Assertion Markup Language

- sFTP - SSH File Transfer Protocol
- SHA1 - Secure Hashing Algorithm version 1
- SSH - Secure Shell
- TLS - Transport Layer Security
- TLP - Traffic Light Protocol

ANNEX B: RECOMMENDED CRYPTOGRAPHY USE CASES TO BE DISCOVERED & DOCUMENTED

This Annex contains a list of technology protocols and broader IM / IT cryptography use-cases applicable to most public and private organizations and businesses across Canada.

Common Protocols:

1) TLS
2) mTLS
3) sFTP
4) FTPS
5) SSH
6) SAML
7) OAuth
8) IPsec
9) IKE
10) Kerberos
11) LDAPS
12) PGP
13) WiFi/WPA
14) S/MIME
15) DECT
16) Mobile NEC
17) DNSsec

Broader Cryptography Use-case Considerations:

A. Code Signing
B. Multi-Factor Authentication (MFA)
C. Encryption of Data at Rest – may be vendor-specific
D. Cloud Native Encryption
E. Hardware Security Modules (HSMs)
F. Certificate Authorities (CAs)
G. Application Layer Payload Encryption

ANNEX C: CONTENT NEEDED TO DESCRIBE AN ORGANIZATION'S USES OF CRYPTO

This Annex provides a list of the information to be sought and then collated when an organization is ready to inventory the cryptography it relies on for any of the use cases listed in Annex B. This information is appropriate to develop during Phase 1 - Discovery.

The content to be inventoried per items 1 to 10 (below) will describe "how things currently are" in one or more of an organization's existing IM, IT and/or OT systems.

1. Use Case Description
2. Business Value
3. Potential Business Data in Scope / Volume of that Data / Lifespan of that Data
4. Use Case Class (e.g., Data in Transit, Data at Rest, Data in Processing, Digital Signature)
5. Technical and Threat Considerations
6. Types of Cryptography Currently in Use
7. Technical Components (e.g., end-points, networks, databases, file servers)
8. Locations where Cryptographic Information Exists (e.g., DLL, hardware)
9. Technical Dependencies (e.g., details on components within this Use Case that depend or rely on other systems for their own security)
10. Ability to Support (Pre and Post-Quantum) Cryptographic Algorithms Simultaneously

After the above information is collected, analyzing it will enable planning "What to do to reduce the quantum risk?" in later project phases (e.g., Quantum Risk Assessment, Quantum Risk Mitigation, Migration to Quantum-safe PQC), including:

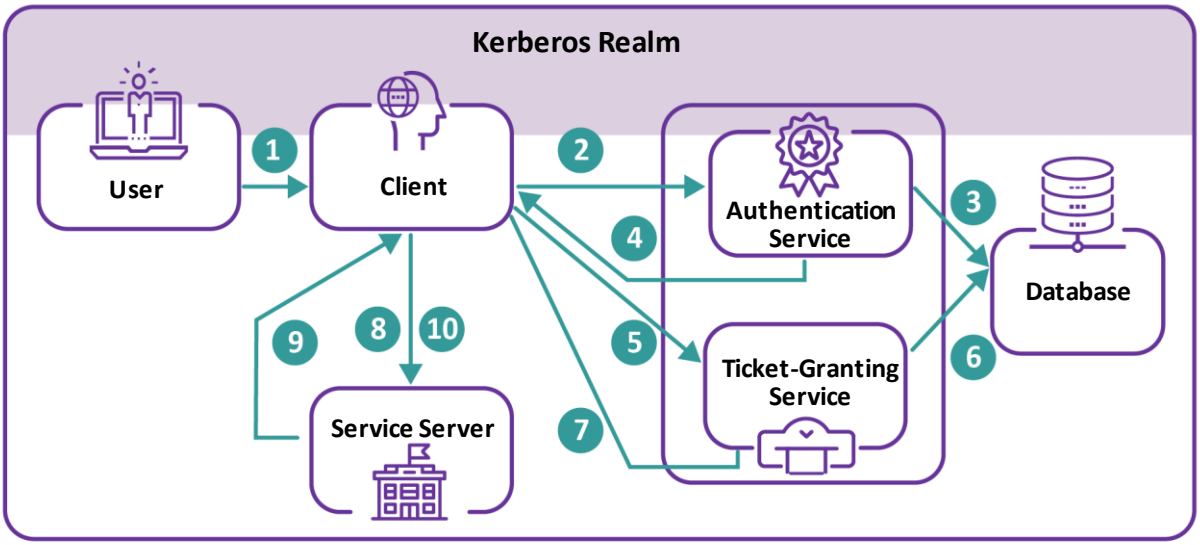
11. Best Choice of Algorithm to Use
12. Order or Sequence of what needs to be Upgraded
13. Path To Inline Quantum Remediation
14. Alternate Paths to Quantum Remediation (e.g., upgrade of entire system, change in paradigm)

ANNEX D: SAMPLE USE CASE #1 – USING KERBEROS FOR AUTHENTICATION

Section 1: Use Case Description

Kerberos is an authentication protocol on computer networks that allows clients to access services from providers. It does so by leveraging a Ticket-Granting Service (TGS) from a Key Distribution Centre (KDC) which will provide tickets to the service requestor to give to the service provider for access. It is often used as a main ingredient in Single-Sign-On (SSO) functionality.

A generic diagram of the network architecture in which Kerberos is used is given here.



1) User enters credentials (username + password).
2) Send KRB_AS_REQ.
3) Lookup user (and password) in database.
4) Send KRB_AS_RSP.
5) Send KRB_TGS_REQ.
6) Lookup service (and password) in database.
7) Send KRB_TGS_RSP.
8) Send KRB_AP_REQ.
9) Send KRB_SP_RSP.
10) Send service request to Service Server.

It should be mentioned that the initial contact and authorization of the client may occur over an insecure channel and, therefore, require some protection such as TLS. This channel is outside the scope of this use case.

Section 2: Business Value

Kerberos is mainly used to grant users and machines access to different services. It is often a critical ingredient in SSO implementations. Kerberos is also one of the basis elements of Microsoft Active Directory (AD).

Section 3: Potential Business Data in Scope/Volume/Lifespan

The data used by Kerberos is often limited to user and/or machine access data or data regarding the service being accessed. This would include userIDs and passwords, IP addresses, and potentially other limited-use and transitional information. Most of the information is of limited use and there is a limited time it would be available.

The data that is available to be accessed due to compromise of Kerberos would be unlimited as it theoretically can be used to access any service. However, this would be within the scope of the service being accessed and not directly tied to the Kerberos implementation.

Section 4: Use Case Class

Identity Management and Access Control

Section 5a: Technical Considerations

The following are considerations for Kerberos with regard to implementing quantum-safe technology:

1) **Availability:** A system implementing Kerberos will often be accessed by many different users and services at the same time. There is always a Denial-of-Service (DOS) risk in any change.
2) **Compatibility:** Kerberos can be used by m any different services, each with its own coding. Any change would have to be one in a way which is compatible with the services that use it.
3) **Credential Management:** Kerberos does manage credential from users and services in order to properly authenticate them. Changes should not put these at risk.

Kerberos is often embedded into other products. Most organizations would be dependent on having their vendors make Kerberos be quantum-safe. However, individual organizations would need to track and test in order to ensure that any changes would not be disruptive.

Section 5b: Threat Considerations

Kerberos implementations often serve as the central access point for user interaction to services within an organization. Compromise of the Kerberos system can range from a limited one-time service access to complete, catastrophic access control failure.

It would be a target both for malicious insiders as well as external attackers.

There exist current classical attacks on Kerberos (e.g., pass-the-hash).

Section 6: Types of Cryptography

Kerberos is traditionally based on symmetric key cryptography and so is not especially vulnerable to quantum. However, there do exist extensions where asymmetric cryptography is used for initial authentication (see RFC 4556).

There are two instances where asymmetric cryptography can be used in Kerberos:

1) **User Authentication:** Classical Kerberos will verify users through traditional access control methods such as a userID and password. However, the public key extension for Kerberos allows a user to send a client certificate which can be verified by a trusted CA.
2) **Session Key Agreement:** Classical Kerberos will use user information (e.g. password) to compute a session key between the client and Key Distribution Centre for encryption purposes. The public key extension allows asymmetric key agreement such as Diffie-Hellman.

Section 7: Technical Components

The main technical components of Kerberos are:

1) **Client (Service Requestor):** the user or machine that is requesting the service.
2) **Service Provider:** the service that is being accessed.
3) **Client Authenticator:** The entity responsible for authenticating the client. This is often embedded within the KDC.
4) **Ticket-Granting Service (TGS):** The service which will grant a ticket to the client which will allow it to access the service. This is often a part of the KDC.
5) **Certificate Authority (CA):** This optional for the extensions which rely upon a CA to verify client certificates.

Domain controllers are an example of a KDC as they often implement the Kerberos protocol.

The network over which communication will take place can also be considered to be a component. However, as Kerberos is not a network protocol, this is considered out of the scope of this use case.

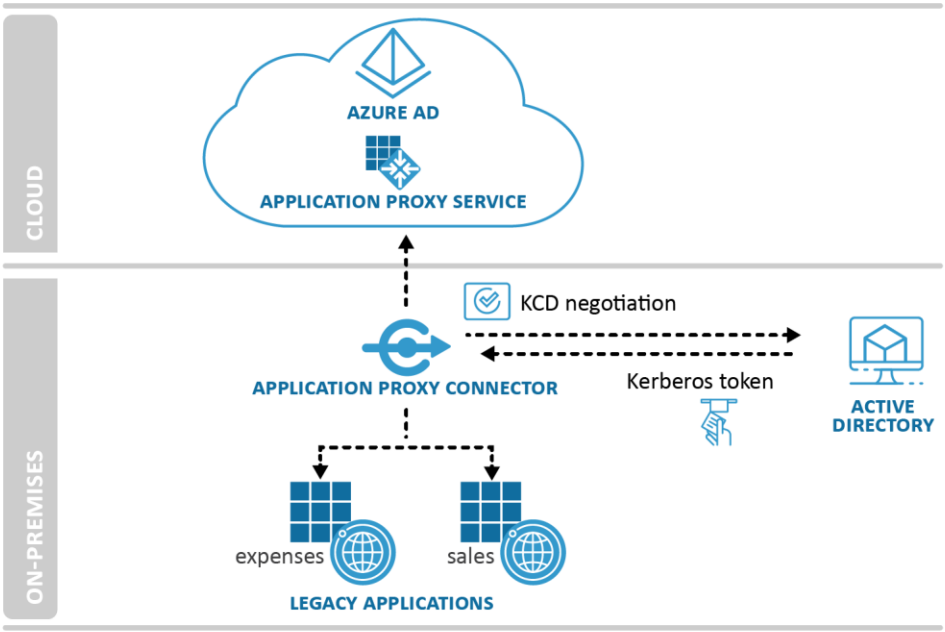
The Client Authenticator and TGS form the heart of the Kerberos system, often within the KDC. The client and Service Provider are separate systems which must be compatible with Kerberos KDC in order to function properly.

Section 8: Crypto Locations

A Kerberos implementation (i.e., the KDC) is usually a centralized system with its own cryptographic code and/or libraries. Its exact location would be product-specific. It must also be able to access a proper CA to verify a client certificate when used for initial authentication extension.

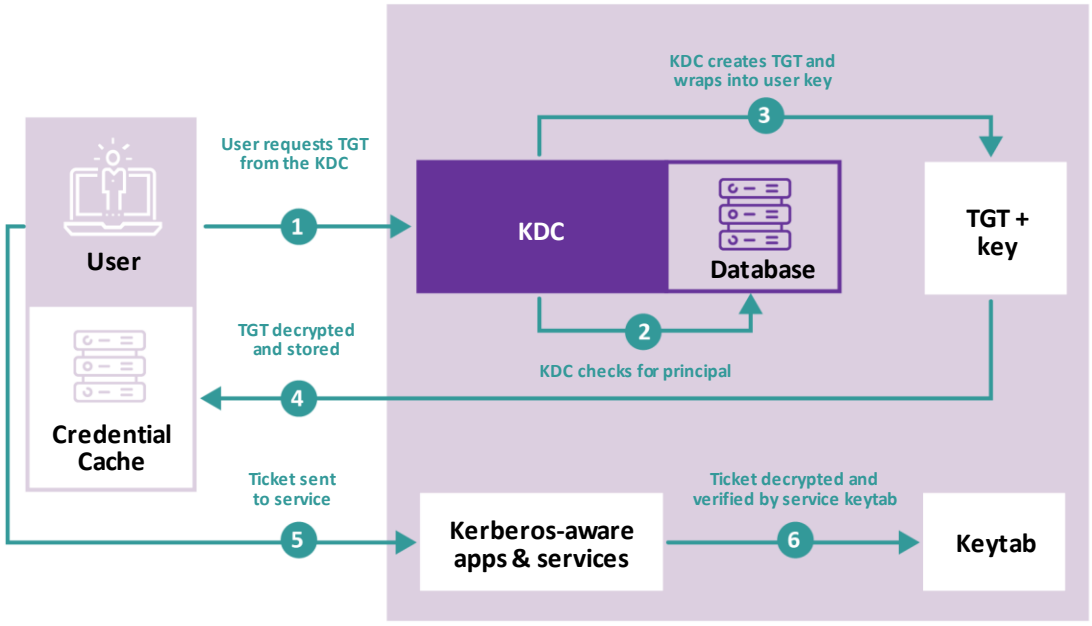
Note that asymmetric keys used within the KDC are ephemeral and so do not need to be stored for any length of time. Client certificates are used only for initial authentication and can then be discarded whereas the asymmetric keys used for key agreement can be discarded once the symmetric key is established.

The client and service provider would have their own method and location of cryptography. This, again, would be very implementation-dependent. The client would need to store the private key for its certificate. However, the asymmetric keys needed for key agreement would be ephemeral and would not need to be stored.



The most popular implementation of Kerberos is within Microsoft Active Directory (AD). An example in Azure AD is diagramed above.

Kerberos is also implemented by Red Hat. The following diagram shows its structure.



Section 9: Dependencies

The dependent use cases for Kerberos are:

- Data Storage – for client private keys (if certificates were used to establish authenticity of public keys)
- PKI/CA – (if certificates were used to establish authenticity of client public keys)
- TLS – to protect the initial client authentication.

Section 10: Ability to Support Algorithms Simultaneously

The main entity which would be required to support algorithms simultaneously would be the KDC. It would need to simultaneously authenticate quantum-safe and non-quantum-safe client public key authentication requests.

If the KDC can support both simultaneously, then it would make sense that it would be upgraded first. The client and service provider would need to support whichever version of the protocol the KDC has implemented. Hence, these can gradually be upgraded at their own pace after the KDC. These upgrades would be independent of each other.

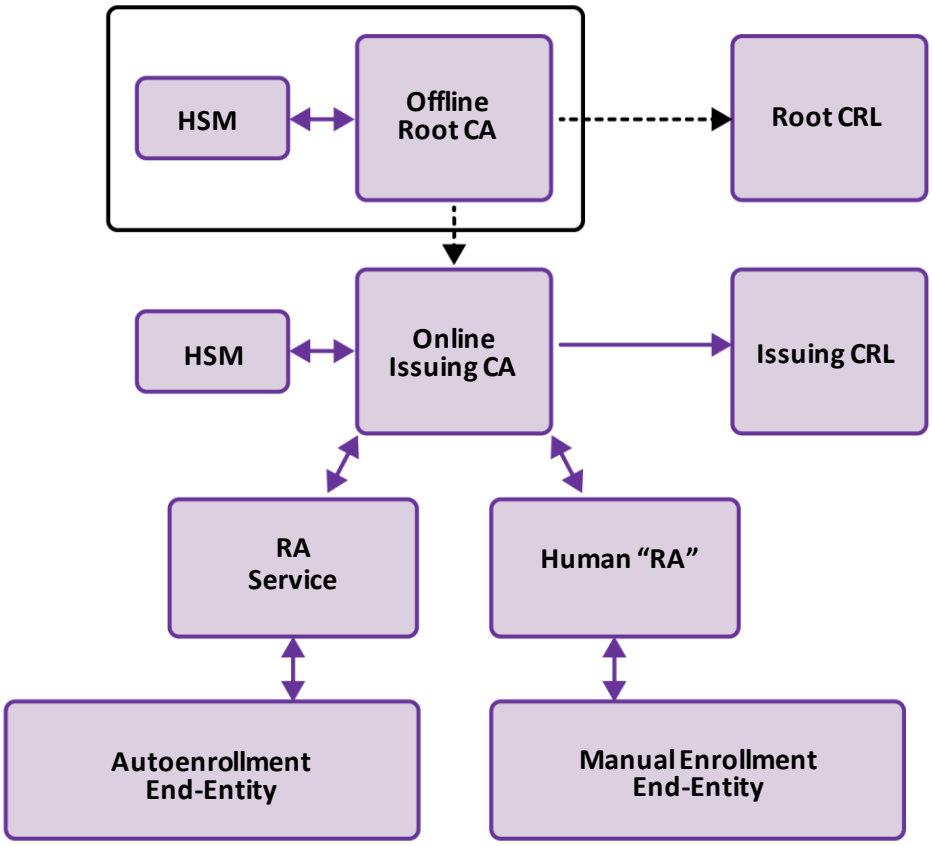
ANNEX E: SAMPLE USE CASE #2 – PKI/CA'S

Section 1: Use Case Description

The purpose of a Public-Key Infrastructure (PKI) is to provide the technology and processes to leverage certificates for various other use cases such as TLS, sFTP, IPSec, and many others.

This is accomplished through the use of a Certificate Authority (CA) which has the ability to issue certificates which relying parties can use to authenticate individual entities. The certificates leverage public-key cryptography for authentication which makes it inherently susceptible to quantum computing.

A Certificate Authority will typically have a hierarchy such as shown in the diagram below:



CAs may have more or fewer levels, but they have the same basic structure.

In terms of scope, this use case will cover only the CA structure itself. It will not cover the use of certificates in such protocols as TLS and sFTP as those will be covered in their own separate use cases.

The CA/PKI use case will be separated into several sub-use-cases:

1. Public CAs – CAs which issue publicly or universally trusted certificates (e.g. Entrust, DigiCert)
2. On-Premises Internal CAs – CAs established within and managed by an internal organization (e.g., Microsoft PKI, KeyFactor)
3. Managed Internal CAs – CAs which are trusted only by an internal organization but managed by an external entity
4. Special Purpose CAs – CAs which are typically application specific within a well-defined domain (e.g. IoT CAs for mobile devices)
5. Inspection CAs – CAs which are used to intercept traffic in a Man-In-The-Middle scenario and inspect content (e.g. web content filtering and TLS inspection)

While similar each have their own characteristics which will be called out where different.

Section 2: Business Value

PKIs are typically classified as technology infrastructure. Its business value lies in its position as a key element in the operational security of critical operations. Thus, it would essentially inherit the business value of whatever application would depend upon it. As most applications which make use of a network require some level of security, PKIs are ubiquitous within most high- and low-value applications.

Section 3: Potential Business Data in Scope/Volume/Lifespan

While PKIs are involved in the protection of business data, they do not typically directly protect business data. This is often left to end-entity certificates within use cases such as TLS, sFTP, etc. This would be out of scope for this use case.

Furthermore, CA certificates are typically used for signing, not encryption or key agreement. Hence, there is no harvest-and-decrypt risk for CA certificates.

The only data present within a PKI would be infrastructure data such as Fully Qualified Domain Names (FQDNs) or routing information. With the advent of Certificate Transparency (CT), much of this information is now publicly available. Hence, it is most important to protect this information from an integrity and authenticity perspective.

Section 4: Use Case Class

Entity Authentication for Critical Infrastructure

Section 5a: Technical Considerations

The following are considerations for PKI with regard to implementing quantum-safe technology:

1) **Certificate Size:** Applications may have limitations on size such as through-the-device or channel constraints or hard-coding of buffer sizes.
2) **Signing Performance:** Some applications require a high throughput CA for large volume or high-speed signing capabilities. The Inspection CAs are a good example as they must create new certificates on-the-fly with little to no noticeable impact to user browsing.
3) **Verification Performance:** Some applications such as IoT or high-volume servers may have restrictions on verification performance as devices may be constrained or deal with large amounts of verifications.

Note that technical considerations of CA chain verification for applications is not in scope as it would be covered in the use cases using the certificates.

Section 5b: Threat Considerations

The CA is often the central root of trust for a large number of systems. Compromise of a CA private key could lead to a large amount of fraudulent certificates and connections and, hence, unauthorized transactions. The potential fraud is directly attributable to the capabilities of the applications leveraging these certificates.

The following would be further considerations for each separate use case:

1) Public CAs are universally accepted, so compromise could be catastrophic and worldwide.
2) On-premises CAs would have affects typically only for the organization. As it is hosted internally, it would likely require access to the organization's internal network to determine the CA certificates and to conduct malicious activity.
3) Managed CAs would be similar to on-premises CAs in that access to the organization is required to conduct fraud. There is an additional threat vector in that compromise of an managed CA provider could compromise many different organizations.
4) Special purpose CAs would be specific to the application they are dedicated to. One of the threat considerations would be discovering these CAs. Quite often, these CAs are embedded within products and agnostic to users and administrators.
5) Inspection CAs would be similar to on-premises CAs except that compromise would likely be limited to browser-based applications accessed by internal users.

Section 6: Types of Cryptography

The cryptography is asymmetric mainly used in:

1) Signing of CA intermediate certificates.
2) Signing of end-entity certificates

3) Signing of Certificate Revocation Lists (CRLs)
4) Authentication of Registration Authority credentials

Note that root certificates are self-signed. However, the signing is often of little value as applications will accept a root if it simply exists within its root store.

The certificates also make use of a hash function within signing and for thumbprint purposes.

The PKI will also make use of random number generation in order to generate public/private key pairs and produce signatures.

Section 7: Technical Components

The technical components in implementing the CA depends on the type of CA being implemented. Several types of CAs are listed here:

A) Root CA
Root CAs are typically held offline and is only used for signing intermediate CAs and the corresponding root CRLs. The components typically consist of:

- Offline Hardware Security Module (HSM) and related peripherals
- Offline machine to facilitate signing (e.g. laptop, desktop, some sort of device)
- Software to facilitate CA functions
- Offline secure storage device to store private key information

B) Intermediate CAs (Networked)
The intermediate CAs are typically used for issuing certificates

- Online networked HSM and related peripherals
- Online server, virtual machine, or equivalent
- Software to facilitate issuing CA functions such as:
  - Certificate Signing Request (CSR) validation and signing
  - OCSP or equivalent compatibility
  - CRL generation and signing
  - RA credential verification
  - Public/private key pair generation (for some use cases where the CA generates and end entity's certificate)
- Online accessible file lookup for CRL
- Access control functionality
- Backup systems to store log and data

C) RAs (either manual or automated)
RAs would need the technical capability to accept certificate requests and perform verification of the request and validation of the entity. This would typically consist of:

- A machine (e.g. laptop, server) to run the RA software
- A portal or Access Control List (ACL) to provide information to validate
- RA credentials (usually an RA certificate)

D) Inspection CAs
Inspection CAs would usually be embedded within an appliance of some sort and have their own protection capabilities for the private key such as an onboard crypt card.

E) Special Purpose CAs
The components of a special purpose CA would be dependent upon the type of application it is used for. For example, such a CA to handle registration of surveillance cameras would have very different components than one for conferencing software. However, there would be at minimum:

- A machine to handle registration, signing, and issuance of the special purpose certificates.

F) End Entities
While end entities are generally out of the scope of this use case, we will include specifically the end entity function of generating a CSR and installing a certificate. In order to do so, the end entity components would be:

- The end entity itself
- The software used to generate the CSR and install the certificate.
- The storage location of the private key as well as any related protection mechanisms.

Section 8: Crypto Locations

1) Root and Intermediate CAs
The primary location of the cryptography in play would be within the HSMs. This would be heavily dependent upon the type of HSM and manufacturer. There may be some residual crypto functionality from the software which is meant to facilitate CA functionality or to perform OCSP signing and RA credential verification.

2) RAs
For RAs, this would likely be the software which facilitates RA login.

3) Inspection CAs
Inspection CAs would mostly rely on the crypto card that they use for certificate generation as well as the corresponding software. This is usually packaged together within an appliance.

4) Special Purpose CAs
This would be completely dependent upon the implementation and would be vendor-specific.

5) End Entities
This would be embedded within the CSR generation software on the entity such as OpenSSL.

For the majority of the use cases, there is typically no CA cryptography outside of the HSM. Crypto for the HSMs is handled in the HSM use case.

When a software-only implementation is used, the private keys are typically stored locally on the machine which is performing the signing. The code is embedded in the software product that is being used.

In terms of generating private keys and CSRs, one standard implementation is OpenSSL's req command-line utility. The requisite code is within the OpenSSL binaries and the keys and CSRs are output to a file specified in the command line.

Section 9: Dependencies

The following use cases are dependencies for this one:

- Data Storage
- HSMs

In addition, certain considerations from other use cases may need to be taken into account from other use cases for which this use case is a dependency in order to ensure compatibility.

Section 10: Ability to Support Algorithms Simultaneously

Proposals exist for combining quantum-safe technology with existing methods to support both as a hybrid as listed here:

- draft-ietf-lamps-cmp-algorithms-06 - Certificate Management Protocol (CMP) Algorithms
- draft-ounsworth-pq-composite-sigs-04 - Composite Keys and Signatures For Use In Internet PKI (ietf.org)

Thus the remaining work would be in getting the CA and end-entity components to implement them. The HSMs and all CA software must be able to support this. Applications would need to support as well.

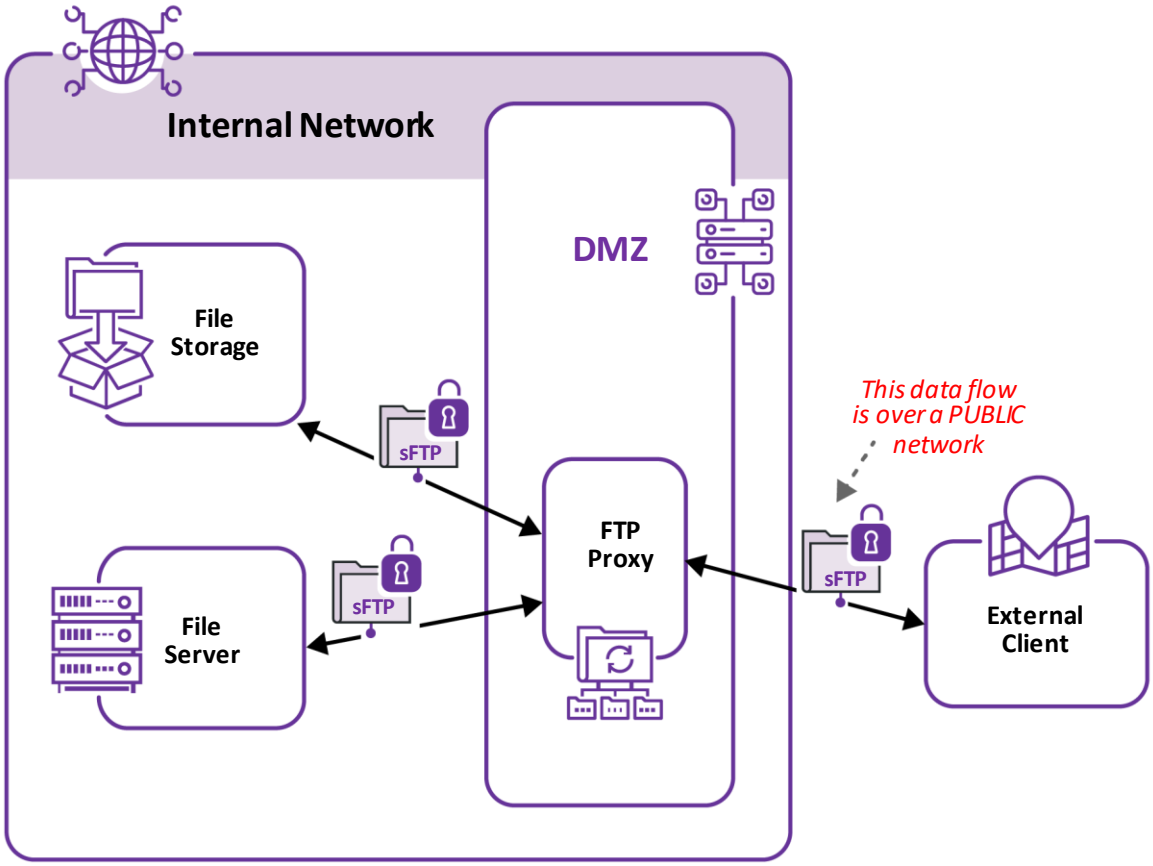
ANNEX F: SAMPLE USE CASE #3 – SFTP

Section 1: Use Case Description

sFTP, the Secure File Transfer Protocol (not to be confused with the Simple File Transfer Protocol) is a network protocol that leverages SSH authentication to securely transmit and manage files between two endpoints.

The SSH protocol is actually its own use case and so will not be considered in generality. However, for scoping purposes, as sFTP is widely used and has high business value, this use case will consider the use of SSH as bound to sFTP protocol and so will be considered one and the same. A separate SSH use case will be created for non-sFTP uses.

A generic diagram of the network architecture in which sFTP is used is given here.



Section 2: Business Value

Many organizations use sFTP servers to exchange files and other critical business documents with their trading partners. It is typically not used for low-latency transactional systems and is more apt for batch or bulk file transfers. Since these types of file transfers are ubiquitous in the

technical implementation of business systems, sFTP could have a place within any business system.

Section 3: Potential Business Data in Scope/Volume/Lifespan

sFTP can be used to transfer any type of data as long as it is in file format. Hence, there is essentially no limit to the value of the data which is transferred. The data itself will be largely dependent on the intended business use of the application leveraging sFTP.

Section 4: Use Case Class

Data-In-Transit Protection – (files)

Section 5a: Technical Considerations

The following are considerations for PKI with regard to implementing quantum-safe technology:

1) **File Size:** sFTP can be used to transfer files of arbitrary size. The only limit could very well be the technical limit of the underlying hardware and software using sFTP.
2) **Throughput:** sFTP is not typically used for low-latency transactional applications, so real-time throughput is NOT typically a consideration. However, some business applications depend on sFTP to transmit large amounts of data within a restricted time window. Throughput becomes a consideration in this sense.
3) **Credential Management:** The underlying protocol enabling sFTP authentication (usually through SSH) requires credentials such as private keys to be properly and securely stored on the endpoints facilitating the sFTP connection.
4) **Support of Underlying Technology:** The endpoints facilitating the sFTP connection need to have the proper capabilities (e.g. OS, network connections, cryptographic software) to implement the sFTP connection.

Section 5b: Threat Considerations

sFTP servers have become a primary target for hackers, putting sFTP servers at risk of a costly data breach. (https://www.goanywhere.com/blog/2018/01/23/10-essential-tips-for-securing-ftp-and-sftp-servers).

The exact threats to sFTP depend upon the security environment in which it is used. For example, sFTP connections which are external over a public network are inherently more vulnerable to attack than those that are internal to an organization. Additional controls such as logging and monitoring can affect the overall threat level.

As sFTP uses asymmetric cryptography for authentication and key agreement, there is a both an inherent quantum threat to compromise the connection as well as a "Harvest-and-Decrypt" risk for the business data that is being transmitted.

Section 6: Types of Cryptography

sFTP mainly uses both symmetric and symmetric cryptography for protection of the file data which is being transmitted.

The asymmetric cryptography is used by the underlying SSH protocol to establish authentication and key agreement between the two endpoints. The files are then protected with symmetric cryptography during transmission.

Section 7: Technical Components

The main technical components are:

1) The Endpoints: the two endpoints engaged in the active session and their underlying technology.
2) The Network: the network over which the transmission occurs.

Note that the network may have several hops in between the connection endpoints. However, for the purpose of this use case, they are transparent passthroughs and so need not be given consideration.

The endpoints must:

3) Have the requisite capabilities to support the sFTP software including the requisite cryptographic functions.
4) Have the requisite capabilities to support the underlying authentication software (SSH).
5) Have the ability to store or otherwise send or receive the files being transmitted.
6) Have the ability to store and manage the credentials of the underlying authentication software (e.g. private keys).
7) Have access to the appropriate network over which the communication is to occur.

The network must be able to support the authentication protocol as well as the transfer of files.

Section 8: Crypto Locations

The sFTP protocol will either leverage its own cryptography as part of its own software when it was installed or will leverage the underlying cryptographic libraries of the machine on which it is used.

Any change to the cryptography used in the sFTP protocol amounts to a change in the cryptographic code in one of these locations. It is important to note that any such changes have some additional considerations:

1) The location of any cryptographic keys should be taken into consideration.

2) The surrounding protocols must be ensured to be compatible with any change in buffer size, throughput or protocol steps.

Please note that some sFTP implementations may either be bundled together with SSH or be modularly separated. In these situations, the cryptography and cryptographic locations of the two protocols may need to considered in tandem instead of separately. When considering changes to the cryptography of an implementation, whether or not the sFTP and SSH implementations are bound together or not should be taken into consideration.

Many popular sFTP products operate similarly in terms of cryptographic locations. The cryptographic code is embedded within the source code and binaries of the product. The private keys or certificates are typically stored locally and exist in .pem or .ppk files.

Section 9: Dependencies

The dependent use cases for sFTP are:

- Data Storage
- PKI/CA – (if certificates were used to establish authenticity of public keys)

Additionally, one would normally consider SSH as a dependent use case, but we have bound it together with sFTP for the purpose of this use case.

Section 10: Ability to Support Algorithms Simultaneously

By its nature, an sFTP endpoint would establish an individual sFTP connection with any number of other endpoints. Each connection would use fixed, established cryptographic algorithms for the lifespan of that connection. However, the connections between different endpoints would be theoretically independent of each other. Hence, any sFTP endpoint could theoretically implement different cryptographic algorithms for different connections. Thus, any migration to new algorithms can be done connection by connection when the other endpoint is ready.

The ability to support different algorithms simultaneously, therefore, depends on whether the particular sFTP product has been programmed to support this functionality. It would be beneficial to encourage sFTP providers to enable this functionality.

APPENDIX A: QUANTUM-READINESS MYTHS AND FAQ'S

	Myth	Reality
1	The Quantum Threat applies only to a small set of organizations within Canada.	The Quantum Threat is of national significance and impact. The risks to information security as well as health and safety, across domains including Critical Infrastructure, 5G, Cloud, AI/ML, and IoT, will require actions at a national scale, and efforts and actions from both government and organizations.
2	Quantum Threat: For my organization, that's an Information Technology (IT) problem ?	For the Organization, the threats and risks posed by Quantum Computing are, first and foremost, a BUSINESS problem.
3	The Information and Communications Technology (ICT) sector and related industry organizations will solve this. My organization / sector don't have to do anything… or not much ?	It is true that the vast array of quantum stakeholders, including standards organizations, ICT sector organizations, academia, and others are working diligently to try to address the threats posed by the future of quantum computing. However, at the end of the day, individual organizations and sectors are ultimately accountable for ensuring the confidentiality, integrity, and availability of all key data of value that is stored, processed, and transmitted.
4	This is not a pressing issue at this time. Getting prepared for Quantum … that can wait ?	The process of Quantum Risk Assessment and Quantum Migration may take many years, if not even longer. The timelines for organizations and sectors will depend on many factors, including but not limited to: numbers, types, complexities, and interdependencies (intra-org and inter-org) of products, systems, interfaces, and solutions employing various cryptographic systems; trusted supply chain of cryptographic systems (hardware & software); Skilled resources' availability; etc.

	Myth	Reality
5	NIST is still in the process of standardizing Post-Quantum Cryptography. Should one wait until that is done, before starting QSC prep ?	From a planning perspective, while standardized quantum-safe crypto is not yet available, there are NO direct dependencies on the outcomes of the NIST Post-Quantum Cryptography Standardization process that would prevent or delay an organization / sector from starting to assess and plan for the impacts of quantum technologies on cryptography. From an QSC migration perspective, the future implementations must be based on standards based and certified cryptographic algorithms and products and solutions.
6	The risk is low within the organization / sector, because cryptography usage is very low / low ?	Cryptography is pervasive and embedded across all aspects of Information and Communications Technology, to help ensure the confidentiality, Integrity of information that is stored, processed, and transmitted.
7	The confidentiality of current sensitive information is safe for now. Getting Quantum-Prepared can wait ?	One of the key threat scenarios is the capture of data today (including encrypted data as well as cryptographic information such as cryptographic key exchanges), and then decrypting the captured data in the future using quantum technologies.
8	Preparing for Quantum Readiness for my org / sector seems simple and straight forward. Getting Quantum-Prepared can wait ?	That depends. Quantum Readiness depends on may factors, including but not limited to : the amounts and types of data of values ; the requirements for keeping the data confidential and integral ; the number and types and systems that store, process and transmit the data ; the number and complexities of interfaces to other systems ; inter-organization dependencies ; A Quantum Readiness assessment may be required to understand the level of simplicity or complexity to prepare for Post-Quantum Cryptography.

	Myth	Reality
9	Preparing for Quantum-Readiness is as simple as some software upgrades to incorporate new crypto protocols. Right ?	This is DEFINITELY NOT like a "simple monthly software update". A detailed technical review of current products, systems, infrastructure, and architectures that leverage cryptographic modules will help determine if any hardware upgrades, software upgrades, application upgrades, or even complete system replacements, may be required.
10	Preparing for Quantum-Readiness seems overwhelming ?	While the detailed technical aspects of Quantum threats and cryptographic aspects are beyond the skills of most, the vast majority of Quantum-Readiness steps are typically incremental steps on existing business as well as technical strategic and operational processes and procedures. Open source information, such as the Quantum-Readiness Best Practices guide, plus exemplars, are intended to help organizations and sectors start immediately.
11	For symmetric cryptography, all that needs to be done is to ensure that the key length is sufficiently large to provide QSC assurance ; it's that simple, right ?	Strictly speaking, from the "narrow" perspective of symmetric cryptography, yes, if the ley length is sufficiently large, then the symmetric cryptography may be deemed safe. However, depending on the use case, in support of the symmetric cryptography, there may be also be a need for key exchange and key management of the symmetric keys, and those techniques typically require using asymmetric cryptography. So if this is the case, then the system will be vulnerable to Quantum based cryptographic attacks.
12	We implement some non-standards based cryptography. That's OK, right ?	Using any proprietary or non-standard cryptography, or any algorithm that has not received substantial review is a big security risk.

APPENDIX B: QUANTUM-SAFE POLICIES, REGULATIONS AND STANDARDS

B.1 QUANTUM-SAFE POLICIES

The Canadian Centre for Cyber Security has published one directive (viz., ITSB-127) relevant to quantum:

- **Mandatory GC Quantum Computing Threat Mitigation** (ITSB-127)

  This ITSB applies to Government of Canada (GC) communications networks, national security systems, and GC end-users who process, handle or retain GC classified information and data, or other sensitive information.

  Canadian Centre for Cyber Security – May 2019

B.2 QUANTUM-SAFE REGULATIONS

Canada has not enacted any regulations related to quantum-readiness or quantum-safe cyber security to date.

B.3 QUANTUM-SAFE STANDARDS

The U.S. National Institute of Standards and Technology began work on new standards for PQC in 2015. Their goals include releasing draft standards for public comments in 2022-2023, and recommending PQC standards in 2024. NIST is also planning:

- ***discovery of all instances where NIST Federal Information Processing Standards (FIPS), 800-series Special Publications (SPs), and other guidance will need to be updated or replaced;***
- ***discovery of which standards from ISO/IEC, IEEE, industry groups like the Trusted Computing Group, and other standards developing organizations will need to be updated or replaced; and***
- ***discovery of which Internet Engineering Task Force (IETF) Request for Comments (RFCs) and other networking protocol standards will need to be updated or replaced.***

Migration to Post-Quantum Cryptography - Project Description
NIST, June 4, 2021, 16 pages

APPENDIX C: U.S. NCCOE PROJECT ON MIGRATION TO PQC

On June 4, 2021, the U.S. National Cybersecurity Center of Excellence (NCCoE) within NIST invited public comments on a draft project description for *Migration to Post-Quantum Cryptography*. [11]

If approved as written, the outputs of the NCCoE project could input to the development of best practice recommendations for Section 3.4 - Migration to PQC (Phase 4).

> ***The NIST National Cybersecurity Center of Excellence (NCCoE) is initiating the development of practices to ease the migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks.***
>
> ***The project will provide systematic approaches for migrating from vulnerable algorithms to quantum-resistant algorithms across the different types of assets and supporting underlying technology.***

The NCCoE's proposed scope for this project includes investigating five demonstration scenarios that would be applicable to a broad range of organizations globally (including organizations in Canada). The scenarios are:

> ***Scenario 1: FIPS-140 validated hardware and software modules that employ quantum-vulnerable public-key cryptography;***
>
> ***Scenario 2: Cryptographic libraries that include quantum-vulnerable public-key cryptography;***
>
> ***Scenario 3: Cryptographic applications and cryptographic support applications that include or are focused on quantum-vulnerable public-key cryptography;***
>
> ***Scenario 4: Embedded quantum-vulnerable cryptographic code in computing platforms; and***
>
> ***Scenario 5: Communication protocols widely deployed in different industry sectors that leverage quantum-vulnerable cryptographic algorithms.***

[11] Migration to Post-Quantum Cryptography - Project Description NIST, June 4, 2021, 16 Pages

The contents of this document were developed
during the course of CFDIR QRWG meetings between July 2020 and June 2021.

This document will be updated annually,
to reflect industry feedback from implementing
the best practices described herein.

Version 01 - July 7, 2021

Prepared by the Quantum-Readiness Working Group
of the Canadian Forum for Digital Infrastructure Resilience