



Post-Quantum Cryptography (PQC) Working Group

Future State Technical Paper

Contents

Introduction	4
Abstract.....	4
Scope.....	5
Objective	5
The Financial Services Industry is at Risk.....	5
When Will Quantum Computers be a Threat?.....	5
Opinions Will Vary	6
Many Opinions Agree	7
Defining the Threat	8
Data Protection.....	10
Data-in-Motion	10
Data-at-Rest	11
Data-in-Use	11
Harvest Now, Decrypt Later	12
Data Management	13
Where are the Crypto Assets?.....	14
The Inventory Problem.....	15
Creating a Full Inventory	15
How do we get There?	16
Self Identification	17
Scanning to Populate an Inventory.....	18
Documenting the Known	18
Documenting the Unknown.....	19
Application Development.....	19
Manual Code Review	20
Software Bill of Materials.....	20

Other Inventory Considerations.....	22
Risk Assessment	23
PQC Risk Assessment Frameworks	23
Summary of Mosca’s Quantum Risk Assessment	24
Summary of the CARAF Framework	26
Phase 1: Identify Threats	27
Phase 2: Inventory of Assets	27
Phase 3: Risk Estimation	27
Phase 4: Secure Assets Through Risk Mitigation	27
Phase 5: Organizational Roadmap	28
FS-ISAC PQC Risk Assessment Guidance	28
Phase 1: Discovery.....	28
What is at Risk?	30
Initial Risk and Exposure Evaluation.....	30
Potential Quick Wins.....	31
Phase 2: Risk Modeling	31
Risk Scoring	31
Phase 3: Define Risk Tolerance	32
Phase 4: Prioritization.....	32
Phase 5: Outcome.....	33
Assessing Vendor Readiness	33
Solution Space	34
Transitioning to PQC	35
Quantum Key Distribution (QKD).....	36
Measuring Readiness	37
Testing/Attestation.....	37
Degrees of Readiness	38



PQC Working Group

Future State

Conclusion	40
References	41

Introduction

This FS-ISAC technical paper discusses the future state of Post-Quantum Cryptography (PQC) for the financial services industry. PQC algorithms are the next generation of asymmetric cryptography under development by the National Institute of Standards and Technology (NIST). The inevitable cryptanalysis threat from quantum computers necessitates yet another cryptographic transition^[2] but on a worldwide basis.

Abstract

For thousands of years, humans have relied on classical (Newtonian) physics to shape and interface with the world. Algebra, geometry, basic chemistry, classical physics and the early laws of motion and gravity were responsible for everything from the wheel to levers & fulcrums, gunpowder, metalsmithing, and even the combustion engine.

About 100 years ago, the First Quantum Revolution fundamentally changed the way humans perceive the world. The revolution was born out of the modern model of the atom and quantum theory where light (and all electromagnetic energy) is made of individual particles (photons) that sometimes behave like particles and sometimes like waves; where space is warped by gravity, and time is relative to the observer.

From this set of revolutionary ideas, sprang virtually every aspect of modern technology and gave rise to inventions like television, microwave ovens, transistors/semiconductors, lasers, space flight & satellites, smart phones, the Internet, and the atomic bomb.

The Second Quantum Revolution peers deeper into the strange world of quantum mechanics and an array of fundamental particles that behave in ways we still don't fully understand but are learning to harness and engineer. Physicists, scientists, architects, engineers, and inventors are leveraging quantum phenomena like entanglement and superposition of individual quantum particles to usher in a new chapter of human technology. As in any revolution, there are profound gains to be made, as well as profound risks to be understood and mitigated.

Scope

The scope of this paper is limited to Post-Quantum Cryptography (PQC) and its impact and ramifications to the landscape of data security to the financial services industry. The larger encompassing field of Quantum Technology (including quantum computing, sensing, navigation, quantum networking, etc.) is out-of-scope.

Objective

The objective of this paper is to provide the reader with an overview of the future state for PQC readiness with suggestions on how to get from “here” to “there” for the financial services industry. Historically, based on previous cryptographic transitions, the projected timeframe is over the next 5 to 20 years.

The Financial Services Industry is at Risk

Who is the financial services industry? The stakeholders include financial institutions (Tier 1 banks) including regional banks & credit unions, merchants (retailers), service providers, payment brands (e.g., Visa, MasterCard, American Express, Discover), payment networks, manufacturers including hardware and software vendors, and government including federal, state, and local agencies.

Financial retail payments encompass issuers (banks who issue cards and authorize payments), acquirers (service providers who process merchant transactions), merchants (retailers who accept payments), cardholders (customers and consumers), and payment networks (service providers who interconnect issuers and acquirers). Note that “retail payments” have expanded beyond just plastic cards to include mobile financial apps. Note that the American National Standards Institute¹ (ANSI) designated the Accredited Standards Committee X9² to develop national standards for the financial industry, as well as designating the X9 US Technical Advisory Group (TAG) to ISO Technical Committee 68³ Financial Services, and the TC68 secretariat.

When Will Quantum Computers be a Threat?

The timeline for achieving the future state is driven by the advancements towards building a quantum computer which can be programmed to mount a viable attack. Essentially, known quantum attacks on classical cryptography amount to executing Shor’s or Grover’s

algorithms (or their optimized variants). It is therefore worth discussing the capacity of a quantum computer that can run those algorithms efficiently, allowing a quantum attacker to succeed in a viable time frame, which is typically much sooner than using the classical computing approaches that resort to an optimized variant of brute force search.

The practical quantum computing journey started some 24 years ago, with the first 2-qubit implementation. The growth in the number of qubits has since been developing significantly and more recently accelerated with Google reaching 72 qubits in 2018 and IBM 128 qubits in 2020. Quantum Computing capability is expected to further develop exponentially, supported by large investments worldwide^{4,5}.

Shor's and Grover's algorithm designs and their optimized variants assume operation on ideal, also called "logical" qubits, that can perform gate operations without the limits posed by the current evolution of quantum computer architecture, e.g., coherence time, fidelity, error correction, etc.

Assuming such an ideal quantum computing architecture, running Shor's algorithm to factor a 2048-bit RSA key is currently estimated to require 8194 ideal qubits. Using error correction and assuming optimistic error rate of 10^{-5} , an attack breaking 2048-bit RSA in one month would thus require ~ 8.7 million physical noisy qubits⁶.

Considering symmetric ciphers, running Grover's algorithm to perform exhaustive search to find an AES-256 key requires ~ 35000 ideal (logical) qubits. Using error correction and assuming optimistic error rate of 10^{-5} , an attack would reduce the security to 166 bits, needing a total of 16 billion noisy qubits⁷.

Opinions Will Vary

Based on expert opinions, the risk of quantum computing breaking current cryptography is accelerating and could materialize in less than a decade.

To assess the likelihood of sufficiently capable quantum computing becoming available to break public-key cryptography in the future, Prof Michele Mosca and his team at the Global Risk Institute and the University of Waterloo have performed a survey every year since 2019. In the survey, they asked prominent global experts in quantum computing theory,

hardware, computer scientists, physicists, and cyber security experts about their sentiment⁸. They record the responses and present them as cumulative probability of quantum computing becoming available that could break RSA in any given period in the future. While the responses still put this capability 10 or more years in the future, there is an interesting positive trend in opinion shifts over just three years, indicating that the predictions are becoming more bullish. See Figure 1 Estimates Breaking RSA-2048 courtesy of the Global Risk Institute.

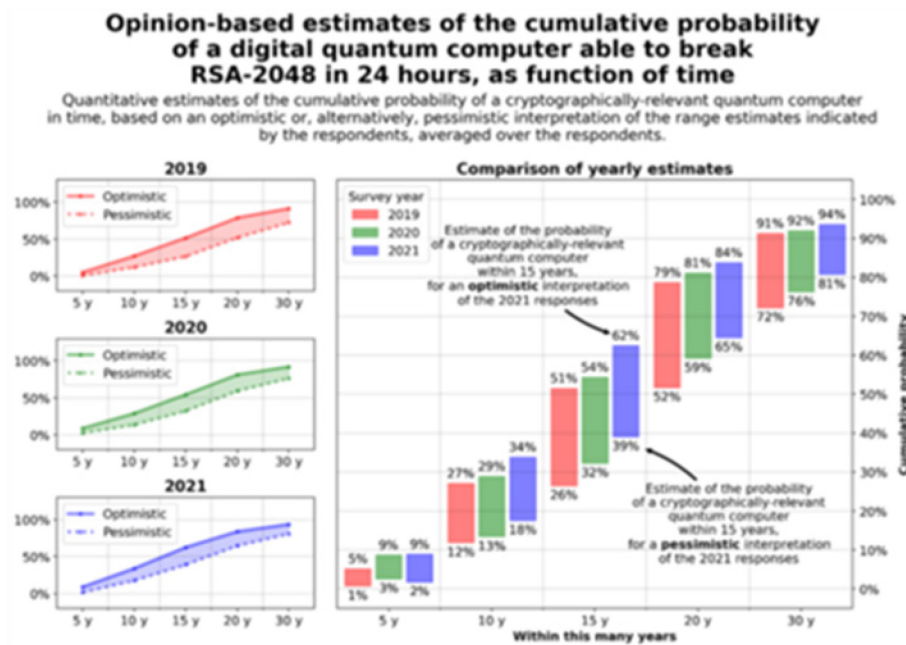


Figure 1 Estimates Breaking RSA-2048

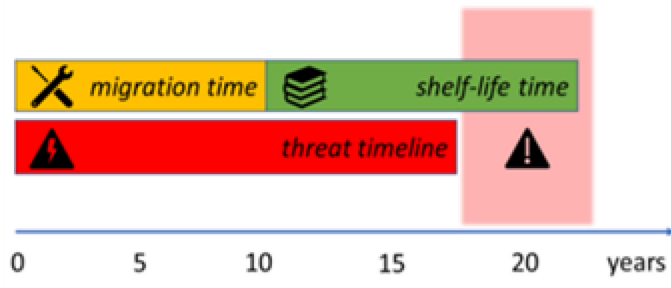
As shown for 2021, the opinion that a cryptographically relevant quantum computer will be available within 15 years was 39% for the pessimists and 62% for the optimists. The pessimistic view increased from 26% in 2019 to 32% in 2020 and 39% in 2021. Similarly, the optimistic view increased from 51% in 2019 to 54% in 2020 and 62% in 2021.

Many Opinions Agree

Even though the risk might not materialize before a decade, it is important to start preparing now.

Academic and technology experts, as well as governmental bodies, advise to start now on a multi-year process of migrating vulnerable computer systems to quantum-resistant cryptography such as with the [National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems](#).

According to Mosca’s theorem⁹ (Figure 2 Mosca Equation), “the urgency to initiate and complete the transition to quantum-safe cryptography depends on individual organizations’ risk attitude and can be evaluated in terms of three simple parameters:



1. shelf-life time: the number of years the data must remain protected,
2. migration time: the number of years needed to safely migrate an organization’s system,
3. threat actors can potentially access cryptographically relevant quantum computers.

Figure 2 Mosca Equation

Defining the Threat

The main concern of cryptographic vulnerability today is public key cryptography (based on asymmetric algorithms such as RSA or Elliptic Curve), which is used to securely exchange data encryption keys. These vulnerabilities mean that the public key cryptosystems that are currently being used are not appropriate to secure data requiring long-term security. An adversary could record encrypted data today and wait until one of these vulnerabilities materializes to decrypt the data.

When considering the specific threat to cryptographic systems, the problem can be broken into a simple diagram that illustrates the threat to public key and symmetric encryption systems. Figure 3 PQC Threat delineates the overall view of the security threat, beginning with asymmetric cryptography at top, and working down through various protocols. Note

that symmetric cryptography and hash algorithms are shown at the bottom of the “threat stack” for completeness.

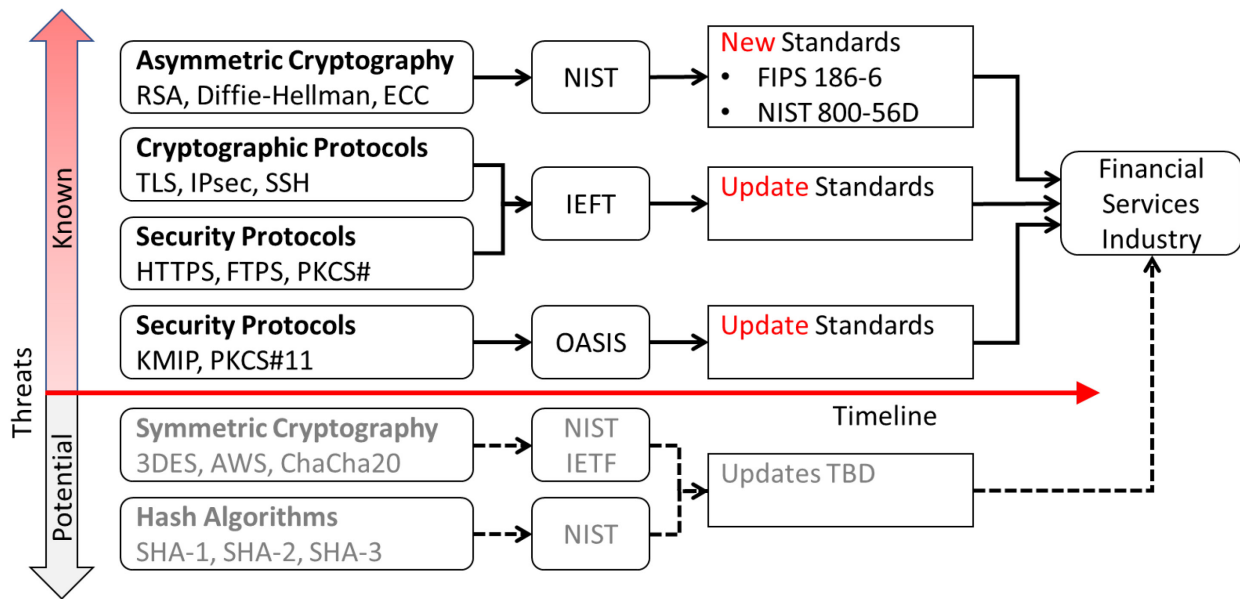


Figure 3 PQC Threat

At the top of the threat stack is asymmetric cryptography. Quantum computers will enable Shor’s Algorithm for factoring RSA public keys and determining discrete logs, breaking Diffie-Hellman, and its Elliptic Curve alternative (ECDH) public keys. Further, RSA digital signatures and both DSA and its Elliptic Curve alternative (ECDSA) are also threatened. Thus, all legacy asymmetric cryptography used for digital signatures, data encryption, or key management, is at risk. The NIST PQC program is developing the next generation asymmetric cryptography and will publish new standards.

Next in the threat stack are various cryptographic protocols that rely on asymmetric cryptography, including TLS, IPsec, and SSH. These protocols will need to be updated to first support PQC algorithms and eventually deprecate legacy asymmetric algorithms. Most of these protocols are managed by the Internet Engineering Task Force (IETF).

Below the cryptographic protocol but above the timeline are other security protocols, including HTTPS, FTPS, KMIP, PKCS#11 and others including PKCS#12, PKCS#10, PKCS#8, and PKCS#5. These protocols will need to be updated to first support the revised cryptographic protocols and eventually deprecate legacy asymmetric algorithms. Some of the security protocols are managed by the IETF but others by OASIS.

Below the timeline are symmetric cryptography and hash algorithms, currently not in scope of the NIST PQC program, but certainly a future concern. Note that there are other application cryptography concerns not listed here. For example, the ANSI standard X9.24-2 defines Remote Key Load (RKL) for use with ATM and POS terminals. RSA is used for key transport and digital signature to install the ATM symmetric keys: the PIN encryption key (PEK) and the key encryption key (KEK). As another example, many applications use Transparent Data Encryption (TDE) for Database Encryption (DBE), and some systems use RSA to manage the symmetric KEK for the symmetric database encryption keys.

Data Protection

Data Protection can be categorized into three areas: data-in-motion, data-at-rest, and data-in-use (though the latter is less commonly discussed). Each of these areas share commonalities, so it's easy to conflate the issues, but they also have differences, which makes it valuable to discuss separately.

Data-in-Motion

Data-in-Motion (DIM) is usually accomplished using a security protocol, such as TLS or IPsec, and typically has two steps: key management and data protection. Key management is the first step, an automated process using asymmetric cryptography to establish session keys. Data protection is the second step, another automated process using symmetric cryptography to encrypt data and provide data integrity. The session keys in the second step are dynamically generated during the key management in the first step. The asymmetric keys in the first step might be static, dynamic, or a combination of both. If the asymmetric keys are too weak or the key management process is vulnerable to attack, the session keys are likewise vulnerable and therefore the data is vulnerable.

In a PQC world, the legacy asymmetric algorithms: namely RSA, Diffie-Helman, and Elliptic Curve Cryptography (ECC), will be extremely vulnerable, making the keys too weak to use. Today, determining the asymmetric private keys from their asymmetric public key counterpart is infeasible with classical computers. We know how to do it, but computational resources are extreme and impractical. We also know that sometime soon, running Shor's Algorithm on reliable quantum computer will crack these keys. Making the keys bigger only takes a larger quantum computer but making them bigger needs so much resource on classical computers that the cryptography becomes unusable. Thus, we need newer asymmetric algorithms that are post-quantum computer resistant.

Data-at-Rest

Data-at-Rest (DAR) solutions also need the first and second step but most solutions separate the steps. Key management is typically done using manual setup procedures, although sometimes there are automated bits, too. The data encryption keys for the second step are generated and installed in the first step, but once allocated the data encryption keys rarely change unless another key change is manually performed. The data encryption keys are static and have a relatively long lifecycle. For example, changing an encryption key for a multi-terabyte database is not a trivial task. Further, there are usually only data encryption keys without data integrity, as integrity is part of database technology.

In a PQC world, since asymmetric keys are rarely used to manage symmetric keys, there is limited impact. However, there are some file storage systems that use a system-level RSA key to protect the symmetric key so the system can be rebooted, and the symmetric key can be recovered.

Data-in-Use

Data-in-Use (DIU) refers to information being cached or processed within system memory, understanding that when the system gets rebooted the memory content is wiped clean and everything starts over. Typically, data in memory is kept as cleartext per the assumption that an attacker needs to circumvent many system controls before memory can be accessed, However, this notion has been challenged and there is research on how to protect data while sitting idle in memory.

One such approach is homomorphic encryption. With partial or fully homomorphic encryption (FHE), some operations can be performed on the ciphertext such that when decrypted the change is reflected in the plaintext. This is being considered not only for data in memory but also for cloud services. Some homomorphic encryption is based on RSA and so would be vulnerable to quantum computers. Other variations of homomorphic encryption are based on AES and so would be resistant to quantum computers. There is also active research on adapting PQC algorithms for homomorphic encryption. While there are some homomorphic encryption products available, homomorphic encryption is not standardized by NIST but continues to be an interesting area of research.

Harvest Now, Decrypt Later

While the quantum computers that pose a credible threat are still years away, the threat of “Harvest now and decrypt later attacks” make this an immediate real security risk that needs to be addressed today. This is a long game attack¹⁰ where bad actors scrape/collect/harvest encrypted data, by the way of breaches or undertake passive interception and hoard the encrypted data, waiting for the day when quantum computers can decrypt it. Therefore, it is imperative to start using quantum resistant algorithms as soon as possible.

A bad actor can record, and store (harvest) encrypted data that is streaming through the internet or cloud today. The bad actor could be storing data to or from a specific website, server, email client, or whatever target they deem worthy of attack. With enough resources, a bad actor could capture petabytes of data (or more) from general Internet traffic. Bad actors can be ‘Nation-States’, internet service providers (ISP) harvesting on a limited basis, or even vendors with backdoors to harvest encrypted data.

The threat stems from the fact that quantum computers will be able to break the asymmetric encryption, disclosing the private keys (when given the public key), thus giving the bad actor unfettered access to the previously ‘encrypted’ data. With advancement in artificial intelligence and machine learning and with the exponential rise of data processing compute power, it would be relatively easy to extract meaningful information from the stored petabytes of data once the keys are broken. This attack is also known as “Data Vaulting”¹¹.

Data Management

Financial companies today have massive amounts of customer data and trillions of transaction data stored in various databases. In addition, millions of transactions are happening daily. The security shelf life of a piece of data is very much driven by business, risk, legal, regulatory, and contractual requirements. Customer data might include personally identifiable information (PII) or protected health information (PHI).

- **Business** requirements are the operational needs to meet customer expectations.
- **Risk** requirements are the practical limits for protecting customer information. And third-party service providers.
- **Legal** requirements are the restrictions imposed by law: e.g., GLBA^[1], CCPA^[4]
- **Regulatory** requirements are the guidelines imposed by the applicable Federal Financial Institutions Examination Council¹² (FFIEC) members: Board of Governors of the Federal Reserve System¹³ (FRB), the Federal Deposit Insurance Corporation¹⁴ (FDIC), the National Credit Union Administration¹⁵ (NCUA), the Office of the Comptroller of the Currency¹⁶ (OCC), and the Consumer Financial Protection Bureau¹⁷ (CFPB), the State Liaison Committee¹⁸ (SLC). The SLC includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS).
- **Contractual** requirements are those per binding agreements: e.g., PCI SSC¹⁹

These risks are amplified by the data retention requirements (e.g., security shelf-life) mandated by government agencies, such as the U.S. Federal Deposit Insurance Corporation (FDIC). Example data retention requirements for various classes of data records are listed in the FDIC's Records Retention Schedule shown below in Table 1.

Table 1. FDIC's Records Retention Schedule

Tax Info	7 years
Mortgage	30 Years
Auto loan	6 years
Equal Credit Opportunity Act	25 months
Truth in Lending Act	2 years
Bank Secrecy Act	5 years
FDIC Activities	Permanent
Personnel Management (PER4100)	56 years
Non-Judicial Matters (LAW1330) (incl. Loans, Foreclosure, ...)	Close of Matter + 10 years
Judicial Matters (LAW1400) (incl. Loans, Foreclosure, ...)	Close of Matter / Entry of Criminal Restitution + 20 years

Where are the Crypto Assets?

When defining and addressing the problem of discovering and inventorying cryptographic assets, it's important to first answer the question "what is a crypto asset?"

In this context, a crypto asset is the "envelope" of Information about a data protection mechanism and the corresponding cryptography and key management methods. Descriptive information is sometimes called "metadata" in the technology industry.

In this description of crypto asset, none of the actual application data or actual cryptographic keys are included. The crypto asset (metadata) is information about the data and keys, not the actual value of the data or keys.

Including the actual keys (and/or actual application data) would not provide additional value to the discovery effort and would represent a significant security risk, increasing opportunities for bad actors to compromise the keys and/or critical data.

The Inventory Problem

Building a clear inventory of cryptographic assets is a critical first step for organizations to carefully navigate strategic and unforeseen challenges in making that organization crypto-agile and planning for future changes in cryptographic requirements. Principles for the crypto asset inventory include the following:

- Determine - What (have we got?), Where (is it?), When (was it created?), Who (owns it?), Why (are we doing it?) How (is it being used?)
- Determine what is in an organization's control and should be inventoried and reported against.
- Determine what is outside an organization's control and should be documented where vendors are asked to provide a risk statement, an approach for risk remediation, and roadmaps as to when changes happen that will increase agility and mitigate risk.
- Standardize business process and deployment methods to simplify both the ability to create inventories and to support cryptographic agility.
- The inventory must be comprehensive and reflect all components for which an organization is solely responsible.

Creating a Full Inventory

Inventories can exist in many places and for different reasons. Usually, inventories catalogue discreet items like hardware devices, collections of data, service offerings and so on. There will often be multiple inventories with each inventory designed and built to meet a specific requirement at a point in time. However, the challenge of creating a cryptography inventory is that it applies across multiple different aspects of the enterprise, e.g., in applications or technology platforms. In that it is very much a cross-disciplinary effort; therefore, a single inventory is unlikely to give a full picture.

On top of this, determining the use of cryptography or persistent keys requires a level of knowledge of the different components involved to find and capture the right information. Figure 4 below is an example of what a holistic inventory may look like.

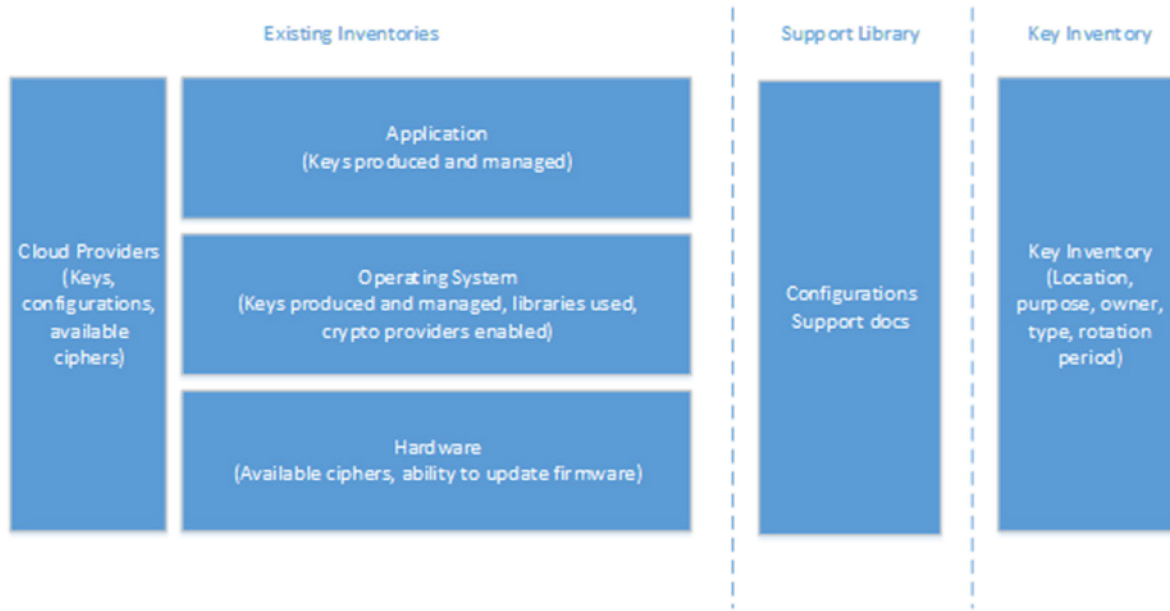


Figure 4: An example holistic inventory

How Do We Get There?

It is not a simple prescriptive set of steps that will get organizations to quantum resiliency. Rather, it's a journey of continuous crypto agility improvement and optimization that needs to be weaved into the organization strategic planning. Here are some tips to help organizations embark on the journey:

- Examine existing inventories and the data elements captured. Can they be expanded to better address cryptographic usage and cryptographic agility?
- Examine tooling used to capture data. Do they provide the necessary visibility into cryptographic to understand its runtime usage? Scanning tools are not a panacea in building an inventory in that a scanner is only as good as the access it has and specifics of what it is looking for.
- Look for Blind Spots - it is crucial to understand potential blind spots scanning tools may have. There may be offline keys, keys in file structures inaccessible to network scanners or keys of unknown format. Where blind spots exist, it may be required to find alternative methods to scan or work on the assumption of keys being present but accept the inability to validate those keys.

- Determine the frequency of scans - frequency should be relevant to the environment being scanned, with more frequent scans for higher change activity or higher risk areas, lower frequency scans for lower risk or areas using keys with longer life.
- Develop or refine an existing process for exception handling and for handling alerts triggered through monitoring (e.g., algorithm deprecated, key expiring).
- Ensure the organization has a well-managed and up-to-date inventory of software libraries used across all development projects.
- Develop and deliver awareness and training to the organization's development teams that address the need for, and provide approaches to, cryptographic agility in the development process and decisions by the project.
- Ensure the organization has a well-managed and up-to-date inventory of vendors and a view into their cryptographic usage, agility, and current posture. Include steps in the procurement process to capture this type of data along with clauses in the legal agreements (where possible) to better ensure cryptographic agility.
- Use the inventories to understand the environment and cryptographic usage. Consider developing a cryptographic agility index (CAI) that can be used to understand your organization's level of preparedness for PQC threat, and to plan to transition to quantum safe algorithm and prioritize work.

Self Identification

Self identification is the simplest method, and it can provide a starting point. Organizations likely have an application inventory today where the inventory identifies characteristics of the application such as data classification, whether the application handles customer personal identifiable information (PII) data, whether it supports financial transactions, etc. Some of the existing fields may provide insight into whether the application may use encryption based on the firm's data protection policies. Here, organizations may want to add a field and require application owners to explicitly record whether the application uses encryption, the type of encryption and a brief description as to its usage, e.g., to protect personal data stored in the application database using AES-128, to digitally sign transactions. This data can then be correlated with data collected via other methods and used to identify key risks to the firm posed by weak or deprecated cryptographic algorithms and to prioritize remediation efforts.

Scanning to Populate an Inventory

Conventional scanning tools can be used to discover, create, and maintain an inventory. Scanning, however, is not a panacea in that any scanner is only as good as the access it has and the specifics of what it is looking for. It's important to consider that many scanning tools:

- passively monitor real-time transactions between systems,
- actively interact with systems,
- search configuration files to gather information,
- search key stores to gather information, and
- use agent software to gather information.

However, not every piece of hardware or software can be scanned, searched, or probed. Proprietary or other non-standards implementations can adversely affect or render some scanning tools ineffective.

Documenting the Known

Discovering and documenting the current cryptographic environment usually begins with scanning tools that collect information and typically provide some type of reporting; these tools are often complimented by various hardware and software products that generate usage and/or access logs (e.g., SNMP) that can also be fed into a log management system to supplement the scanning tools.

In addition to logs and scans, many organizations regularly perform internal and external vulnerability scans on production systems and execute penetration testing on quasi production systems. For example, PCI DSS^[7] requires regular vulnerability scans and manages its own Approved Scanning Vendors²⁰ (ASV) program. PCI further recommends Pen Testing per its Penetration Testing Guidance^[8].

The ANSI standard X9.111 Penetration Testing within the Financial Services Industry^[9] specifies recommended processes for conducting penetration testing with financial service organizations, describes a framework for specifying, describing, and conducting penetration testing, and then relating the results of the penetration testing.

Documenting the Unknown

Where a device, piece of software, or application uses cryptographic methods that are not visible or configurable by an administrator, those must be treated as black boxes. A simple documented model of an inventory item would allow detail to be captured without trying to understand every library, key, and internal process.

A library of assets relating to each of these items would provide a reference to understand the wider cryptographic landscapes.

In the event of changes to the cryptographic landscape or related regulations, it would be up to the vendors supporting these items to make the relevant changes and for those changes to be tracked across an organization.

Where a third-party is providing a service, an organization's inventory should reflect only that which they are responsible for or can administer. Other inaccessible keys or cryptographic capabilities should be treated as a black box.

Based on the analysis, which existing cryptographic algorithms are at risk, the next important step is to understand which quantum computer safe alternatives will be available.

Application Development

Applications often use cryptography to accomplish specific tasks including the protection of sensitive data, signing and/or verifying the authenticity of transactions or documents, etc. These tasks rely on specific algorithms, cryptographic libraries, keys, modes of operation, protocol versions, certificates, etc. This is important information that should be collecting and adding to the firm's cryptographic inventory.

Several methods can be used to collect and maintain this type of data. These methods include self-identification by the application owner where the use of cryptography is explicitly recorded in the firm's application inventory, manual code review, static code scanning, dynamic execution, and file system discovery. In addition, the introduction of Software Bill of Materials (SBOM), although in its early days, may provide a view into the

use of cryptography in third-party products. Each of these methods is discussed in the subsections below.

Manual Code Review

Manual code review may be useful for top-tier applications handling highly sensitive data. Note however, that it is unlikely that this method will scale and additional methods that leverage automated tools to address the discovery problem should be adopted to establish and maintain a comprehensive and useful inventory.

Software Bill of Materials

A Software Bill of Materials (SBOM) is a formal, machine readable inventory of software components and dependencies and the information about those components and their hierarchical relationships. These inventories should be comprehensive or should explicitly state where they could not be.

SBOMs should include baseline attributes with the ability to uniquely identify individual components in a standard data format. The most efficient generation of SBOMs is as a byproduct of Continuous Delivery or secure development operations (SECDevOps) process.

Baseline Component Information

The primary purpose of an SBOM is to identify components and their relationships uniquely and unambiguously to one another. To do so, some combination of baseline component information is required. These baseline components support many use cases, but not all. Additional attributes may be required to support advanced use cases. The following table provides a list of baseline components typically included in SBOM inventory, as well as proposed baseline component information for recording inventory of data protection assets.

Baseline Information	Inventory Information
Author Name	Owner
Supplier Name	Generated inside which module
Component Name	
Version string	Validity dates
Component Hash	Fingerprint [where possible]
Unique Identifier	Human readable alias
Relationship	Primary Key and Foreign key relationships (example)

The following are three examples of SBOM formats and specifications.

Format	Specification	Tools
SPDX	https://spdx.github.io/spdx-spec/	https://tiny.cc/SPDX
CycloneDX	https://cyclonedx.org	https://tiny.cc/CycloneDX
SWID	ISO/IEC 19770-2:2015	https://tiny.cc/SWID

For more resources about SBOM, see <http://www.ntia.gov/sbom>.

Other Inventory Considerations

The following questions may be very useful when developing an inventory of data protection assets and its security.

1. Does the organization have inventory of all instances of non-console administrative access?
2. Does every instance of the non-console administrative access utilize cryptographic mechanisms to protect the confidentiality and integrity of the data being transmitted?
3. Do all mobile devices containing sensitive data utilize a cryptographic mechanism to prevent the unauthorized disclosure of information at rest and in transit?
4. Do all databases containing sensitive data utilize a cryptographic mechanism to prevent the unauthorized disclosure of information in the database?
5. Do all network communications containing sensitive data utilize a cryptographic mechanism to prevent the unauthorized disclosure of information while in transit?
6. Is wireless access protected via secure authentication and encryption?
7. Are systems / applications / services that include cryptographic mechanisms controlled to ensure the exporting of cryptographic technologies and in compliance with relevant statutory and regulatory requirements?
8. Do systems / applications / services that store, process, or transmit sensitive data utilize cryptographic mechanisms to prevent unauthorized disclosure of information as an alternate to physical safeguards?
9. Does a dedicated PKI infrastructure team, or similar function, implement and maintain an internal Public Key Infrastructure (PKI) infrastructure or does it obtain PKI services from an industry-reputable PKI service provider?
10. Does the PKI management function facilitate the implementation of cryptographic key management controls to protect the confidentiality, integrity, and availability of keys?
11. Does an IT infrastructure team, or similar function, facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS) or their Internal organization standards compliant key management technology?
12. Does an IT infrastructure team, or similar function, facilitate the production and management of asymmetric cryptographic keys using Federal Information Processing Standards (FIPS) or NIST 800-53 or NIST 800-57 or their Internal

- organization standards compliant key management technology such that private key never leaves a secure boundary?
13. How does the PKI infrastructure ensure or provide assurances of the availability of information in the event of the loss of cryptographic keys by individual users? How frequently are the entitlements and existing architecture reviewed?
 14. How does the PKI infrastructure facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes? Who is the owner of the shared-secret, keys, endpoints, and users?
 15. Is there a 1:1 mapping/binding of All cryptographic keys and secrets to individual identities?
 16. How does the SSH infrastructure ensure or provide assurances of the availability of information in the event of the loss of cryptographic keys by individual users? How frequently are the entitlements and existing architecture reviewed?
 17. How does the SSH infrastructure facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes? Who would be owner of the shared-secret, keys, endpoints, and users?
 18. Can all the secrets related use cases be automated and managed via a privileged access control model from a central secrets Manager with essential audit and reporting capabilities?

For additional information, refer to the [FS-ISAC PQC Infrastructure Inventory paper](#).

Risk Assessment

Once a crypto asset inventory is created, an effective risk management exercise can be deployed to help assess and prioritize subsequent remediation efforts for an organization to become quantum resilient. The following sections provide some information of several standard risk management frameworks.

PQC Risk Assessment Frameworks

There are two well-known PQC risk assessment frameworks currently available: Dr. Michele Mosca's Quantum Risk Assessment (QRA) and the Crypto Risk Assessment Framework (CARAF). Mosca's QRA uses a time-based approach to define risk, dependent

on when the process of migration to a quantum-safe state begins and considers “harvest now decrypt later” attacks. CARAF builds on Mosca’s QRA but focuses on “crypto agility” – the ability to quickly swap out vulnerable primitives, algorithms, and protocols for ones which are safer – and seeks to define organizational policies for specific asset groups. In addition, the FS-ISAC PQC workgroup has developed its own risk assessment framework, based on a patented²¹ risk modeling algorithm developed by Wells Fargo. The following section provides additional information about each of these frameworks.

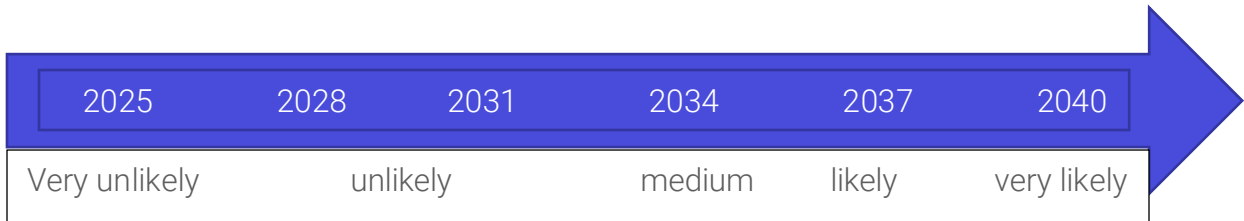
Summary of Mosca’s Quantum Risk Assessment

Dr. Michele Mosca, a major contributor to the theory and practice of quantum information processing and quantum readiness, formulated a strategy for organizations to evaluate their risk and take proactive steps to becoming quantum resilient. The risk assessment framework focuses on the timeline to migrate to a quantum safe state long before quantum computing is available to avoid “harvest now decrypt later” type attacks.

The methodology used in Mosca’s QRA is adapted from the six stages for conducting a risk assessment in the NIST Cybersecurity Framework, identified in ID.RA. Mosca’s QRA is intended to supplement or be performed after a regular risk assessment. The stages are as follows:

Phase 1 Identify and document valuable information assets, the degree to which they are protected by encryption, and the types of encryption used.

Phase 2 Research the state of emerging quantum computers and quantum-safe cryptography. As it is a challenge to create a realistic estimate for when quantum computers will emerge, the guidance for this step is to create a Quantum Risk Timeline for the probable emergence of a scalable quantum computer based on the current state of quantum technologies.



Phase 3 Identify threat actors and estimate their time to access quantum technology. This value is recommended to be at least 2 years. When combined with the results of Phase 2, an estimated Quantum Risk Timeline “z” can be determined. The Quantum Risk Timeline can be graphically represented, for example:

Phase 4 Identify the lifetime of your assets “x” and evaluate the potential business impacts should the assets become vulnerable within the timeframe “z” identified in Phase 3. Determine also the time required to transform the organization’s technical infrastructure to a quantum-safe state “y”.

Phase 5 Based on the variables defined in the previous phases, determine quantum risk with respect to a system by calculating “x + y > z”, i.e., whether business assets will become vulnerable before the organization can move to protect them. Since “z” was defined as a timeline with associated probabilities, the calculation in this phase produces a new timeline of the probability of quantum risk to the organization:

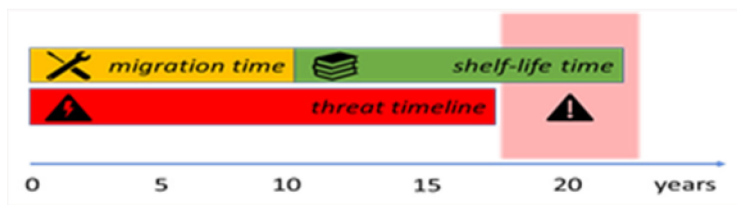


This timeline indicates the level of risk dependent on when the initiative to migrate to a quantum-safe state begins. It is important to note here that there are many assumptions made when calculating “x”, “y”, and “z”.

Phase 6 Identify and prioritize the activities required to maintain awareness, and to migrate the organization’s technology to a quantum-safe state.

This type of assessment provides evidence that quantum threats are emerging sooner than expected. The result can be stated, "if the assumptions made in the analysis hold true, then the system will face significant quantum risk unless it begins migrating to a quantum safe state by the year 20XX".

Summary of Mosca's Theorem



If a large-scale quantum computer (z) is built before the infrastructure has been re-tooled to be quantum-safe and the required duration of information-security has passed ($x+y$), then the encrypted information will not be secure, leaving it vulnerable to adversarial attack.

x : Security Shelf life. "How many years we need our encryption to be secure."

y : Migration time. "How many years it will take us to make our IT infrastructure quantum-safe."

z : Collapse Time. "How many years before a large-scale quantum computer will be built."

Summary of the CARAF Framework

Crypto agility refers to the ability of an entity to replace existing crypto primitives, algorithms, or protocols with a new alternative quickly, inexpensively, with no or acceptable risk exposure. Transition from one crypto solution to another can then take a long time and expose organizations to unnecessary security risk. Therefore, the [CARAF framework](#) was created to analyze and evaluate the risk that results from the lack of crypto agility and can be used by organizations to determine an appropriate mitigation strategy commensurate with their risk tolerance. The framework is comprised of 5 phases and below is a summary of each of them.

Phase 1: Identify Threats

To identify potential threats vectors that will affect assets subject to crypto agility risks. For example, a large quantum computer will impact public key crypto algorithms more severely than symmetric key algorithms. It may be adequate to just double the key size for symmetric key algorithms, but public key algorithms will need to be replaced with quantum-safe alternatives, which will necessitate a greater change management effort.

Phase 2: Inventory of Assets

To inventory a list of impacted assets. Assets can then be categorized and prioritized according to the nature of the assets and the expected security risk exposure. The framework suggests documenting the following factors:

- Scope
- Sensitivity
- Cryptography
- Secrets management
- Implementation
- Ownership
- Location
- Lifecycle management

Phase 3: Risk Estimation

Inventory will need to be prioritized for risk mitigation based on exposure. The framework suggests a new approach to risk prioritization as opposed to the well-known Risk = Impact x Probability estimation. The framework leverages the “timeline to exposure” variable from Mosca’s Model by including its information from Phase 1 and 2. The three components (shelf-life, mitigation, and threat) get a score between 1 and 4 (low risk, medium risk, high risk, critical). Additionally, cost is also used to estimate the risk and will vary depending on the type of assets and availability of resources for each organization.

Phase 4: Secure Assets Through Risk Mitigation

The framework suggests three options for risk mitigation:

1. Secure the asset by spending resources.
 - a. This may be rational when the value of an asset is greater than the cost to secure it.
2. Accept the risk and maintain the status quo.
 - a. This is reasonable when the expected value of the risk is lower than the organization's risk tolerance.
3. Phase out impacted assets.
 - a. This option may apply if the value of the asset is lower than the expected risk, especially if the cost to secure is high.

Phase 5: Organizational Roadmap

To develop a tactical roadmap to address crypto agility (or the risks from a lack of). The framework suggests that organizations must have coherent crypto policy that supports and guides different teams in making decisions about their cryptography choices. It gives further recommendation stating that crypto policy should be updated to remove deprecated algorithms and incorporate any replacements, and that associated processes should be leveraged to push those requirements.

FS-ISAC PQC Risk Assessment Guidance

While Mosca's QRA and the CARAF provide useful approaches to assessing PQC risk, the FS-ISAC team believes that larger or more complex financial institutions may want to take a more comprehensive risk model approach that assesses information, devices, cryptography, and remediation across the network. The FS-ISAC team leveraged a model developed by Wells Fargo to provide complex or large institutions guidance on how to conduct a more thorough and comprehensive risk assessment.

The FS-ISAC PQC Risk Assessment Guidance includes five phases: Discovery, Risk Model, Defining Risk Tolerance, Prioritization, Outcome/Recommendations. It also includes supplemental information on how to assess vendor readiness.

Phase 1: Discovery

By undertaking a thorough investigation into their use of cryptography, an organization can understand the risks they face from a change to cryptographic landscape such as the threat posed by post-quantum cryptography and the threat it presents to current

cryptographic algorithms. This will allow organizations to plan for and risk model both strategic and unforeseen challenges that future changes in cryptographic requirements will present.

To complete an effective discovery exercise that will support an organizational risk model there are three main areas that should be considered:

1. Undertaking and maintain an inventory of their current cryptographic systems and algorithm usage.
2. Identifying the data being protected and the most sensitive and critical datasets within an organization.
3. Initial triage of the systems identified for transition based on the organisations risk appetite.

Data Identification and Classification

A critical aspect in the development of an effective risk model is understanding what data is being protected.

To understand the scope of protected data and develop a risk model to assess the impact on an organization the following items should be considered, captured, and maintained at a minimum:

- In-house applications and their use of cryptographic algorithm
- Vendor applications and their use of cryptographic algorithms
- Vendor Roadmaps to support Post-Quantum Cryptography
- How long does the data asset need to be protected?
- Inventorying the organizations most sensitive and critical datasets
- Inventory of critical and high availability systems
- Internal and external connections
- Is the asset at risk from a harvest now/decrypt later attack scenario?

What is at Risk?

Once the organization has identified the data being protected by which algorithms, the organization should identify where and for what purpose public key cryptography is being used and mark those systems as quantum vulnerable.

While symmetric key cryptography is not currently considered imminently at risk from post-quantum cryptography it is important to consider the algorithms in use and whether there is any need to consider migration to a new key type or a longer key length to maintain their strength and usability in a post-quantum world.

The following table provides some examples of algorithms that have been identified as potentially not safe in a PQC environment and which algorithms are being used to protect them.

Cryptographic Algorithm	Type	Purpose	PQC Approach
AES-256	Symmetric	Encryption / Confidentially	Larger Key Sizes
SHA-256, SHA-3	Hash	Hash Functions / Integrity	Larger Key Sizes
RSA	Asymmetric	Signatures / Key Establishment	NO LONGER SECURE
ECDSA, ECDH (Elliptic Curve Encryption)	Asymmetric	Signatures / Key Establishment	NO LONGER SECURE
DAS (Finite Field Encryption)	Asymmetric	Signatures / Key Establishment	NO LONGER SECURE

Table x: PQC Risks - Asymmetric cryptography is primarily at risk (Source: NIST 8105)

Initial Risk and Exposure Evaluation

To assist in developing a risk model some initial evaluation is required to feed the risk model and provide initial triage of system risk and the potential exposure. This may depend on the size of the organization and their usage of at-risk cryptographic algorithms. This initial triage should, at minimum, include the following considerations:

- Can the system be replaced or deprecated?
- Is the data being protected likely to be at risk in a post-quantum world?
- Are there opportunities to prepare or change systems up front to support crypto agility?

- Are there opportunities to rationalize systems?
- Are there any external drivers such as regulatory requirements to prioritize or migrate a system early than anticipated?

Potential Quick Wins


Completing this triage exercise may provide an organization with some quick wins in terms of how they manage their use of cryptographic algorithms and provide agility options in how applications interact with those algorithms. This may provide the opportunity to refine the inputs to the risk model or indeed remove a system from the scope of any risk modelling.

Phase 2: Risk Modeling

Assessing and quantifying cryptographic risks is a difficult task. The threat of cryptographic relevant quantum computers (CRQC) is significant, but the timeline for when this will happen is murky at best. Asking experts in the field is a flawed and insufficient approach for enterprises to use for planning the significant cryptographic transition. (If you ask 10 experts when a CRQC will be available, they will give 10 different answers).

Another concern is how we quantify the risk of a cryptographically relevant quantum computer when they don't yet exist. We don't yet know all the ways quantum computers present a risk. In this sense we can create many scenarios on how risky a quantum threat is to an asset with some of these scenarios being "more likely" than others. This has a lot of similarities with the evaluation of climate change risk. With climate change we also have a very complex, highly coupled system which is exposed to external forcing. We know there are risks, but we don't know how big the risks are nor when they will take effect.

Risk Scoring

FS-ISAC risk scoring follows the risk scoring in the CARAF model - where risks are defined as: $\text{risk} = \text{cost} * \text{timeline}$ 

This model considers five different data tables:

1. **Application:** Applications are data sources which carry some financial impact if compromised. Could be the data for a product, customer data, etc. Applications have an annual financial impact score and a shelf-life for how long that data is stored.
2. **Node:** Points in the network through which applications pass through. It could be a server, router, encryptor, firewall, etc. Calculations are done at the node model level. All node models have a cryptographic profile.
3. **Geospatial:** Contains data about the geospatial locations of nodes.
4. **Cryptography:** Details of the cryptography used by a node. Each cryptographic method has a series of possible remediations to become quantum resilient.
5. **Remediation:** Details of the remediation for the relevant current cryptography. Could be a PQC algorithm, larger key size, etc. Each remediation has an associated cost. This cost is the estimated implementation time in years.

Phase 3: Define Risk Tolerance

According to the Nation Institute for Science and Technology (NIST) Assessing Security and Privacy Controls in Information Systems and Organizations NIST Special Publication 800-53A Revision 5 Risk Tolerance is the level of risk or the degree of uncertainty that is acceptable to an organization.

Financial institutions should leverage their existing information security risk assessment programs to assess the risk and impact of cryptographic vulnerabilities caused by cryptographic relevant quantum computers (CRQC). Risk treatment (avoid, mitigate, or accept) should be applied based on the company's risk appetite and tolerance.

Phase 4: Prioritization

According to the Department of Homeland Security Post-Quantum Cryptography Roadmap: Prioritizing one system over another for cryptographic transition is highly dependent on organization functions, goals, and needs. To supplement prioritization efforts, organizations should consider the following factors when evaluating a quantum vulnerable system:

- Is the system a high value asset based on organizational requirements?

- What is the system protecting (e.g., key stores, passwords, root keys, signing keys, personally identifiable information, sensitive personally identifiable information)?
- What other systems does the system communicate with?
- To what extent does the system share information with federal entities?
- To what extent does the system share information with other entities outside of your organization?
- Does the system support a critical infrastructure sector?
- How long does the data need to be protected?

Using the discovery, risk model, and risk tolerance described in this paper will allow organizations to develop plans for transition once the post-quantum cryptographic standards are published.

Phase 5: Outcome

The risk assessment along with risk tolerance analysis will provide organizations with a clear understanding of their quantum risk based on a variety of potential estimates for the development of cryptographic relevant quantum computers (CRQC).

Assessing Vendor Readiness

Assessing third-party service providers PQC readiness may be a little premature at this time since industry standards have not been developed. Instead, companies should begin thinking about vendor PQC requirements, updating existing risk assessment processes, and updating legal/contract requirements. In addition, companies should focus on increasing awareness of PQC amongst vendors. This can be accomplished via information sharing platforms, third-party risk conferences, informational brochures, or on social media. The FS-ISAC Group developed the questions below based on the DHS PQC Roadmap to help institutions understand their vendor's PQC status. Questions for vendors:

- Are your Chief Information Officers engaged with standard developing organizations related to Post-Quantum Cryptography?
- Is your company inventorying your most sensitive and critical datasets that will need to be secured once quantum computing arrives?

- Is your company aware that data may be harvested today and decrypted once cryptographically relevant quantum computers are available?
- Is your company inventorying all the systems using cryptographic technologies to facilitate a smooth transition in the future?
- Is your company identifying data security standards that will require updating to reflect post-quantum requirements?
- Is your company identifying where and for what purpose public key cryptography is being used and tagging those systems as quantum vulnerable?
- Does your company have a way to prioritize systems for cryptographic transition that considers; asset value, key stores, communications, ties to other entities, critical infrastructure or how long the data must be protected?
- Does your company have a plan for system transitions upon publication of the new post-quantum cryptographic standards?

Solution Space

To prepare for the eventual advent of quantum computers, security professionals are discussing multiple families of post-quantum cryptography strategies. The National Institute of Standards and Technology (NIST) is leading a Post-Quantum Cryptography Standardization project to identify and test the best cryptography schemes. Currently, there are multiple candidate families, including Code-based, Lattice-based, and Hash-based schemes.

Each of these schemes is based on mathematical problems that are very hard to solve, not only for traditional computers, but also for quantum computers.

- **CODE-BASED:** Based on public-key encryption and the use of error-correcting codes to hide the contents of a message during transmission. Decoding this random linear code is computationally hard, depending on the code parameters. Code-based cryptography was originally invented in 1978 and has been intensively studied especially in recent years as the post-quantum secure properties of the algorithm became appreciated. Leda is a candidate algorithm in the 2nd round of the NIST Post-Quantum Cryptography Standardization project.
- **LATTICE-BASED:** Based on public-key encryption, the computationally hard problem for this cryptography is trying to find the shortest vector in a high-dimensional

lattice. Round5 is a candidate algorithm in the 2nd round of the NIST Post-Quantum Cryptography Standardization project.

- **HASH-BASED:** Hash functions are one-way functions that map bit strings of an arbitrary length to short, fixed-length strings called hash values. LMS (RFC 8554) is a hash-based signature scheme which is in the process of getting approved by NIST (SP 800-208).

How can organizations choose the right post-quantum solution today to thwart an eventual quantum cryptanalysis attack?

The two-part answer is:

1. Choose a solution that incorporates one or more of the post-quantum algorithm schemes.
2. Make sure the solution you choose is flexible enough to incorporate future post-quantum algorithms when/if they become available.

When considering how to address this risk it is important to look not only at the algorithms at risk, but also at the cryptographic functions achieved by those algorithms. For example, RSA can be used to encrypt as well as to sign, so to replace RSA both use cases need to be covered, not necessarily with the same algorithm. The next important step is to understand which quantum computer safe alternatives will be available.

Transitioning to PQC

The transition to PQC affects a broad landscape of systems, applications, and network appliances that use asymmetric cryptographic algorithms. Common security protocols such as TLS, IPsec, and SSH are in scope, as well as other proprietary protocols. Most security protocols use asymmetric cryptography with key management algorithms to establish symmetric session keys, and many security protocols use digital signatures for identity, authentication, and data integrity^{[6]22}.

Generally, transitioning asymmetric cryptography will have two fundamental guidelines:

- Key management algorithms such as RSA, Diffie Helman, and ECDH can be replaced by the Round 3 CRYSTALS KYBER algorithm.
- Digital signature algorithms such as RSA, DSA, and ECDSA can be replaced by one of the Round 3: CRYSTALS DILITHIUM, FALCON, or SPHINCS+ algorithms.

As the NIST program evolves, other digital signature and key management algorithms might be selected within the next few years. Further, as the quantum threat evolves, cryptanalysis methods other than Shor's Algorithm might be developed that compromise one or more of the PQC algorithms.

In addition, asymmetric key exchange/wrapping, as well as digital signature can be replaced in some cases with symmetric encryption and signatures.

Quantum Key Distribution (QKD)

Any discussion on PQC transition would be incomplete without mentioning key management alternatives such as Quantum Key Distribution (QKD)²³²⁴. QKD can also be used to replace asymmetric key exchange. The primary QKD use case is to protect data transmission.

QKD uses quantum mechanical principles to share photons across fiberoptic cabling between two parties (e.g., Alice and Bob) to establish a random shared secret key. While several QKD products are commercially available and in use today, the underlying technology still has some challenges, i.e., there are inherent limitations in using fiberoptic cabling due to energy loss that limit the effective distances that QKD can be deployed.

Effective QKD distances over fiber optic cables have been reported to be as far as a thousand kilometers (about 620 miles). Continued developments and improvements in quantum repeaters and quantum memory promise to extend these distance limitations to more practical levels. Eventually, QKD will enable parties to derive symmetric session keys without using modern asymmetric or PQC algorithms over thousands of miles.

Measuring Readiness

The definition of “ready” varies from one organization to another. From identifying and understanding the threats to implementing remediation, readiness is relative to the level of risk an organization is willing to accept.

There are multiple routes that the organization can follow to test whether their crypto capability is quantum resistant. These include testing crypto changes, third-party assessment, red teams, and keeping up to date of the threat through threat intelligence and incident response management. Moreover, a maturity model provides a way to consolidate the organization efforts to improve the effectiveness and reliability of the quantum-resistant crypto capability.

Testing/Attestation

A testing strategy is needed to ensure that the proposed solutions satisfy the use case requirements and that the implemented change provides the protection needed to mitigate the quantum crypto threat.

A test environment that is representative of the organization’s systems and configurations is essential. A good inventory of the current assets, the architecture and crypto configurations are also crucial for producing reliable test results.

Systems and interactions may span multiple organizational boundaries such as in the case of hosting service providers and SaaS providers. Dependencies on third-party systems must be identified and addressed via active testing (where allowed) and/or third-party assessment. An organization’s third-party assurance functions (e.g., questionnaires) are a good place to start embedding the quantum crypto safety queries.

Vendors offer PQC test kits to help organizations set up and test solution approaches. For instance, Hybrid TLS certificates testing toolkit uses a post-quantum cryptographic algorithm paired with a classical encryption algorithm, enabling organizations to test the viability of deploying post-quantum hybrid TLS certs while maintaining backwards compatibility. Testing results (vulnerabilities and incompatibilities) must be logged and tracked for remediation. This includes tracking third-party partners remediation plans to ensure that the risk to data is managed beyond the organizational boundary.

Degrees of Readiness

To help organizations on their journey of building quantum-safe crypto capability, a standard maturity model can be adapted to identify an organization's current state versus where they would like to be in the future. Note that maturity ratings are not a measurement of cyber risk mitigation.

While an organization may its own maturity models and definitions, the following sections present one approach to creating a maturity framework that captures how well the organization is doing in implementing and operating PQC capability. The following model is presented as a reference that can be embedded into the current maturity models. This will help ensure that progress on the crypto journey is assessed and tracked as part of an existing governance structure. Scores can be assigned to each level to form a quantitative representation of the organization's overall maturity level.

The model below is defined based on the CMMI maturity levels with five levels of maturity against dimensions of the PQC landscape. The levels are:

- Initial: No standards are in place and inconsistency exists across the organization.
- Managed: A process is planned and managed, often reactive within certain areas of the organization.
- Defined: A process is defined as a standard across the organization and is tailored for individual projects.
- Quantitatively Managed: The process is quantitatively measured and any deviation from the standard is addressed.
- Optimizing: The organization has a set of consistent processes that are constantly being improved and optimized.

	Inventory	Risk Modelling	Third-Party/CA or Internal Assessment	Change Program
Initial	Limited or non-existent coverage of certain areas of the estate.	Inconsistent or non-existent PQC risk model	Ad hoc or non-existent plan	
Managed	Coverage of the organization with known exceptions	Consistent risk model(s) applied across areas of the business	Included in third-party assessments for renewals/procurement Internal assessment	Ad hoc business unit projects
Defined	Coverage of known exceptions. Embedded processes for maintaining data records.	Consistent risk models used for assessing crypto risks with understanding of applicability across the financial use cases.	Pen testing and simulations Testing attestations	Programs
Quantitatively Managed		Consistent quantitative risk models used for assessing crypto risks feeding into and driving the crypto remediation process		Risk and impact led

Optimizing		Consistent risk models used for Assessing crypto risks and optimized based on the threat intelligence		
-------------------	--	---	--	--

Conclusion

Transitioning to different cryptographic algorithms or protocols is a complex undertaking and a clear understanding of the end state requirements is essential to proper planning.

Cryptographic environments are not static. Existing systems are upgraded, new systems are deployed, and old systems are decommissioned. Sometimes systems get out sourced to third-party service providers including migration to the cloud. The cryptographic architecture²⁵, including a complete cryptographic inventory, needs to be discovered, documented, and maintained throughout a transition. Knowing the current state is essential in successfully planning to get to a destination and track progress along the way²⁶.

References

- [1] [Gramm–Leach–Bliley Act, Public Law 106–102–Nov. 12 \(1999\)](#)
- [2] [Jeff Stapleton; Ralph Poore, *Cryptographic Transitions* \(2006\), IEEE Region 5 Conference](#)
- [3] [Bernstein, D. J., Biasse, J.-F., & Mosca, M. \(2017\). *A Low-Resource Quantum Factoring Algorithm*. Retrieved from Semantic Scholar](#)
- [4] [TITLE 1.81.5. California Consumer Privacy Act \(2018\) \[1798.100 - 1798.199.100\]](#)
- [5] [Bordow \(et al\). \(2019\). *Post-Quantum Cryptography and the Quantum Threat*](#)
- [6] [Jeff Stapleton; Ralph Poore, Peter Bordow, *Cryptographic Transitions: Historical Considerations* \(2022\), Volume 20 Issue 9](#)
- [7] [PCI Data Security Standard \(DSS\) v4.0 \(2022\) Requirements and Testing Procedures](#)
- [8] [PCI DSS Information Supplement: Penetration Testing Guidance \(2017\) v1.1](#)
- [9] [ANSI X9.111 \(2018\) Penetration Testing within the Financial Services Industry](#)

Alternate Format

1. [ANSI](#)
2. [ASC X9](#)
3. [ISO TC68](#)
4. [Feldman, S. \(2019\) 20 Years of Quantum Computing Growth](#)
5. [IBM \(2022\) Our New 2022 Development Roadmap](#)
6. [Gheorghiu, V. & Mosca, M. \(2021\) A Resource Estimation Framework for Quantum Attacks Against Cryptographic Functions - Recent Developments. GRI Quantum Risk Assessment Report Feb. 2021](#)
7. [Grassl, M. et al. \(2016\) Applying Grover's Algorithm to AES: Quantum Resource Estimates](#)
8. [Mosca, M. & Piani, M. \(2022\) 2021 Quantum Threat Timeline Report. Global Risk Institute](#)
9. [Mosca, M. \(2015\) Cybersecurity in a Quantum World: will we be ready?](#)
10. [Carter, G. \(2016, February 18\). Your Best Kept Secrets Aren't Really Secrets](#)
11. [CSA. \(2017\). Applied Quantum-Safe Security. Retrieved from Cloud Security Alliance](#)
12. [FFIEC](#)
13. [FRB](#)
14. [FDIC](#)
15. [NCUA](#)

16. [OCC](#)
17. [CFPB](#)
18. [SLC](#)
19. [PCI SSC](#)
20. [PCI AVS](#)
21. [NTIA](#)
22. [Jeff Stapleton; Ralph Poore, Peter Bordow, Cryptographic Transitions: Historical Considerations \(2022\), Volume 20 Issue 9](#)
23. Quantum cryptography: Public key distribution and coin tossing, C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, 1984
24. Quantum cryptography based on Bell's theorem, Ekert, Artur K., Physical Review Letters. 67 (6): 661–663, 1991
25. Cryptographic Architectures: Missing in Action, Jeff Stapleton, ISSA July 2017 Journal, Volume 15, Issue 7

If you are an FS-ISAC member and would like to join the PQC Working Group, please [email us](#).