Practical Preparations for the Post-Quantum World

Tasks Every Organization Should be Performing Now to Prepare

cloud security alliance®

The permanent and official location for Quantum-Safe Security Working Group is
https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

Acknowledgments

Lead Authors:

Roger Grimes

Contributors:

Edward Chiu
Jim Gable
Bruno Huttner
Ludovic Perret

Reviewers:

Hillary Baron
John Hooks
Erez Kalman
Ashish Mehta
Surenda Sharma

CSA Staff:

Hillary Baron

Special Thanks:

Bowen Close

Executive Summary

Quantum information sciences and technologies continue to make steady improvement and, in the near-term future, they are likely to result in key challenges and threats. Sufficiently capable quantum computers may compromise or weaken most forms of traditional asymmetric and symmetric cryptography. Consequently, there are tasks every organization should be performing today, and in the years ahead, to prepare for the coming quantum threats and changes.

This two-part paper has been prepared by the Quantum-Safe Security (QSS) working group of the Cloud Security Alliance to discuss cybersecurity challenges and recommended steps to reduce likely new risks due to quantum information sciences. This paper was created for awareness and education and to communicate examples of steps every organization should be performing to prepare for the post-quantum world. Following these recommendations should result in increased project efficiencies, decreased cybersecurity risk, and increased long-term crypto-agility.

Part I is a discussion of the various quantum threats requiring mitigation. Part II is an actionable, step-by-step blueprint for preparing for the post-quantum world.

Post-Quantum Mitigation Plan Summary

This post-quantum mitigation plan has five main stages: education, implement a project team and plan, take a data protection inventory, analyze findings, and implement mitigations. These stages are summarized graphically below.

Each stage requires the right blend of policies, technical controls, and education to provide the most efficient reduction in cybersecurity risk. Each stage is discussed in more detail in Part II, including actionable steps, recommendations, and example content.

Note: Although helpful, no special quantum information sciences expertise is needed to successfully understand this plan or to perform a successful post-quantum migration.

You can get more information about the CSA's Quantum-Safe Security working group at their website.

WE RECOMMEND THAT EVERY ORGANIZATION SHOULD BEGIN THEIR POST-QUANTUM MITIGATION PLAN AS SOON AS POSSIBLE.

Table of Contents

1. Quantum Threats Against Traditional Cryptography

This part of the paper will summarize quantum threats that require mitigation. Part I assumes the reader understands the basics of quantum mechanics, quantum computers, qubits, and quantum devices, although it is not required to prepare for the post-quantum world. There are many existing resources dedicated to quantum theory introductory material and it is not the focus of this paper.

The increasing power of quantum computers will likely bring about new threats and challenges, only some of which are known at this time. Chief among those known threats and risks are the likely weakening or complete compromise of many traditional forms of cryptography, including public key cryptography, asymmetric key exchange mechanisms, digital signatures, symmetric keys, and other cryptographic applications.

> Note: If you are relatively familiar and understand the threats proposed by sufficiently capable quantum computers you can skip to *Part II. A Prescriptive Mitigation Post-Quantum Mitigation Plan*.

1.1 Asymmetric Cryptography Breaks

Sufficiently capable quantum computers are likely to be able to "break" the most widely used forms of traditional asymmetric cryptography (including RSA, Diffie-Hellman, and ECC). Asymmetric cryptography (also known as public key cryptography) is used for two different purposes: encryption and digital signatures. Asymmetric cryptography works using two types of mathematically related keys of a key pair. The private key, only known or used by the legitimate owner(s)/holder(s), is used to decrypt data encrypted by the related public key. Only the holder of the private key can decrypt data encrypted by the related public key. A compromise of the private key by unauthorized parties compromises the entire key pair. The related public key is used to encrypt data sent to the private key holder. Anyone can have, view, or use the public key without compromising the integrity of the key pair or the encrypted data.

Asymmetric cryptography key pairs are also used to authenticate and digitally verify the integrity of signed content. Here, the key pair is used in the opposite way: the private key is used to sign or encrypt contents, while the public key is used to decrypt it. Digital signing is the act of providing digital proof that the signed content is still as it was at the moment of the signing. To sign content, a user or process on behalf of a subject uses a private key to sign the content (or a hash result of the content). If the key pair belongs to a verified identity, the resulting signed content is known as a digital signature. Any content signed by the private key can be revealed back to its plain-text equivalent only by using the related public key. If the content can be verified ("decrypted") by the related public key, it must have been signed by the related private key because the only thing the related public key can "decrypt" is something signed by the related private key. Similar processes can be used to authenticate user identities involved in cryptographic operations. Common digital signature ciphers include Digital Signature Algorithm (DSA) and Elliptic Curve DSA (ECDSA).

Since asymmetric-based digital signatures use asymmetric key pairs, the same threats and risks from sufficiently strong quantum computers apply. Asymmetric-based digital signatures are considered "broken" once sufficiently capable quantum computers are created or used. Hence, like asymmetric ciphers, quantum-susceptible asymmetric digital schemes need to be replaced with quantum-resistant ciphers when the new quantum-resistant digital signature schemes are announced. NIST will select one or more post-quantum digital signature schemes as early as 2022.

Note: "Break" is a colloquial term used to describe when a particular cryptographic algorithm no longer provides the sufficiently strong protection promised by the creators and early reviewers. A break can mean that it is far easier to reveal protected information than was originally designed for by the cipher all the way to a particular algorithm providing little to no protection. Cryptographic breaks can happen because of revealed design flaws or because of newly discovered attack method(s) that were not previously known or possible. Quantum computer "attacks" against cryptography are the latter type.

One important aspect of public key cryptography is that the public key of the key pair can be mathematically derived from the private key. However, it is currently impossible to do it using a traditional computer, or even a very large set of traditional computers, in any reasonable period of time. This is precisely what allows public key cryptography to provide its protection. But a sufficiently capable quantum computer can quickly derive a private key from its related public key for many forms of traditional public key cryptography (including all currently existing public key standards).

Asymmetric cryptography is closely associated with *Public Key Infrastructure* (PKI) hierarchical implementations, where one or more *Certificate Authority* (CA) services are used to verify and attest to the identity of key pair owners (using what are known as *digital certificates*). This allows the holder of a public key to trust who the public key claims to be from. PKIs are used to issue, renew, revoke, and manage their related digital certificates. You do not need a PKI to use asymmetric cryptography, but it helps provide trust in distributed communications involving asymmetric cryptography with more than a few participants.

In the late 1970s, the first publicly known asymmetric algorithm determined using large prime numbers in a mathematical formula produced results that humans and even the most powerful traditional computers could not factor back into the original prime numbers (at least in a reasonable period of time and effort). Simplified, the most popular traditional public key cryptography uses two large prime numbers to create the public key. The private key is one of those large involved prime numbers used to create the public key. Even if the public key is known, it is impossible for traditional computers to figure out (i.e., *factor*) the involved private key. This type of problem is called the *integer factorization problem*. Later on, other asymmetric algorithms used different but still very difficult to solve problems, known as the *discrete logarithm problem* (on a finite field or on elliptic curves). Both types of problems rely on the difficulty of solving their involved math problems. When used correctly and with sufficiently large inputs, those inputs are for all intents and purposes very hard to determine (i.e., factor) or guess, even if given all the traditional computers in the world to use at once in the effort and given millions of years of computing time.

Quantum computers, with a sufficient number of usable qubits and logic "gates," change that. In 1994, an algorithm created by mathematician Peter Shor (*Shor's algorithm*) posited that when quantum computers are able to process the large numbers used in cryptographic applications, they would be able to more quickly resolve most traditional forms of asymmetric cryptography. Shor's algorithm has been tried on early quantum computers with very simple asymmetric problems and found to support the idea that sufficiently capable quantum computers could far more easily break most forms of traditional asymmetric cryptography. Instead of it taking millions of years, like it might on a traditional, non-quantum computer, a sufficiently capable quantum computer might be able to do it in minutes to days.

It is believed that once quantum computers of particular types become capable enough, all the information protected by most traditional asymmetric cryptography will be readily accessible to attackers who possess sufficiently capable quantum computers and access to the desired protected data. The biggest outstanding question is that no one knows (at least publicly) when a quantum computer will reach this point. This has been a worry since Shor's algorithm was publicly revealed in 1994, although at the time not a single quantum computer existed. Now, we have likely have hundreds of quantum computers, each competing to get more and more usable. Most experts believe that a sufficiently capable quantum computer will be available in under 10 years (from this publication date). Some experts believe it might be only a few years away. There is even a possibility that some group or nation-state has already done so but has not publicly revealed the achievement, though this idea is not supported by the majority of quantum computing scientists. The main point is that it is unknown when sufficiently capable quantum computers will be available, but most experts feel it will occur in the reasonable near-term future.

Note: Shor's algorithm was the first algorithm publicly announced that could potentially break asymmetric keys using sufficiently capable quantum computers. Since then, efficiency improvements have been published (and more are likely to be made) that likely decrease the resources or workload effort needed for success, below what Shor's original algorithm initially indicated was required. Thus, Shor's original resource requirements are likely a ceiling on the resources needed and further modifications or different algorithms could make an asymmetric break easier.

Asymmetric algorithms likely protect over 90% of the world's encrypted and transmitted information. Asymmetric algorithms are involved in HTTPS (which protects over 90% of the World Wide Web), Public Key Infrastructure (PKI), digital signatures, Wi-Fi protection, smartcards, hardware authentication tokens, banking networks, cryptocurrencies, and most virtual private networks (VPN). An asymmetric cryptography break would have tremendous repercussions in the digital world.

Common, traditional, asymmetric cryptography algorithms include Diffie-Hellman (Merkel), Rivest, Shamir, Adleman (RSA), and Elliptic Curve Cryptography (ECC). RSA is probably the most commonly used asymmetric cipher, followed by Diffie-Hellman and ECC, and all three are considered susceptible to quantum computers. However, not all traditional asymmetric cipher algorithms are susceptible to quantum computation. For example, the McEliece cipher, released in 1978, is resistant to quantum computing but was never widely adopted. It is considered a post-quantum cipher alternative. Over the last decade, many new but broadly unused quantum-resistant asymmetric ciphers have been created and are being evaluated.

Many organizations and researchers are evaluating known and proposed quantum-resistant ciphers as potential new national or global cryptography standards that the world can use to decrease the threat from quantum computers. For example, since 2016 the U.S. National Institute of Standards and Technology (NIST) and participants have been involved in submitting and evaluating dozens of supposed quantum-resistant cryptography.[1] NIST's goal is to select one or more *post-quantum cryptography* (aka PQC or PQ) standards. Once the new standard(s) are chosen, everyone respecting NIST's choice(s), can migrate from their quantum-susceptible ciphers and digital signatures to quantum-resistant versions. The new post-quantum algorithms are expected to be selected as early as 2022. Once NIST chooses the final PQC standards, it is expected that much of the world will begin to transition from quantum-susceptible to quantum-resistant cryptography.

The significant remaining question is whether the world's remaining quantum-susceptible ciphers will be replaced by quantum-resistant ciphers (or otherwise protected) before quantum computers gain enough power to begin routinely cracking them. This is considered the biggest known threat introduced by quantum computing.

1.2 Symmetric Encryption Weakening

Quantum computers will also weaken traditional symmetric encryption. Most encryption is done using symmetric encryption, where the same key that is used to encrypt data is used to decrypt the data. Asymmetric cryptography can also be used for encryption, but because of the larger amount of computation required to create and use asymmetric keys (as compared to symmetric encryption) it is considered too slow and weak to encrypt large flows of data. The standard solution used in most cryptographic protocols is to use asymmetric cryptography to encrypt and securely distribute the shorter symmetric keys, which do the encryption.

When asymmetric cryptography is broken by quantum computers, this compromises the many encryption applications that use asymmetric cryptography to securely transmit the symmetric key(s) between senders and receivers. But even without asymmetric cryptography involvement, symmetric encryption is threatened by sufficiently capable quantum computers.

Symmetric ciphers, where the same key is used to encrypt and decrypt confidential data, are not completely "broken" by quantum computers but there is significant weakening. To date, there is no known method for breaking symmetric cryptography with a traditional computer. Using an algorithm known as *Grover's algorithm*, quantum computers can drastically reduce the time needed to break existing symmetric keys. Grover's algorithm allows a quadratic speed-up to discover symmetric keys. Because symmetric key strength is doubled by every added bit, this means that Grover's algorithm has the capability to decrease the protective strength of existing symmetric keys by half. All any defender must do is double their symmetric key sizes, if needed, to get the same protective strength as provided by the symmetric cipher before the challenge of sufficiently capable quantum computers.

---

1 National Institute of Standards and Technology (NIST). *Post-Quantum Cryptography*. Accessed August 18, 2021, at https://csrc.nist.gov/projects/post-quantum-cryptography.

The most commonly used symmetric cipher is *Advanced Encryption Standard (AES)*. It has proven reliable since its selection by NIST in 2001 as the United States' official symmetric encryption standard. AES implementations with key sizes of 256-bits are considered quantum-resistant.

Note: Special attention should be paid to the impacts of quantum attacks on the various "operation modes" available with symmetric ciphers when multiple modes of operation exist. For example, it is currently recommended to only use GCM (Galois/Counter Mode) mode when using AES.

Although traditional symmetric encryption ciphers are not completely broken by sufficiently strong quantum computers, symmetric keys are commonly transmitted between authorized source and destination parties using asymmetric cryptography. In most cases of encryption involving asymmetric keys, the asymmetric keys are used to securely transport symmetric key(s), which are used to do the actual encryption between source and destination. Once the asymmetric cryptography has been successfully used to transport the symmetric keys, the asymmetric cryptography channel is often removed or only remains for partner integrity verification purposes. Thus, many applications using symmetric encryption may still be susceptible to sufficiently strong quantum computers if they use quantum-susceptible asymmetric cryptography or digital signatures as part of their process. Other times, the public key continues to be used and may be renewed very often to frustrate crypto attackers.

1.3 Hash Functions and Hash-Based Digital Signatures Weakening

Hash functions are a special type of one-way functions where an input of any size results in a fixed length output (typically 256-bits). Hash functions are widely used in cryptography to prevent unauthorized tampering, for example. They are also used in hash-based digital signature schemes to authenticate and verify the integrity of digitally signed content.

Common traditional hashes include NT, SHA-2, and Bcrypt. In addition, hash functions form the basis of hash-based cryptography, with signature schemes such as the Lamport one-time signature, the Merkle signature schemes, and the more recent LMS, XMSS, and SPHINCS+ schemes.
Note: Cryptography that is already considered weak or broken in the world of classical computers, such as MD-4, LM, MD-5, SHA-1, etc., are not acceptable to use in cryptography nor are they quantum-resistant.

Hash-based cryptography with sufficient hash lengths (256-bits or longer), are also quantum-resistant. Cryptographic hash algorithms can be used to document and verify the authenticity of hashed content. With hashing, content is manipulated according to a fixed series of steps as dictated by the hashing algorithm. This produces an output that is unique for all different inputs and is known as a *digital signature* when paired with a verified identity of who hashed it. Subsequent hashing of the same purported content can be made and then compared to the original verified hashed value from the time of the signing to prove or disprove whether the content has changed since it was signed.

Grover's algorithm (discussed above), along with sufficiently capable quantum computers, allows quadratic speed ups of "black box" problems, such as would be needed to compromise a hash function. As mentioned above, Grover's algorithm halves the protected strength of symmetric ciphers. This likely impacts the protection of other cryptographic functions, such as hashing functions and hash-based digital signatures. In general, it is believed that only hashes with sizes 256-bits or longer should be used in a post-quantum world.

Note that several quantum-resistant hash-based signature schemes, both *stateful* (i.e., the signer has to record every time they sign a document and make sure that they do not reuse the same private key) and *stateless* (i.e., where there is only a constraint on the number of times a given private key can be used), have already been standardized by various bodies.

1.4 Storing Captured Data Now

For some defenders, the future threats posed by the post-quantum world may already apply. For targeted organizations and individuals who need to keep quantum-susceptible secrets protected longer than a few years, motivated and monied adversaries could be secretly eavesdropping on the defender's cryptographically protected secrets now, if accessible, waiting to decrypt those secrets when sufficiently strong quantum computing power becomes available to them. Thus, defenders with the most critical secrets should begin to think about how to protect those secrets now. This will be discussed in Part II.

Note: These are the known attacks against traditional quantum-susceptible cryptography today. Additional quantum discoveries may come to pass that present new challenges and increased risks.

1.5 Quantum Threat Solution Summary

Each type of quantum threat can be mitigated using one or more known defenses. Depending on the threat they include:

- Physical isolation
- Increasing symmetric key sizes
- Using Quantum Key Distribution (QKD)
- Replacing quantum-susceptible cryptography with quantum-resistant cryptography
- Using hybrid solutions
- Using quantum random number generators (QRNG)
- Using quantum-enabled defenses

The solutions to these quantum threats are covered in more detail in Part II, which covers how to perform an entire post-quantum mitigation plan from beginning to end, including the education, policies, and tools that can be used. The specific defensive mitigations for each threat listed above are covered in the subsection *Technical Mitigations*.

1.6 Post-Quantum Migration Goal

The express goal of defenders interested in post-quantum mitigations is that the appropriate mitigations be placed ahead of any cryptographic threats being realized by quantum computers and attacks. The world has faced other necessary mass cryptographic migrations in the face of cryptographic threats, such as the move from SHA-1 to SHA-2 hashes in the last decade. Organizations following a post-quantum mitigation plan sooner are more likely to be prepared ahead of the realized threat and with less anxiety. The Cloud Security Alliance's Quantum-Safe Security Working Group believes all organizations should start to implement a post-quantum mitigation plan now. Part II of this paper is an example post-quantum mitigation plan as created and supported by the working group and other invited subject matter expert reviewers.

1.7 Additional Resources

- Cloud Security Alliance Quantum-Safe Security Working Group
- NIST Post-Quantum Cryptography

2. A Prescriptive Post-Quantum Mitigation Plan

Part II summarizes and then details a prescriptive mitigation plan that any organization can use to reduce cybersecurity risks posed by sufficiently capable quantum computers. Some parts of the plan should be started immediately, while others can or should wait for other involved events. Recommended timing is covered with each step.

2.1 Post-Quantum Mitigation Plan Summary

Our post-quantum mitigation plan has five main stages: education, implement a project team and plan, take a data protection inventory, analyze data, and implement mitigations. These plan stages are summarized graphically below.

The plan's structured intent is to most efficiently prepare any organization for the post-quantum migration in which it will surely be involved. By following the steps in order, a participant organization can be expected to most efficiently utilize existing resources (money, people, time, etc.). This plan will also help an organization with its current and future crypto-agility. The process is based on past cryptographic migrations and experience (DES to 3DES, SHA-1 to SHA-2, etc.).

Each stage requires the right blend of policies, technical controls, and education to provide the most efficient reduction in cybersecurity risk. Some stages will require more education and policies and other stages require more technical controls.

WE RECOMMEND THAT EVERY ORGANIZATION SHOULD BEGIN THEIR POST-QUANTUM MITIGATION PLAN AS SOON AS POSSIBLE.

Note: There is no need to wait for formal NIST PQC standards selection to begin your post-quantum mitigation project. The majority of the steps and needed resources will be consumed in phases that can be (and should be) accomplished ahead of the standards finalization process.

Each stage will now be discussed in more detail, including actionable steps, recommendations, and exampled content.

2.2 Awareness and Education

Most people, including even IT workers, are unaware of the potential serious increase in cybersecurity risk in a post-quantum world. Most cybersecurity defenders are already overtasked with an abundance of defensive requirements not involving quantum computers and likely do not have post-quantum mitigations and tasks on their current worklist as a priority.

The primary task of most readers who are in charge of decreasing cybersecurity risk is for their organization to formally recognize the challenges posed by a post-quantum world and get senior management support for a post-quantum project as a top priority.

This can be accomplished by awareness training, education, and formal documents given to project team members and senior management for review.

Preparation for the post-quantum world has been recommended by the US government and other national bodies since 2016. In 2016, NIST, the National Security Agency (NSA), and Central Security Service (CSS) stated in their *Commercial National Security Algorithm Suite and Quantum Computing FAQ*:[2]

> "NSA believes the time is now right [to start preparing for the post-quantum world] —consistent with advances in quantum computing."

In 2018, the U.S. National Academy of Sciences, Engineering, and Medicine published a consensus study report titled *Quantum Computing: Progress and Prospects*,[3] which stated in Key Finding 10:

> "Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster."

Note: The NIST National Cybersecurity Center of Excellence (NCCoE) prepared *Migration to Post-Quantum Cryptography*[4] to assist with PQC migrations. The NCCoE's guide aligns with this document.

---

2 NIST, National Security Agency (NSA), Central Security Service (CSS). (January 2016). *Informational Assurance Directorate Commercial National Security Algorithm Suite and Quantum Computing FAQ*. Accessed at https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf.

3 The National Academies of Sciences, Engineering, and Medicine. (2018). *Quantum Computing: Progress and Prospects*. Washington, DC: The National Academies Press. Accessed at http://cs.brown.edu/courses/csci1800/sources/2018_NAE_QuantumComputing_ProgressAndProspects.pdf.

4 NIST National Cybersecurity Center of Excellent. (June 2021). *Migration to Post-Quantum Cryptography DRAFT*. Accessed at https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/pqc-migration-project-description-draft.pdf.

> It is clear that the US government entities that are the most aware of the challenges from quantum computer believe that everyone should start preparing for the post-quantum world now if they have not already done so.

Although not necessary, it can help if the people in charge of mitigating cybersecurity risk in an organization are generally aware (at a basic level) of the challenges posed by quantum computers. However, the recommended steps can be accomplished by anyone with a basic understanding of cryptography and no one needs to be a quantum subject matter expert in order for a quantum migration project to be successful. Senior management needs to understand the strategic threat to the organization and needs to adequately address the cybersecurity risk in a timely fashion. The right time to begin a post-quantum mitigation plan is now. Post-quantum project team members need to have a strong understanding of the issues as discussed above and to understand which mitigations to apply to which challenges.

There may naturally be project advocates who better understand the technology and issues involved. There should be one or more people in the organization who have the official responsibility to follow the advancements made in quantum information sciences as it impacts the organization's post-quantum project and whose role it is to update the project team and senior management, as needed. For example, if news came that a sufficiently strong quantum computer was used to successfully break a 2048-bit RSA key before the NIST post-quantum cryptography standards were selected, this would significantly impact risk and accelerate timelines for any organization not having achieved post-quantum readiness.

Note: It is believed by the vast majority of experts that NIST will select PQC standards before quantum computers are sufficiently capable of threatening traditional cryptography.

2.2.1 Senior Management Communication and Memo Example

Senior management must be sufficiently advised of the post-quantum challenges, risks, and potential mitigations. Your objective is to get senior management support for a multi-year post-quantum project team and project. To this end, you can use this document. In general, senior management usually has less time to dedicate to learning about each individual risk than other team members. Post-quantum project leaders should create and send a short 1–2-page memo to senior management outlining all the critical facts.

Note: In Appendix A, The Cloud Security Alliance provides a sample senior management memo which you can copy, use, and modify.

2.2.2 Post-Quantum Migration Training and Awareness Goals

All training and education should seek to achieve awareness of the following items with the appropriate stakeholders:

- Likely possible threats coming from sufficiently capable quantum computers and how that increases cybersecurity risk
- Specific threats to asymmetric, symmetric, and other quantum-susceptible cryptography
- Common mitigations

Stakeholders include senior management, project team members, IT security team members, IT team members, members of any application support team that is impacted by the post-quantum world, policy and compliance team members, IT auditors, "super users" of any impacted application, and anyone else in the organization which could be directly impacted by the post-quantum changes. Not everyone is educated at the same level. Quantum and post-quantum education should be equivalent to an individual's needs, depending on their role and impacts of the post-quantum mitigations upon their role. Senior management likely doesn't need to know the ins and out of cryptographic protocols. Application support teams do likely need to know generally about cryptography and the difference between symmetric, asymmetric, and post-quantum encryption. Project leaders need to have a general understanding of quantum information sciences, cryptography, and the recommended mitigations for particular cryptography scenarios. Subject matter experts need to know the details.

Objective: All stakeholders are appropriately made aware of and trained in post-quantum challenges and mitigations.

2.2.3 Awareness and Education Critical Task Summary

- Create and/or distribute post-quantum awareness and training to senior management and likely post-quantum project team members.
- Get senior management commitment to post-quantum project.
- Start post-quantum project.

2.3 Creating a Post-Quantum Project

Form a post-quantum project and team, create a project timeline, and plan.

2.3.1 Create a Post-Quantum Project Team

Mitigating the threat of quantum computers will likely take many people years to accomplish. The first step after getting senior management approval and support is to create a project team. It is possible that many of the project team members who started on the team may not be on it by the end. An official project will need to be created – lead by a project team and following a project plan with an estimated timeline. The process for creating an official project team varies by organization. In identifying the key participants for your project team, it can be helpful to create a briefing memo, similar to the one used with senior management (as exampled above). This memo introduces the

concept of the post-quantum project and team to possible team members and/or their supervisors. The post-quantum project team needs to include key stakeholders or their representatives.

Generally, the team should include:

- Senior management sponsor
- Project leader, knowledgeable with quantum computing and other related topics
- Project management specialist/leader (with project management skills)
- Meeting recorder (e.g., written, electronic, voice recording)
- Cryptography advisor
- Quantum information sciences advisor (optional)
- IT security manager
- Other IT employees as required
- Compliance/policy administrator
- End-user representative
- Communications specialist
- Accounting/budgeting/purchasing representative
- Inventory manager/specialist
- Other stakeholders as needed

In small organizations, many of these roles may be represented by a single person. In a really small organization, all of these roles may be represented by one person. Many organizations may find it helpful to hire outside consultants who specialize in post-quantum migrations.

It is crucial to work with vendors of the impacted systems as early as possible. They need to be educated about your post-quantum concerns and be able to communicate back to you what their company is doing to address them. Ideally, you want them to assist with the mitigation solutions. You might need to get the vendor involved during or right after the data collection phase of the project.

A communications specialist can be helpful. If all goes according to plan and all the post-quantum mitigations are put into place before the quantum crypto break happens, the communications specialist can help communicate the project to the organization as it is smoothly accomplished. If, however, the quantum crypto break happens before all issues are mitigated, you will need to enact an emergency accelerated plan and timeline. Critical impacted assets may need to be taken offline, there could be business interruption issues, and you will need an incident response plan that includes a thoughtful communication response. Let management and the communications specialist know that the accelerated timeline scenario has a lower likelihood of happening but that you want to be prepared in case it is required.

It might also be wise to initiate discussions with others in your industry, trade organizations, and potentially even competitors. Every organization is going to be tackling a post-quantum project of some type, although with varying timelines and objectives, and everyone will have similar overall goals (i.e., migrating to quantum-resistant cryptography, using QKD, etc.). Everyone can share which actions did and didn't work for them. Make phone calls, have meetings, and bring up the topic at industry meetings and conferences. This is a major migration project of the biggest proportions and it needs an "all hands" approach, starting with awareness.

2.3.2 Create a Plan and Timeline

Every project leader needs to create a detailed project plan, likely creating, tracking, and using some project management software program. It's critical to figure out and document the key tasks and critical paths. The more detail and estimated timelines, the better. Overall, any project management plan should encompass the five major post-quantum mitigation project phases listed above:

- Awareness and education
- Creating a project team and plan
- Taking a data protection inventory
- Analysis
- Implementing post-quantum mitigations

The ultimate objective is to protect or eliminate all quantum-susceptible cryptographic systems that protect sensitive critical data before the quantum cryptographic threat is a realistic threat to your organization. The following is an example table showing major project tasks and estimated timelines of a small to mid-size organization.

Obviously, a real project plan and timeline would have substantially more detail and subtasks, but this is a general, high-level guide for where to start. Many tasks can be started and accomplished simultaneously and run in parallel. Timelines for larger organizations can be substantially longer. This table is simply used as a summary example.

Table 1. Example Post-Quantum Major Project Tasks and Estimated Timelines

Major Project Steps	Estimated Timeline
Education and Awareness	1 month
Get Senior Management Support	1 month
Form a Project Team, Plan, and Estimated Timeline	1 month
Perform a Data Protection Inventory	3-12 months
Analyze Collected Data and Make Mitigation Decisions	3-6 months
Testing, Experimentation, R&D	1-2 years
Implement Post-Quantum Mitigations	1-5 years
Re-Assess Project	End

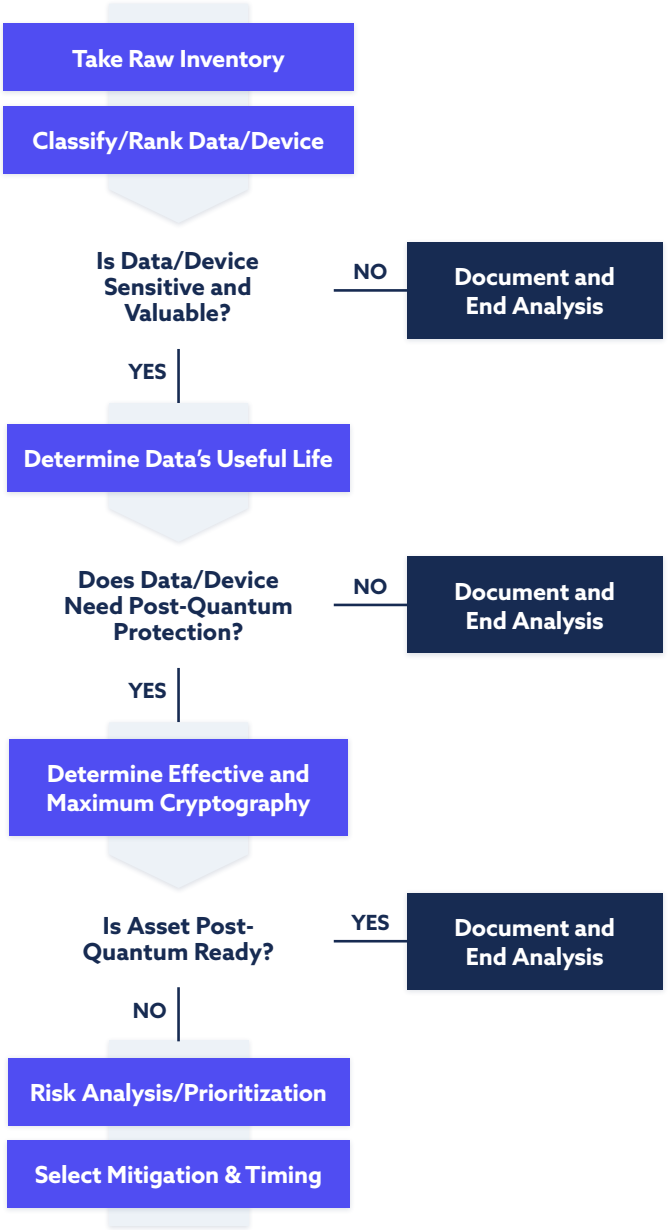
Objective: Formation of the post-quantum project team and approval of members' participation along with funding, resource commitments, meeting space, assets, etc.

2.3.3 Project Team and Plan Phase Critical Task Summary

- Form a project and project team.
- Hold a kick-off meeting.
- Create an initial project plan and timeline.
- Assign project tasks and commitment dates for meeting critical project pathway deadlines.
- Assure the data protection inventory phase will start.

2.4 Taking a Data Protection Inventory

Taking a data protection inventory, analyzing the findings, and using it to determine mitigations are very closely linked steps. A graphic summary is below:



The overall objective of this phase is to determine what data is at risk and determine if it needs to be protected with additional post-quantum mitigations. Performing a data protection inventory is usually one of the most time-consuming and difficult phases of the project and it helps to break it down into smaller subtasks.

Assign someone the ultimate owner role of the data protection inventory task, with responsibilities and authority to accomplish the task. The success of a post-quantum project depends on the accuracy and thoroughness of this step.

2.4.1 Take Raw Inventory

The raw inventory portion of this phase requires that any critical data and devices that could possibly need post-quantum protection be located, identified, and ranked, along with the systems involved in protecting it.

2.4.1.1 Data Protection Inventory Fields

A data protection inventory should include at least these components:

- Description of devices and/or data, including any version information
- Location of all sensitive data and devices
- Identification of owners, stakeholders, and vendors (if any)
- Criticality of the data to the organization
- Determination of how long the data or devices need to be protected from unauthorized eavesdropping (e.g., useful life)
- Identification of data protection systems currently involved
- Effective cryptography they use, particularly cryptographic algorithms, algorithm type (e.g., symmetric, asymmetric, hash, etc.), existing key sizes, and maximum configurable key size
    - Cryptography name/description
    - Cryptographic type (e.g., symmetric, asymmetric, key exchange, hash, digital signature, etc.)
    - Current key size
    - Maximum key size
- Vendor support timeline for data protections
- Other post-quantum mitigations already involved (e.g., physical, QKD, PQC, etc.)
- Post-quantum protected already (Y/N?)

Note: Many data protection systems will have multiple cryptographic selections involved in a single system. For example, Microsoft Windows might show something like TLS_RSA_WITH_AES_SHA2, which means RSA asymmetric cryptography, AES symmetric encryption, and SHA-2 hashing is used. Thus, you'll need to have the ability to record multiple cryptographic algorithms involvement for a single data protection system.

2.4.1.2 Find Data

The task identifies all possible data sources and/or devices that may need to be protected.

One of the most difficult parts is in identifying all information. In most organizations, data is all over the organization. It's on servers, on workstations, on storage devices, portable storage devices, databases, emails, messaging platforms, clouds, backups, etc. One way to start identifying all data is to determine all the inputs and outputs of data to and from every department and team in the organization.

2.4.1.3 Data Protection Inventory Questionnaire

It may be best to begin the inventory with a stakeholder questionnaire. Send out a questionnaire to all department heads and leaders, asking them to identify information they receive, process, store, or transmit, and what systems are involved to do the same – including all devices, software, hardware, and vendors involved. Then ask them to document asset information, versioning information, and cryptographic systems and details, if known.

Your data protection inventory needs to include vendors, consultants, and third parties that either access your network or manipulate your data, similar to the risk management process you should already have in place for vendor risk management. If a device uses cryptography and protects something nonpublic, it needs to be on the list.

Note: Not all devices and applications must be inventoried – only ones that access data you possibly need to protect before and during the post-quantum period.

The inventory should include a thorough accounting of all sensitive data and devices that you need to prevent from unauthorized disclosure before and during the post-quantum period. You need to do the best accounting of where all sensitive data and devices are located, along with the stakeholders who own, safeguard, and rely on the information and devices. Stakeholders are needed to ascertain all the other needed information.

All devices holding or involved with holding sensitive information must be inventoried and investigated. This includes computers, laptops, pad devices, smartphones, smartwatches, network equipment, authentication devices, physical security devices, and others. In most cases, you need to inventory the device's cryptographic protections (including OS) and any applications used to access critical data. Your data protection inventory needs to include hardware and firmware components and all operating systems, servers, workstations, front-end servers, middleware, back-end databases, and supporting infrastructure. The inventory should include critical data and Internet of Things (IoT) devices, such as security cameras, badging systems, and building access control systems. If IoT devices are recording sensitive information or in sensitive areas, they need to be on the inventory list. Identical devices or software programs may contain different data protection systems if they are different versions. Each version will need to be inventoried separately to maintain accuracy.

2.4.2 Classify and Rank Data and Devices

All data and involved systems must be classified according to how critical the data and systems are to the organization and the risk involved to the organization if they were revealed to unauthorized eavesdroppers. Essentially, "do you need to protect it?" There should be several levels of classification so that data and devices can be ranked if they conflict in sensitivity and only one can be protected first. If data is not sensitive and valuable to the organization, it does not need to be protected.

Some organizations use traditional military rankings: top secret, secret, confidential, and public. Others use more corporate equivalents: high business value, medium business value, low business value, etc. Some organizations may use just two labels: confidential and public. Whatever data classification system you use, the central task is to determine if the data or device needs to be protected against unauthorized access in the post-quantum period.

2.4.3 Determine Data's Useful Life

If the data is sensitive and valuable to the organization, you must determine if its useful life to the organization lives into the post-quantum period. The project team should have already determined when they think the post-quantum period starts (in what current or future time period). Then estimate the useful life of the asset and assess if it is still useful and used in the post-quantum period. If the useful life of the data does not live into the post-quantum period, it does not need to have post-quantum protections and can be dropped from the project (unless other weaknesses have been revealed and identified for other remediation efforts). If the useful life of the valuable and sensitive data extends into the post-quantum period, it needs post-quantum protections.

2.4.4 Inventory Cryptography

The next step is to determine if the current cryptographic protection is sufficient to protect that data in the post-quantum period or if it needs additional protection mitigations. Start by determining which cryptography is involved in the data protection system (e.g., algorithm, cryptographic type, key size, etc.). Document what the current settings are for each involved protection system and what maximum cryptography protection could easily be configured. The goal is to determine the effective protection currently provided by the data protection system and the maximum/best cryptography that can be easily enabled, if they are different. For example, a Microsoft Windows 10 system may currently use or offer AES-128-based protection, but can also be easily configured to use AES-256 (and longer). This is not to say that changing a configuration setting involving cryptography is always easy, but that you can recognize that sometimes a "simple" configuration change can allow a strong choice.

Many times, users and stakeholders will be able to identify the systems involved but not the cryptography. Provide subject matter experts when needed. In some instances, you may need to contact vendors (sometimes several times). There are likely to be systems where cryptographic protections cannot be determined.

Every level of cryptographic protection in a complete system protecting data must be documented. Many systems will contain many different, often layered, levels of cryptography. For example, consider a Microsoft Windows system used by an employee or as a database server. The hardware involved will come with cryptography built-in at the firmware layer. There will be cryptography used in the BIOS/Universal Extensible Firmware Interface (UEFI). There can be cryptography used in the firmware of any involved interface cards. Microsoft Windows has lots of cryptography in it, built-in and unconfigurable, configurable, and optional. If you use Microsoft BitLocker to protect hard drive volumes, that will be protected by cryptography. Microsoft Windows uses cryptography all throughout its software, and what cryptography is used changes over versions. Some of the cryptography is "hard-coded," meaning it cannot be changed by the user. Some of the cryptography can be modified by the user/administrator. Some cryptography options are selected by default, but can be changed by the end-user/administrator.

The applications that run on the computer may come with their own built-in cryptography as well. For example, a user can choose among dozens of different browser programs. The cryptography used by Microsoft Edge will be different from than that used by Google Chrome, Mozilla Firefox, or Opera. If the user or computer gets PKI digital certificates to use for encryption and digital signing, those may be of another type of cryptography.

Note: Organizations with industrial control scenarios (e.g., SCADA, ISC, etc.) will need to include equipment, sensors, embedded devices, etc., in their inventory. If it is involved in critical data protection, it should be surveyed and inventoried.

In other instances, developers programming cryptography may implement their cryptography solutions or rely on other existing cryptographic providers. It may require looking at the source code or talking with the developers to confirm what cryptography is used with a particular program. If the source code or developers are not available, it may be difficult or impossible to find out what cryptography is used. If a particular application's or data store's cryptography cannot be determined, it should be considered as "unknown" and considered high risk, making replacement necessary if the involved data is critical and needs to be protected into the future.

Lastly, you must determine the support life of any data protection system vendor involved in protecting the data. How long will the vendor continue to support the current data protection implementation? Is the vendor or data protection system going to go out of support before the post-quantum mitigations can be implemented? Is the vendor going to support and be a part of the post-quantum mitigation process or do you have to work without or around them? You need to determine how involved the current implementation's vendor will or won't be in your post-quantum mitigation project. Some vendors may be actively planning and will help you migrate to post-quantum solutions. Some vendors may require a big upgrade or new version to be purchased to support your post-quantum plans. Many vendors are likely to be unaware of the coming quantum threats and your inquiry could be among the first they receive inquiring about the risks, leading the vendor to their own post-quantum project.

2.4.5 Determine Effective Cryptography

It's also important for the data protection inventory process to determine the effective "ruling" cryptography that ultimately protects each piece of critical data – both currently and the maximum, most protective values that can be easily configured. Continuing our last example using a Microsoft Windows system, the critical data may currently protected by AES-256 (AES using 256-bit keys) using field-level encryption in Microsoft SQL Server 2019, even if the user's own workstation only uses a maximum AES-128 (AES using 128-bit keys). What is the effective cryptographic protection in that scenario? It's important that the data protection inventory analysis determines which encryption is providing the ultimate "effective" protection, which is what concerns us. If the evaluator feels the database server's protection effectively protects the data even if the user's workstation protection is less, the data can still be documented as being protected by the higher-level of cryptographic protection.

The converse may often be true (and usually is). Continuing our example, if the workstation's cryptographic protection is less than the server's but the data is accessible on the workstation, then the data's effective protection is likely to be the lesser of the two protection levels because an attacker can attack the data using or at the user's workstation level. In most cases, the effective cryptographic protection of a critical piece of data is the least strong cryptography involved – if an attacker can attack it to gain access.

Note: When determining the effective solution, special care must be given to key generation (see RFC 4086), key distribution, and key rotation, as well as key protection at rest and while in use.
It is also important to track both existing and implemented cryptography settings and maximum possible cryptographic choices. For example, if a system currently uses AES-128 but could be easily modified to use AES-256 or longer, that should be noted as the maximum effective protection possible. A system that can be easily modified to meet post-quantum requirements would not require upgrading, replacement, or removal.

Note: It is also not uncommon for particular cryptography to be present but not used. Don't let a simple inventory process that detects a particular type of cryptography always indicate that that particular cryptography is used. Ensure that the cryptography you capture as the "effective" cryptography is the cryptographic protection being used.

2.4.6 Track by Implementation Version

It is up to the data protection inventory process to capture all the possible cryptography used by the organization to protect post-quantum data. It can be a very difficult task. The task can be simplified some by documenting the cryptography used by a particular version of a common item. For example, all users using Microsoft Windows 10 of particular "build" versions will have the same Windows cryptography available. The same is true of users of the same devices with similar range of firmware versions. Once an inventory individual has verified and documented the various cryptography used by different component versions, knowing the components and the versions of the components can help the inventory collector establish what cryptography is present without having to individually interrogate each duplicate component.

For many systems, you may be unable to determine what the ciphers, schemes, and key sizes are. The vendors or developers may be gone, with little to no available documentation regarding the implemented cryptography. The project team will need to review each found "unknown" and determine whether the risk is so minor that it can be ignored for migration purposes or if upgrading the involved system needs to be considered a top priority. Plan for your unknowns.

It's important to involve any impacted third-party vendors into the project as soon as possible so that they understand your concern and can let you know how their company is planning to help. In many cases, the vendors may be completely unaware of the issue or, if they are aware, they have not practically addressed it because they think it's 10-20 years off. Discussing your concerns with them may be the start of serious discussion within their company. You may even learn that they don't plan on moving to a post-quantum implementation or that it requires upgrading to the latest version of their software to fix. In the past, many vendors (most of the time rightly so) used the SHA2 migration move to force customers to upgrade to the latest software.

Many companies may have internally developed applications and will need to find out who is in charge of them and how they can be upgraded. It is common to find internally developed applications for which no information can be found and for which no one can be hired to analyze and update. Your project team should have already decided how to handle such applications, or perhaps they are reviewed on a case-by-case basis.

Note: Data protection inventories can easily involve a lot of time and resources. Every project leader must be prepared for this to be one of the most time-consuming and challenging parts of the project. This is to be expected. However, the outcome of the inventory can be used for all other types of useful purposes and projects, especially if maintained in an ongoing state.

2.4.7 Data Protection Inventory Tools

The Cloud Security Alliance Quantum-Safe Security Working Group is unaware of any tools or vendors that easily automate the collection of the information needed for the data protection inventory, but there are some inventory tools that can be used to automatically collect some answers of some components. For example, some PKI inventory systems can reveal digital certificates which have been issued to subscribers and the relevant and necessary cryptographic information. However, in practice, most of the automated checks are very limited in the type of inventory information they can collect and/or hugely inaccurate.

Some sort of customized data protection tracking tool must usually be created and used. Most data protection inventory managers use a custom-created database or spreadsheet program. It can be useful to import any hardware and software inventories the organization may already maintain as a starting point. Conversely, the hardware and software inventory program may be a place to document the data protection inventory if custom fields can be added.

Objective: Documentation of all involved systems storing critical data needing protection during the post-quantum period, including the cryptographic protections involved (e.g., cryptographic algorithms, cryptographic algorithm type, current key sizes, and maximum key sizes allowed).

2.4.8 Data Protection Inventory Phase Critical Task Summary

- Select data protection inventory task owner.
- Document all involved systems storing critical data needing protection before and during the post-quantum period, including the cryptographic protections involved (e.g., cryptographic algorithms, cryptographic algorithm type, current key sizes, and maximum key sizes allowed).

2.5 Analysis

In this phase of the project, determine which systems have adequate post-quantum protection and select the appropriate mitigations for those needing additional protection. This process can be assisted by this section and the next, *Selecting and Implementing Mitigations*.

2.5.1 Analysis Objectives

Analysis and recommendations will include the following tasks:

- Identifying quantum-susceptible data protection systems protecting critical sensitive data and devices
- Prioritizing/ranking the systems needing remediation
- Determining if systems already meet post-quantum requirements or if they require setting modifications, updating, replacement, additional mitigations, or removal
- If needed, selecting post-quantum remediations (from the list of mitigations in the next section)
- Determining related resources, costs, and timelines
- Getting approval for implementing mitigations and timelines

2.5.2 Determine Post-Quantum Readiness

Verify if systems already meet post-quantum requirements or if they require setting modifications, updating, replacement, or removal. Determining if a system needs post-quantum mitigations involves looking at current protections. If a system is already protected by physical isolation, QKD, PQC, long enough symmetric key sizes, or quantum-enabled programs, no additional remediation may be needed. If remediation is needed, the project team should select the appropriate remediation. In some cases, configuration changes can provide mitigation. In others, upgrades or replacements may be needed. In some cases, removal of a weakly protected asset may be the best decision. In other cases, a weakly protected asset may gain protection by being moved into a highly isolated space where unauthorized access is difficult to perform.

Many post-quantum mitigations will come down to common choices including:

- Physical isolation
- Increasing symmetric and hash key sizes
- Replacing asymmetric ciphers, keys, and digital signatures, with post-quantum cryptography alternatives

- Using QKD
- Using hybrid solutions
- Using quantum-enabled protections

The rest of this section focuses on how to determine if a known and commonly used cryptographic standard is considered quantum-susceptible or quantum-resistant (i.e., PQC).

2.5.3 Quantum-Susceptible Cryptography

The following cryptographic algorithms are considered quantum-susceptible:

- All cryptography already considered weak or broken by classical computers.
- Current asymmetric cryptography standards (i.e., public key exchange, public key encryption and signature) that **are not** considered PQC; these include RSA, Diffie-Hellman, Elliptic Curve Cryptography, and ElGamal. In most organizations, this will cover all currently used public key schemes.
- Symmetric ciphers with key sizes less than 256-bits and older ciphers, including AES-128.
- Hashes with hash sizes less than 256-bits.
- Unknown, private ("homegrown"), and non-standard cryptography unless proven otherwise (even if the vendor claims their private cryptography is PQC).
- Any cryptography not listed as a quantum-resistant standard by NIST or other internationally-accepted cryptography standards bodies.

Note: Quantum-susceptible and quantum-resistant ciphers and their characteristics can be found In several sources (including: https://csrc.nist.rip/Projects/Post-Quantum-Cryptography/faqs).

2.5.4 Quantum-Resistant Cryptography

Quantum-resistant cryptography includes:

- Known NIST PQC asymmetric ciphers/key exchanges, including: Classic McEliece, CRYSTALS-KYBER, NTRU, SABER, BIKE, FrodoKEM, HQC, NTRU Prime, and SIKE.
- Known NIST PQC asymmetric digital signatures, including: CRYSTALS-DILITHIUM, FALCON, Rainbow, GeMss, Picnic, and SPHINCS+.
- Generally accepted traditional symmetric algorithms with key sizes 256-bits or longer, using secure modes of operation, including AES.
- Generally accepted traditional hashes with key sizes 256-bits or longer, including SHA-2 and SHA-3.
- Any cryptography listed as quantum-resistant by NIST or other international cryptography standards body.
- QKD.
- Quantum-enabled cryptography (as accepted as a standard from an internationally-accepted cryptographic standards body, like NIST).

WE RECOMMEND THAT EVERY ORGANIZATION SHOULD BEGIN THEIR POST-QUANTUM MITIGATION PLAN AS SOON AS POSSIBLE.

Note: The quantum-resistant cryptography listed above are the known NIST-acceptable candidates at the time of publication. Please check the NIST PQC site for updated information and consideration. Some PQC cryptography candidates may be disqualified for NIST consideration as new attack information is learned.

Note: Some previous NIST PQC candidates may have been dropped from further consideration due to flaws found in the submitted configurations. Just because a candidate was dropped from the current NIST PQC consideration does not mean the cryptography isn't quantum-resistant; however, using a cryptographic algorithm that is not approved or recommended by NIST comes with additional risks and considerations and is not recommended.

Note: If you have not been able to determine if an identified cryptographic function is quantum-susceptible or quantum-resistant, mark its status as unknown but treat it as potentially quantum-susceptible until disproven.

Compare what you learn in the analysis phase to the list of cryptography and key sizes listed above. Any data protection system protecting critical data or devices and using quantum-susceptible cryptography should be highlighted, with special attention paid to the most critical systems. Then, after a thorough examination of all the involved systems, criticalities, timelines, and costs, project leaders and stakeholders should decide what remediation to deploy and when. Document the decisions and present them to senior management for approval and budgeting. If you've done the analysis and review correctly and thoroughly, the possible solutions make the ultimate decision easy for most of the decisions.

Objective: Determination of needed post-quantum mitigations.

2.5.5 Analysis Phase Critical Task Summary

- Identify critical systems needing post-quantum mitigation.
- Decide which mitigations will be used to mitigate post-quantum risks.

2.5.6 Risk-Analysis Approaches and Timing

Not all at-risk assets (i.e., data, devices, systems, etc.) have the same mitigation priority.

2.5.6.1 Greatest Risk Remediation First

Mitigation timing should be driven by the risk analysis, with the biggest, most likely risks mitigated first. It is likely that it will be determined that a few at-risk assets need to be protected immediately, followed by the bulk of at-risk assets protected during the main stages of the post-quantum protection project, followed by less risky assets that can be neglected until after the higher-risk assets are protected.

In most post-quantum mitigation plans, the traditional risk analysis approach should be followed. However, there are some other alternatives some organizations may wish to consider.

2.5.6.2 Low-Hanging Fruit Approach

Some quantum mitigations are easier and less resource-intensive to implement than others. There may opportunities for defenders to make quick improvements in some areas even if the risk analysis portion of the mitigation plan indicates other focus and timing. For example, it is likely that post-quantum asymmetric cryptography replacement of quantum-susceptible cryptography algorithms will take longer and be harder to perform than upgrading susceptible key sizes of existing quantum-resistant symmetric ciphers and hashes. Defenders might look for opportunities for "low-hanging fruit" and "easy wins" to see if they might benefit their overall post-quantum mitigation plan enough to adjust timing of various tasks based on risk analysis alone. Many times, accomplishing smaller, easier project tasks helps multi-year teams accomplish the longer and more resource-intensive mitigations by using the previously demonstrated success to improve overall morale.

2.5.6.3 Low Complexity Approach

With the standard risk analysis approach, each asset to be protected may have a different risk analysis and thus a different timeline and task in the post-quantum mitigation plan. You could even have, for example, two tables in the same database which need different levels of protection. In many post-quantum mitigation plans, the data protection inventory analysis portion could easily result in dozens to hundreds of different mitigation plans and timings. Some organizations may find it less resource intensive to categorize related data with mixed levels of risk into a single remediation task to reduce remediation complexity. Continuing the simple example above, instead of fixing two tables using two different remediation plans and timings, fixing the entire database at once resolves both the higher-risk and lower-risk tables with fewer resources than if they were handled separately.

Objective: Determination of mitigation timing for various at-risk assets.

2.5.6.4 Risk-Analysis and Timing Critical Task Summary

- Determine which assets need to be mitigated and in what order.

2.6 Implementing Post-Quantum Mitigations

Defending against cybersecurity risks and threats requires the best defense-in-depth, cost-justified combination of policies, technical defenses, and education that a defender can deploy. This section of the paper summarizes the recommended policies and technical controls a defender can deploy to significantly reduce risk of compromise from quantum computer threats.

2.6.1 Policies and Documents

A defender must create policies that decrease the risk in the post-quantum world. If not already enacted, these policies should be implemented as soon as possible to reduce risk now and in the future.

Note: Every organization must determine which post-quantum solutions are desired, required, or denied by any governing compliance regulations or agencies. It is possible that current requirements could prevent one or more mitigations ahead of the government body updating their standards or requirements. Standards and regulations must be considered when selecting mitigations and updating organizational policies and documents.

2.6.1.1 Update Existing Acceptable Cryptography Standards

Every organization should have "acceptable cryptography" policies that define which cryptographic algorithms and key sizes are allowed and acceptable in the products and services they purchase or use. If not, one should be created or a section added to existing security policy. At the very least, it should state that any products under consideration for purchase or use, if they use symmetric ciphers, should use key sizes 256-bits or longer. Strong consideration should be given to products which are "crypto-agile," meaning that the existing cryptography can be easily swapped out with NIST-approved PQC finalists when they are announced. The intent of this policy addition is to prevent additional problematic cryptography from continuing to be introduced into the organization, knowing that every quantum-susceptible protection must be mitigated or replaced. Require senior management approval for exceptions.

2.6.1.2 Update IT Audit Programs

If your organization has internal IT audit programs performed by internal or external auditors, ask the auditors if their audits consider post-quantum risks. They are likely not to understand the question, so provide appropriate awareness and education. Ask that IT audit programs be updated to reflect post-quantum risks and controls. For example, an audit program might ask if all utilized symmetric ciphers use key sizes 256-bits or longer.

2.6.1.3 Vendor Attestation Documents

Reach out to all vendors who provide data protection to critical data and get their official statements on their post-quantum protections and future roadmaps, if not already known and documented. You want to make sure all your vendors are aware of your concerns, your expectations concerning their products, and the threat posed by the post-quantum world.

2.6.1.4 Third-Party Vendor Management

Update third-party vendor computer security surveys and controls to take account of post-quantum concerns. All third-party vendors, consultants, and contractors should be educated about the coming post-quantum risks and be asked to participate in your post-quantum project's efforts.

2.6.2 Technical Mitigations

Here are some common technical mitigations that can be used to provide post-quantum protection to assets and data needing it:

2.6.2.1 Physical Isolation

In some scenarios, physical separation/isolation might be desired or required to prevent unauthorized access to critical information in a post-quantum world (or before that, if worried about early eavesdropping). If possible, keep your most critical data from being eavesdropped on. This means off the network, and especially Wi-Fi networks, especially if those Wi-Fi networks are contactable remotely from public areas. Remember, most existing Wi-Fi networks are not quantum-resistant without additional remediation.

2.6.2.2 Strengthen Symmetric Key Sizes

Any existing symmetric ciphers that are not quantum-resistant should be replaced or upgraded to commonly accepted quantum-resistant ciphers and key sizes. This means generally accepted traditional symmetric algorithms with key sizes 256-bits or longer, including AES, SHAKE, and SNOW 3G.

2.6.2.3 Use Post-Quantum Cryptography

For asymmetric cryptography, replace quantum-susceptible versions with NIST PQC versions[5] **after** NIST approves the finalists. Early adopters or organizations with enough resources may want to begin moving to one or more PQC latest-round candidates (as listed above in the *Quantum-Resistant Cryptography* section) in test or limited-scale projects early.

Once NIST selects the finalists, any organization can begin immediately testing and migrating their quantum-susceptible versions to PQC versions. There is still a risk that any NIST-selected PQC finalist could later be found to be overly susceptible to a cryptographic attack and removed as a NIST standard, but the risk is low and would be shared with every organization in the world who used the same cryptography.

2.6.2.4 Implement Quantum Key Distribution to Protect Networks

Because of the observer effect and no-cloning theorem, quantum mechanics can be used in Quantum Key Distribution (QKD) devices to securely create, protect, and transmit encryption keys (traditional or post-quantum) between an authorized source and destination. Consider using QKD to protect entire network segments. There are already hundreds of QKD-protected networks in real-world use today.

QKD devices are offered by many vendors. Many customers have been buying and using QKD devices since their availability. You need a QKD device on each side of the network between the authorized source and destinations, usually using direct fiber optic segments. Keep in mind that QKD-protected wired networks are limited to about a maximum transmission length for a single unrepeated, segment due to limitations of quantum-transmitted information over physical (bound),

---

5 National Institute of Standards and Technology (NIST). *Post-Quantum Cryptography*. Accessed August 18, 2021, at https://csrc.nist.gov/projects/post-quantum-cryptography.

fiber optic cable mediums. To utilize QKD over longer bounded distances requires removing the transmitted information from its quantum state, reading it, reconstituting the data back into another quantum state instance, and then re-transmitting again using quantum methods and "trusted nodes" – but doing so removes the complete, end-to-end quantum protection.

This limitation should be lifted in the future with the use of *quantum repeaters*, which will allow carrying quantum states from end to end. The main missing technology brick to build these quantum repeaters is the quantum memory, which can store and release qubits upon request. We expect that quantum repeaters shall be available within 10 to 15 years, and they could then be added as upgrades to existing QKD networks. The ultimate goal of quantum communication is the Quantum Internet, which will coexist with the current classical internet and offer new, probably unexpected, applications.

PQC and QKD mitigations are both valid options for protecting transmitted data, and they are often considered as the only two options by evaluators looking for post-quantum protection for their networks. There are advantages and disadvantages for each approach. With the current technology limits on QKD discussed above, PQC will be used for all general public applications and QKD will be restricted to more specialized ones. Trying to predict the future evolution once the necessary quantum technology is available would go far beyond the scope of this paper.

2.6.2.5 Hybrid Defenses

There are a myriad of post-quantum mitigations that implement the combination of PQC or QKD with traditional cryptography in a single solution. These implementations are often used as a way to provide increased protection or easier coverage. For example, PQC can be used in addition to/over/under classical cryptography in TLS connections to provide enhanced TLS connections between websites and customers. When classical and PQC are combined, if one becomes compromised, the other may continue to provide protection. Hybrid solutions often bridge the gap between quantum-susceptible to fully quantum-resistant defenses.

2.6.2.6 Implement Quantum Random Number Generators

Random number generators (RNGs) are crucial to digital security and cryptography. Quantum random number generators (QRNGs) can provide true randomness. For applications needing the best randomness, consider using QRNGs. As the price, size, power consumption, and availability of QRNGs becomes comparable to non-quantum RNGs, QRNGs will become more widespread across the whole industry.

Both PQC and QKD benefit from QRNG. Many of the leading contenders in the NIST PQC evaluation are lattice-based algorithms, which require both higher bandwidth and higher-quality entropy than current standard asymmetric algorithms. That is to say, PQC often needs far more random numbers as well as a different sort of randomness than existing cryptography standards. For example, using the RSA protocol requires between two and four random numbers for each key exchange operation. Under a structured lattice-based algorithm, such as NewHope, the same transaction may require a few hundred random numbers for equivalent security. For an unstructured lattice PQC algorithm such as FrodoKEM, the entropy requirements are higher than that by roughly a factor of ten.

Furthermore, the security proofs of these PQC algorithms require that their entropy be obtained by sampling gaussian distributions rather than uniformly distributed entropy, which is what is typically produced by most current RNGs.

QKD systems also depend on high-quality random numbers for their security, but generally the entropy sources will be included with the QKD system. You should inquire of the vendor if their entropy is based on QRNG sources.

2.6.2.7 Other Quantum-Enabled Protections

Several projects are working on quantum-enabled protections, such as using quantum-enabled networks and cryptography. In general, these types of "full quantum" protections are further out than the previously listed mitigations and certainly are more limited and more expensive. But keep abreast of the latest news about quantum information science and offer to learn when full quantum protections become widely available and cost effective.

Note: It's important to understand that PQC protection does not use any quantum information science to provide its protection, whereas quantum-enabled cryptography does. Theoretically, quantum-enabled cryptographic protections have the likelihood of providing greater protection than non-quantum solutions.

2.6.2.8 Testing

Organizations with the appropriate resources are encouraged to begin testing potential PQC solutions in their own environments and applications. PQC solutions can impact performance and usability. By testing PQC solutions, an organization may learn about particular challenges in their own environment and be better prepared for the post-quantum migration project overall. There are many resources available to help developers and testers with PQC implementations, including:

- Open Quantum Safe
- NIST *Post-Quantum Cryptography Standardization*
- NIST National Cybersecurity Center of Excellence *Migration to Post-Quantum Cryptography*
- ETSI *Quantum-Safe Cryptography*

Regardless, all organizations must test quantum mitigations before implementing at full-scale in production environments. Catastrophic operational interruption can result from inadequate testing.

2.6.2.9 Encourage Crypto-Agility

It is important that all implementations of cryptography be "crypto-agile" if possible, meaning that cryptographic routines and ciphers can be easily upgraded or replaced without having to completely replace the underlying application or device. For example, for many features of Microsoft Windows and even in Microsoft's flagship Certification Authority platform, Active Directory Certificate Services, the cryptography used can be installed and uninstalled away from the product (the individual cryptographic algorithms are implemented as a Key Storage Provider or Cryptographic Service Provider).

Note: Other Microsoft products, such as Microsoft Office 365, Azure, SQL, Azure Key Vault, etc., are currently not crypto-agile. Crypto-agility is determined on a case-by-case basis, but should become a part of every solution and application.

OpenSSL is a common, open source cryptography program. It was designed from the very beginning to allow the switching of and use of different cryptography algorithms.

Contrast crypto-agile programs with devices, systems, and programs that require a complete upgrade or replacement to support the newer cryptography. In general, you want to avoid things which are not crypto-agile and to encourage all vendors who use cryptography in their products to be crypto-agile. In the event you need to replace a quantum-susceptible algorithm with a quantum-resistant one, accomplishing it on a crypto-agile implementation makes it easier. Encourage buyers, administrators, and users to look for and use crypto-agile products when given a choice.

2.7 Post-Quantum Implementation

The final phase is to select and implement the appropriate post-quantum defense.

Objective: Implementation of all policies, technical controls, and education needed to mitigate critical post-quantum cybersecurity risk.

2.7.1 Mitigation Phase Critical Task Summary

- Select the appropriate post-quantum mitigations to significantly reduce cybersecurity risks from sufficiently strong quantum computers.
- Implement all policies, technical controls, and education needed to mitigate critical post-quantum cybersecurity risk.

2.8 Other Post-Quantum Implementation Resources

- NIST *Getting Ready for Post-Quantum Cryptography*
- NIST *Report on Post-Quantum Cryptography*

Appendix A. Example Senior Management Memo Explaining Quantum Threat and Project

To: Whom It May Concern

Re: Preparing for Coming Quantum Cryptographic Risks

This document was created to help introduce management to a newly proposed project tentatively titled Post-Quantum Data Protection Project and to share critical details, the proposed response to reduce cybersecurity risk, and estimated project timeline. The objective is to obtain senior management recognition and support for this critical new project.

Computers based on quantum mechanics are maturing to a point where they seriously threaten to compromise much of today's existing cryptography, including HTTPS, Wi-Fi networks, logon authentication, smartcards, multifactor authentication, and public key infrastructure (PKI). No one knows exactly when quantum computers will mature to the point of being a real threat to most organizations, but estimates range from a few years to over ten years. In 2016, the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) recommended that all organizations start to prepare for the coming cryptographic break.

As part of following those recommendations and due to ever-increasing improvements in quantum computing, we are preparing this organization by creating a special project team to address the issue. We will be performing a data protection inventory (to determine which of our critical digital assets need long-term protection against unauthorized access) and creating a plan to ensure that critical data is protected by the appropriate quantum-resistant mitigations.

The first major phase of the project, along with the work of our newly formed project team, will begin in the next few weeks and is expected to last multiple years until threat is fully remediated. Our goal is to upgrade our quantum-susceptible cryptography to quantum-resistant forms and other mitigations before the quantum computer threats become realized. However, the work product created as a result will help with our "crypto-agility" and will useful in other future projects.

This project is likely to impact many of our existing data protection implementations and our reason for beginning this project now is to minimize future business disruption and costs. Overall project costs, resources, and timelines cannot be adequately estimated until after the Data Protection Inventory and Analysis tasks, which are expected to be accomplished in the next 6-12 months. We will be following and using industry guidelines and methodologies wherever possible.

I will be glad to answer any of your questions and/or provide you with more details and education.

Page 2 – Frequently Asked Questions (FAQ)

What is quantum mechanics?
Quantum mechanics/physics is a long-proven physical science that describes actions and properties of very small particles. Everything in the universe works and depends on quantum mechanics. It's how the world works. Computers and software are being created that function using quantum particles and properties. Within a few years, if not already, we will have quantum computers capable of doing things non-quantum computers cannot, including breaking many forms of traditional cryptography and creating new, unbreakable forms of cryptography.

How long have quantum computers been around?
The first working quantum computer was created in 1998. Today there are hundreds of fairly crude quantum computers and hundreds of different types of quantum devices. All known quantum computers are still relatively weak and are in the laboratory and experimental stages, but are predicted to become stronger as time goes on. The world's governments and corporations are spending billions of dollars a year in the pursuit to build quantum supercomputers and networks. Quantum computer vendors include the world's largest companies, such as Google, IBM, Intel, Microsoft, and Alibaba.

How is quantum computing able to threaten traditional cryptography?
Particular types of quantum computers, armed with a mathematical algorithm known as Shor's algorithm, can quickly factor math equations that involve large prime numbers. Equations involving large prime numbers are what gives most traditional public key cryptography its protective capabilities. Traditional binary-based computers cannot easily factor large prime number equations. Quantum computers with enough "qubits" can factor large prime number equations in a very short amount of time, measured in minutes to days.

When will quantum computers break traditional public key cryptography?
No one knows for sure, although as soon as quantum computers get four thousand or so "stable" or usable qubits, or that computational equivalent, it is believed that traditional public keys 2048-bits long or shorter will be quickly crackable. Most of the world's existing public cryptography relies on such keys. Quantum computers are capable of weakening the protective power of the other types of cryptography, such symmetric key cryptography. General estimates of time until quantum computers are capable of breaking traditional public crypto range from a few years to over ten years. Either way, most experts and the US government say now is the time to start preparing. If the break happens sooner than people are expecting, then we are better prepared to respond appropriately.

What are we doing?
We are forming a new project team, called the Post-Quantum Data Protection Project Group, to look at all the places where our critical data protection could be impacted and where the risk may need to be mitigated. Near-term mitigations are likely to include increasing existing cryptographic key sizes, isolating critical data, implementing quantum key distribution protections, implementing hybrid solutions, and moving to quantum-resistant cryptography. Long-term mitigations, many years out, include migrating to quantum-based ciphers and devices.

How can you help?
We need senior management to approve this project and give it their backing. An empowered stakeholder needs to attend the first project meeting, perhaps attend further meetings, and answer questions from other senior managers.