FS-ISAC

Post-Quantum Cryptography (PQC) Working Group

Risk Model Technical Paper

TLP WHITE

PQC Working Group

Risk Model

Contents

Executive Summary

Quantum computers and algorithms will significantly impact the security of today's cryptographic systems. The National Institute of Standards and Technology (NIST) has led the initiative to create new cryptographic systems specifically made to withstand quantum attacks. These methods, also called post-quantum cryptography, are meant to maintain communication security even in the presence of quantum computers.

While it is challenging to foresee with precision the availability of quantum computers or the extent of their capabilities, it is anticipated that cryptographically relevant quantum computers that could break RSA 2048 encryption will be available in the next 10-30 years.

It is believed that some nation-states or criminal organizations may be collecting data to decrypt sensitive information once cryptographically relevant quantum computers (CRQCs) are available. With the potential of quantum cryptanalysis in the future, it may be possible for attackers to decrypt the information once CRQCs are available. This is also known as a "Harvest Now, Decrypt Later" attack.

By building a clear inventory of assets and uses of cryptography, an organization can proactively identify risks and challenges introduced by advances in quantum computing. Organizations should also incorporate quantum risks into existing risk assessment processes with the goal of understanding the likelihood and impact of any particular risk and to help prioritize them for remediation.

Organizations should use a risk model to evaluate the risk that quantum computing may pose to cybersecurity. Wells Fargo has developed a PQC (Post-Quantum Cryptography) risk model to measure the risk posed by cryptographically relevant quantum computers (CRQCs). Other frameworks, such as the Quantum Risk Assessment and the Crypto Agility Risk Management Framework (CARAF), are also good options for organizations.

Remediation will require companies to migrate to Post-Quantum Cryptography (PQC). Throughout this process, organizations should consider increasing their crypto agility. There are several migration strategy frameworks that companies can utilize to plan for their PQC migration. Companies will also need to work with their third-parties to ensure they implement post-quantum cryptography to safeguard against quantum computers.

Companies should prepare for the coming quantum revolution by understanding and assessing their PQC risk to ensure the security of classical computers in the face of these new technologies. This paper assists businesses in comprehending the current state of quantum computing, considering the potential impacts on security. It also assists them in preparing by offering data and resources to help assess the risk and understand how to prioritize remediation.

Quantum's Impact on Cybersecurity

The security of today's computers will be significantly impacted by quantum computers. Quantum computers, along with known quantum algorithms, could break many of the cryptographic systems in place today. That is because many of the encryption methods utilized today are based on the difficulty of finding prime factors in very large numbers, for example 2048-bit encryption. RSA, one of the most commonly used public key cryptosystem today utilizes a cryptographic method based on factoring prime numbers. Today's "classical computers" could take years if not decades to conduct the cryptanalysis required to break such encryption. However, quantum computers along with known algorithms, such as Shor's algorithm, will be able to decrypt encryption based on prime factoring in a matter of minutes.

Due to this risk, numerous initiatives are being made to create new cryptographic systems that are specifically made to withstand quantum attacks. These methods, also referred to as post-quantum or quantum-safe cryptography, are meant to maintain communication security even in the presence of quantum computers.

Quantum encryption, which uses quantum mechanics to secure communication in a manner fundamentally different from conventional encryption, is another way that quantum computers may have an impact on security.

In general, it is expected that the development and advancement of quantum computers will have a significant impact on the field of cybersecurity. It will be crucial for researchers and practitioners to keep up with the most recent advancements in order to ensure the security of classical computers in the face of these new technologies.

Status of Quantum Computing

Existing quantum computers have some limitations in terms of the size of the quantum systems they can implement and the kinds of problems they can address. However, it is anticipated that cryptographically relevant quantum computers that could break RSA 2048 encryption will be available in the next 10-30 years. Please refer to the 2022 Quantum Threat Timeline Report - Global Risk Institute[1] for additional information. As is evident throughout the report, it is challenging to foresee with precision the availability of quantum computers or the extent of their capabilities. The field of quantum computing is still undergoing research and development, and it is anticipated that significant advancements will be made over the next few years.

Status of Post-Quantum Cryptography

Since 2016, the National Institute of Standards and Technology (NIST) led an effort to identify and standardize post-quantum cryptography. Most recently, in July of 2022, NIST announced that it had selected several algorithms for standardization. It is expected that NIST will finalize the standards for the selected algorithms around 2024. Please refer to NIST's Post-Quantum Cryptography Standardization[2] website for current information. Additional information regarding the standardization process, requirements, evaluation criteria, and transition & migration is available NIST PQC FAQ[3].

Harvest Now, Decrypt Later Attacks

It is believed that some nation-states or criminal organizations may be collecting data to decrypt sensitive information once cryptographically relevant quantum computers (CRQCs) are available. These groups are likely to be interested in a range of technologies and capabilities that could potentially give them an advantage in terms of intelligence gathering, cyber operations, or financial gain.

The financial industry is a prime target for cyber attacks for financial gain, as it handles large amounts of sensitive financial data and is often seen as a lucrative target for attackers. These attacks often involve the use of malware to gain access to a company's systems and steal sensitive data. There have been several high-profile incidents in which the stolen data was encrypted, meaning that the hackers were unable to access or use the sensitive information. With the potential of quantum cryptanalysis in the future, it may be possible for attackers to decrypt the information once CRQCs are available. As such, organizations need to carefully consider the shelf life of information stolen during data breaches and should consider additional mitigating controls to ensure their customer's confidentiality and security.

Cryptographic Infrastructure and Data Inventory

The ability of an organization to understand its ability to react to changes in the cryptographic landscape requires knowledge of all uses of cryptography across its businesses. It is broader than just the encryption keys and algorithms and must also include the underlying technology and business processes that are being supported.

By building a clear inventory of assets and uses of cryptography, an organization can proactively identify risks and challenges being introduced by advances in PQC and allow the organization to be crypto-agile in planning for future changes in cryptographic requirements.

With an inventory of available cryptographic keys, it is important to understand the data being protected by those keys and who is responsible for the maintenance of those systems and applications. This information can then be used to develop and implement a risk model. To ensure the potential impact on an organization is adequately monitored, the following items should be considered, captured, and maintained at a minimum:

- Application Considerations
    - In-house applications and their use of cryptographic algorithms
    - Vendor applications and their use of cryptographic algorithms
    - Inventory of critical and high-availability applications
    - Inventory of internal and external application connections
- Third-Party Risk Management
    - Vendor roadmaps to support post-quantum cryptography
    - Procurement consideration to support post-quantum cryptograhpy
- Data Considerations
    - How long does the data asset need to be protected for
    - Inventorying the organization's most sensitive and critical datasets
    - Is the data at risk from a harvest now / decrypt later attack scenario
- Regulatory Considerations
    - Is the data under external regulation

- Data Residency/Location of Data – there may be different timelines associated with different regions

The FS-ISAC PQC Working Group published a paper on infrastructure inventory[4] that provides details on several methods that can be used to discover, create, and maintain inventories to accurately reflect cryptographic usage across the enterprise and business functions. Please refer to the paper for additional details.

Risk Assessments

An information security risk assessment is the outcome of identifying and evaluating risks to an organization's information assets. It includes identifying the assets, threats, vulnerabilities, and the potential impact of a security incident or data breach. The assessment's goal is to understand the likelihood and impact of any particular risk and help prioritize them for remediation. Information security risk assessments should be updated to specifically address the risks of quantum computing, similar to the following example:

1. Quantum computing attacks on cryptographic algorithms:
   - Description: This risk entails the possibility that quantum computers may one day break some cryptographic algorithms currently used to safeguard sensitive data.
   - Likelihood: Low (currently, as quantum computers are still in the early stages of development)
   - Impact: High (A quantum computer could potentially compromise sensitive data if it were able to defeat a cryptographic algorithm.)
   - Current controls: Monitoring the progress of quantum computing regularly and applying cryptographic algorithms that are thought to be resistant to quantum attacks
   - Additional controls: monitoring NIST's development of new post-quantum cryptographic algorithms

The risk assessment's outcome should include a comprehensive list of all risks, the controls in place to mitigate those risks, and any actions that are needed to further mitigate risks. This is sometimes called a risk register, and it is a comprehensive, well-organized list of every risk that has been identified, as well as any measures being taken to reduce or manage the risk. Risk assessments also identify higher-value and/or higher-risk assets that should be leveraged to prioritize quantum remediation.

Risk Modeling

Risk modeling is the process of identifying, analyzing, and evaluating potential risks in order to prioritize and mitigate them. It is a critical tool for businesses and organizations to manage risk and make informed decisions. To evaluate the risk that quantum computing may pose to cybersecurity, organizations should use a risk model that considers several factors, such as:

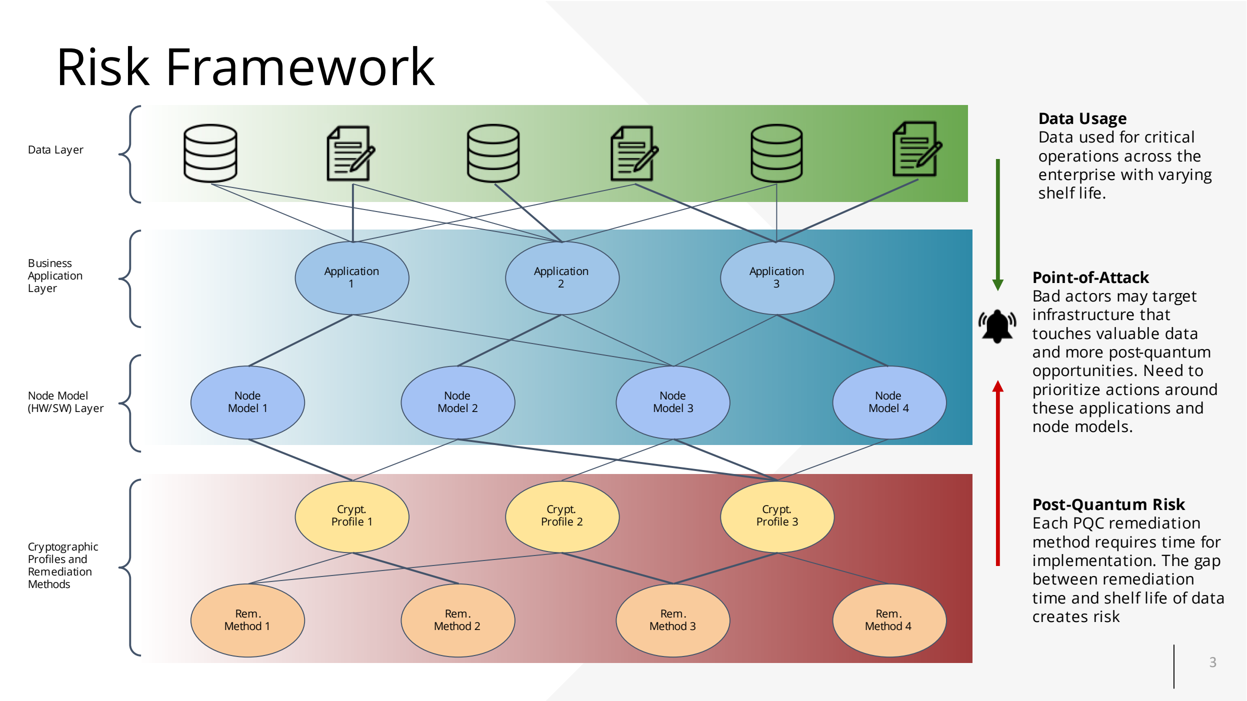
- The current and future capabilities of quantum computers: This may entail considering elements like the size of the currently accessible quantum systems, the kinds of issues that quantum computers can handle, and the anticipated pace of development in the quantum computing space.
- The vulnerabilities of current cryptographic systems: This may entail assessing the susceptibility of existing cryptographic systems to quantum attacks and determining whether those vulnerabilities are likely to be used in the near future.
- The importance of the information being protected: This may entail considering the importance of the data being protected, the potential repercussions of a breach, and the likelihood that one will occur.
- The potential costs and benefits of transitioning to post-quantum cryptography: This may entail weighing the advantages of increased security against the costs of switching to post-quantum cryptography, such as the costs of implementing new cryptographic systems and the potential disruption to existing systems.

Overall, risk models are designed to help organizations understand and manage risk by producing a range of outputs that can be used to inform risk management decisions.

Wells Fargo’s PQC Risk Model

Wells Fargo has developed a PQC risk model to measure the risk posed by cryptographically relevant quantum computers (CRQCs). The mathematical model is inspired by the methods used to capture the economic externalities of climate change. The risk management challenges posed by climate change and the potential deployment of CRQCs are similar in a few keyways. Both involve highly complex systems with many interconnected variables and significant uncertainty about the timing and magnitude of potential impacts.

The Wells Fargo PQC risk model involves identifying the risks associated with CRQCs by analyzing traffic across nodes within the network, the financial impact of data compromise, the cryptography utilized by those nodes, and the remediation or cost required to mitigate those nodes. This approach can provide a risk view across applications (data sources) and specific nodes. This approach can also help organizations better understand the potential risks posed by CRQCs and take proactive measures to protect against those risks. The diagram below depicts Wells Fargo's risk model framework.



Data Usage
Data used for critical operations across the enterprise with varying shelf life.

Point-of-Attack
Bad actors may target infrastructure that touches valuable data and more post-quantum opportunities. Need to prioritize actions around these applications and node models.

Post-Quantum Risk
Each PQC remediation method requires time for implementation. The gap between remediation time and shelf life of data creates risk

It's worth noting that the Wells Fargo PQC risk model (see Appendix A for more details) is just one example of how organizations can approach the risk management challenges posed by CRQCs. There are many other approaches and frameworks that organizations can use, depending on their specific needs and circumstances. Two other well-known PQC risk assessment frameworks are summarized later in this paper: Dr. Mosca's Quantum Risk Assessment (QRA) and the Crypto Agility Risk Assessment Framework (CARAF).

Risk Tolerance

Risk tolerance is the level of risk an organization is willing to accept. An organization should utilize the information gathered through risk modeling and risk assessments to fully identify and assess the risks created by quantum computers. This information should provide a view of all information assets, the vulnerabilities that exist, and the potential impacts of a security breach. Since risk tolerance will vary from organization to organization, each organization must set risk tolerance levels based on their own risk appetite. Companies should regularly review and update their risk tolerance as their goals, objectives, and the cyber threat landscape changes.

The NIST Cybersecurity Framework recommends that companies communicate their risk tolerance to key stakeholders on an ongoing basis to promote transparency and ensure informed decision-making. This will make it easier to ensure that everyone is aware of the company's strategy for managing cyber risk and the precautions that must be taken to safeguard its assets.

Remediation

Remediation will require companies to migrate to Post-quantum Cryptography (PQC) once it is available (see Status of Post-Quantum Cryptography above). Companies should begin by conducting an inventory, as discussed in the Infrastructure Inventory section above, and in the related FS-ISAC PQC Workgroup paper. Once the inventory of assets and cryptography is complete, companies should conduct a risk assessment or utilize a risk modeling tool as discussed in the Risk Modeling and Risk Assessment sections above. Organizations can better understand their risk profile and prioritize remediation by utilizing a risk model such as the Wells Fargo PQC Risk Model, Dr. Mosca’s Quantum Risk Assessment (QRA), or the Crypto Agility Risk Assessment Framework (CARAF), as discussed in this paper.

Throughout this process, organizations should consider increasing their crypto agility to keep up with the changes in cryptographic technologies and protocols that are going to consistently change and evolve due to quantum computers. Please refer to the crypto agility section below for additional details.

Organizations should utilize an existing quantum-safe mitigation strategy, framework, and informational source such as those listed in Table 9 of the ASC X9 Informative Report[5].

Companies will also need to work with their third-parties to ensure they implement post-quantum cryptography to safeguard against quantum computers. Please refer to the section below on third party PQC readiness for additional information.

Additionally, the Department of Homeland Security has published a Post-Quantum Cryptography Roadmap[6] which recommends utilizing 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)?
- With what other systems does this system communicate?
- To what extent does the system share information with federal entities?
- To what extent does the system share information with other entities outside your organization?
- Does the system support a critical infrastructure sector?
- How long does the data need to be protected?

Overall, companies need to prioritize quantum remediation to ensure the security of their systems and data in the face of the potential threat posed by quantum computers.

Crypto Agility

The term "crypto agility" describes an organization's or system's capacity to quickly adjust to modifications in the cryptographic technologies and protocols it employs. This is crucial to maintaining strong security and safeguarding against new threats. Implementing strong key management procedures, updating cryptographic protocols and technologies, and providing training and resources to ensure that staff members are knowledgeable about both established and new cryptographic technologies are just a few examples of the various activities that can go into achieving crypto agility. An organization can use a crypto agility framework as a set of rules and procedures to ensure that it can quickly adapt to cryptographic technologies and protocol changes.

The Crypto Agility Risk Assessment Framework (CARAF)[7] published in the Journal of Cybersecurity, is an excellent resource for companies to follow to understand and develop crypto agility. According to the framework, crypto agility refers to the ability of an entity to replace existing crypto primitives, algorithms, or protocols with a new alternative quickly, inexpensively, and with no or acceptable risk exposure. Transitioning from one crypto solution to another can take a long time and expose organizations to unnecessary security risks. Therefore, the framework was created to analyze and evaluate the risk resulting from the lack of crypto agility. It can be used by an organization to determine an appropriate mitigation strategy commensurate with their risk tolerance.

In addition to the CARAF Framework, companies should consider creating a cryptographic agility index (CAI) that takes a holistic view and reflects specific points about prioritization, controls, business capabilities, vendors, mitigation, and an implementation plan. The FS-ISAC infrastructure inventory paper describes such an agility index in Appendix A. Please refer to the infrastructure paper for additional details.

Overall, by ensuring that an organization can quickly adapt to changes in cryptographic technologies and protocols, a crypto agility framework can assist it in maintaining robust security while safeguarding against emerging threats.

Vendor Readiness

The following actions can be taken by a business to determine whether its third-party vendors are prepared for post-quantum cryptography:

- Identify important vendors: The first step is determining which important vendors the business uses and who deals with sensitive data. Vendors who provide software or other products that the business uses, as well as those who in some way handle the business's data, may fall under this category (e.g., hosting, storage, processing).
- Review the vendor's security policies:
- Reviewing each of the identified vendors' security procedures is the next step. Reviewing the vendor's cybersecurity policies and practices, and any pertinent security accreditations or certifications may be part of this activity. Inquiries should be made about the vendor's plans for dealing with potential risks associated with quantum computing, as well as whether any preparations for post-quantum cryptography have been made.

- Vendor readiness assessment: The business should evaluate the vendor's readiness for post-quantum cryptography based on a review of the vendor's security procedures. This might entail assessing the vendor's adoption of cryptographic algorithms that are thought to be immune to quantum attacks as well as the vendor's general cybersecurity strategy.
- Determine any gaps: The company should cooperate with its vendors to close any gaps in post-quantum cryptography readiness that are discovered. This may entail adding more security precautions, like using stronger access controls or different cryptographic algorithms.

The FS-ISAC PQC group created a list of potential vendor questions based on the DHS PQC Roadmap to help institutions understand their vendors' PQC status. Please refer to Appendix C.

The Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR) paper on BEST PRACTICES AND GUIDELINES v2.0[8] published in June 2022, also includes a series of questions to help an organization to begin assessing the PQC maturity or 'posture' of third-parties.

In general, it's critical that businesses keep abreast of the most recent quantum computing advancements and regularly review and gauge their third-party vendor's readiness for post-quantum cryptography. As a result, sensitive data will be better protected from risks associated with quantum computing.

Summary

Quantum computers will significantly impact the security of today's computers. Along with known quantum algorithms, quantum computers could break many of the cryptographic systems in place today. The National Institute of Standards and Technology (NIST) has been leading the initiative to create new cryptographic systems that are specifically made to withstand quantum attacks. These methods, also referred to as post-quantum cryptography, are meant to maintain communication security in the presence of quantum computers.

While it is challenging to predict with precision the availability of quantum computers or the extent of their capabilities, it is anticipated that cryptographically relevant quantum computers that could break RSA 2048 encryption will be available in the next 10-30 years.

It is believed that some nation-states or criminal organizations may be collecting data with the intention of using it to decrypt sensitive information once cryptographically relevant quantum computers (CRQCs) are available. With the potential of quantum cryptanalysis in the future, it may be possible for attackers to decrypt the information once CRQCs are available. This is also known as a “Harvest Now, Decrypt Later” attack.

By building a clear inventory of assets and uses of cryptography, an organization can proactively identify the risks and challenges introduced by advances in quantum computing. Organizations should also incorporate quantum risks into existing risk assessment processes with the goal of understanding the likelihood and impact of any particular risk and help prioritize them for remediation. Organizations should use a risk model to evaluate the risks that quantum computing may pose to cybersecurity.

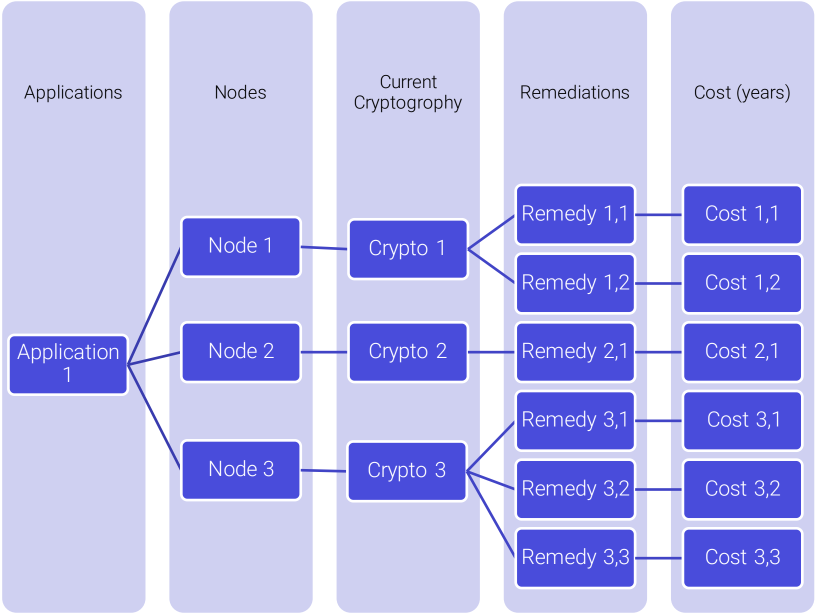
Remediation will require companies to migrate to Post-quantum Cryptography (PQC). Throughout this process, organizations should consider increasing their crypto agility. Companies can use several migration strategy frameworks to plan for their PQC migration. Companies will also need to work with their third parties to ensure they are implementing post-quantum cryptography to safeguard against quantum computers.

Companies should prepare for the coming quantum revolution by understanding and assessing their PQC risk to ensure the security of classical computers in the face of these new technologies. This paper assists businesses in comprehending the current state of quantum computing, considering the potential impacts on security. It assists them in preparing by offering data and resources to help assess the risk and understand how to prioritize remediation.

Appendix A: Wells Fargo’s PQC Risk Model

The Wells Fargo PQC risk model involves identifying the risks associated with CRQCs by analyzing traffic across nodes, like servers, routers, encryptors, or firewalls.) within the network, the financial impact of data compromise, the cryptography utilized by those nodes, and the remediation or cost required to mitigate the nodes. This approach can provide a risk view across applications (data sources) and specific nodes. This approach can also help organizations better understand the potential risks posed by CRQCs and take proactive measures to protect against those risks.

By utilizing a model, an organization can determine the cost of remediation for any particular application and the potential impact if Q date comes before remediation. Extending this to all applications, along with iterating for different Q date distributions, will show changes in risk for other timeline estimates for the development of cryptographic relevant quantum computers (CRQC).



Example data tables:

1. **Application:** Applications are data sources that 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 the cryptography used by a node. Each cryptographic method has a series of possible remediations to become quantum resilient.
5. Remediation: Details the remediation for the relevant current cryptography. It could be a PQC algorithm, a larger key size, etc. Each remediation has an associated cost. This cost is the estimated implementation time in years.

Example attributes of each of the data tables

Application	Nodes	Geospatial	Current Cryptography	Remediations
application_id: ID associated with application	node_model_id: id of the node model	coordinates: coordinates of a location	crypto_id: unique id for each crypto method	remediation_id: unique id for each remediation method
application_desc: Description of application	node_desc: description of node and node function	individual_node_ids list of individual nodes that are at this location	name: name of method	name: name of method
financial_impact: annual financial impact if application is compromised	num_instances: number of node_ids affiliated with the node_model_id		purpose: cryptographic function	purpose: cryptographic function that is addressed

line_of_business: division who owns the application	individual_node_ids: ids associated with individual node (serial number)		standards: standards reference material	standards: standards reference material
Shelflife: remaining years app will be in use	crypto_profile: list of cyrpto IDs		remediations: list of remediation method ids	affected_crypto_names: list of crypto names which are addressed
aff_node_models: list of node_model_ids affiliated with the app	device_3rd_party			implementation_cost: how many years it will take to implement remediation across the enterprise (for each individual node model)

Appendix B: Other PQC Risk Assessment Frameworks

There are two well-known PQC risk assessment frameworks currently available: Mosca's Quantum Risk Assessment (QRA) and Crypto Agility Risk Assessment Framework (CARAF). Mosca's QRA uses a time-based approach to define risk, dependent on when migration to a quantum-safe state begins and considers "harvest now decrypt later" attacks. CARAF builds on Mosca's QRA but focuses on "crypto agility" – the ability to quickly swap out vulnerable primitives, algorithms, and protocols for ones that are safer – and seeks to define organizational policies for specific asset groups. The following section provides additional information about each of these frameworks.

Mosca's Quantum Risk Assessment (QRA)

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 become quantum resilient. The risk assessment 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.

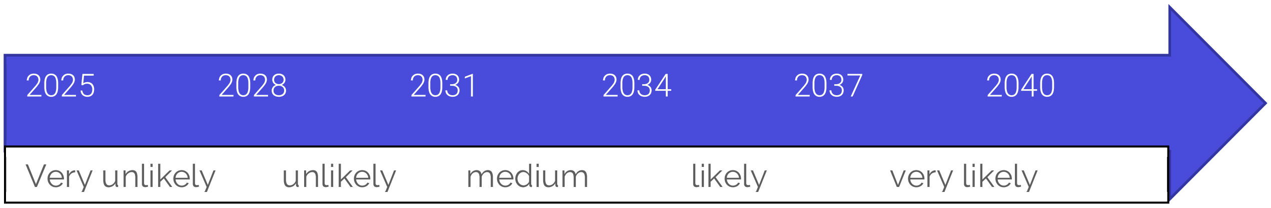
The methodology used in Mosca's QRA is adapted from the six stages for conducting a risk assessment in the NIST Cybersecurity Framework, identified in ID.RA. Mosca's QRA is intended to supplement or be performed after a regular risk assessment.

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.

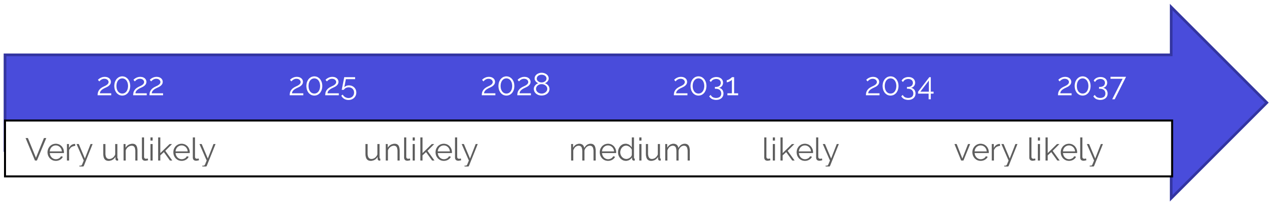
Phase 2 Research the state of emerging quantum computers and quantum-safe cryptography. As it is a challenge to create a realistic estimate for when quantum computers will emerge, the guidance for this step is to create a Quantum Risk Timeline for the probable emergence of a scalable quantum computer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

Crypto Agility Risk Assessment Framework (CARAF)

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

Phase 1: Identify threats

To identify potential threat vectors that will affect assets subject to crypto agility risks. For example, a large quantum computer will more severely impact public key crypto algorithms than symmetric key algorithms. It may be adequate to double the key size for symmetric key algorithms. However, 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

An inventory of impacted assets should be developed. 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	Assets will be in scope based on the threat identified in Phase 1. Interdependencies of services and devices should be considered.
Sensitivity	Measured based on impact if the asset is compromised, e.g., in terms of loss of confidentiality, integrity, or availability.
Cryptography	The cryptographic solutions that are being used to secure the in-scope assets with adequate sensitivity. May include algorithm security and key lengths.
Secrets Management	Information about the management of secrets (e.g., keys, passwords, API tokens, certificates) related to individual cryptographic solutions, such as frequency of use and updates.
Implementation	Information about how the cryptographic solution is implemented, e.g., hardcoded, hardware, software. May include the automated management of keys.
Ownership	Information about asset ownership, e.g., third-party vendor or product team, as well as ownership of upstream/downstream applications.
Location	Information on the location of the asset which may affect cryptographic agility, e.g., on premise, cloud, as well as jurisdiction.
Lifecycle Management	Data sharing arrangements with third parties, back up or recovery procedures, asset's lifespan, as well as the end-of-life processing.

Phase 3: Risk estimation

The 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 formula recommended by CARAF is Risk = Timeline x Cost. The "timeline to exposure" parameter is calculated based on information gathered from Phases 1 and 2 from Mosca's Model. The three components (shelf-life, mitigation, and threat) are scored between 1 and 4 (low risk, medium risk, high risk, critical). The Cost variable is defined as the cost of updating an asset to a secure state within the required timeline. The cost 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:

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

Phase 5: Organizational roadmap

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

Comparison of Mosca's QRA and the CARAF

	Mosca's QRA	**CARAF**
Overall goal	Identify and prioritize the activities required to maintain awareness, and to migrate the organization's technology to a quantum-safe state	To create a tactical roadmap to address risks identified from the lack of crypto agility assessment and thereby reduce the change management effort later
Overall Complexity	Low	Medium

Input	Univariate Risk-Timeline
	X = Security Shelf Life
	Y = Migration time
	Z = Collapse time
		Multivariate Risk-Timeline (extension of XYZ from Mosca's QRA) to accommodate different asset classes with additional risk score.
		Cost of migrating each asset class according to the timeline

Output	Level of organizational risk based on migration start date	Remediation roadmap prioritized based on risk estimation
Phases	1. Identify and document valuable information assets 2. Research the state of emerging quantum computers and quantum-safe cryptography 3. Determine Z	1. Identify threats 2. Inventory of assets 3. Risk estimation 4. Secure assets through risk mitigation 5. Organizational roadmap

	4. Determine X and Y 5. Determine quantum risk 6. Identify and prioritize activities for awareness and migration	

Appendix C: The FS-ISAC PQC Vendor Questionnaire

The FS-ISAC PQC group created a list of potential vendor questions based on the DHS PQC Roadmap to help institutions understand their vendor's PQC status:

- Are your Chief Information Officers engaged with standards-developing organizations related to Post-quantum Cryptography?
- Is your company inventorying your most sensitive and critical datasets that must 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 a 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?

References:

[1] 2022 Quantum Threat Timeline Report - Global Risk Institute
[2] NIST's Post-Quantum Cryptography Standardization
[3] NIST PQC FAQ
[4] FS-ISAC PQC Infrastructure Inventory Paper
[5] ASC X9 Informative Report
[6] Homeland Security Post-Quantum Cryptography Roadmap
[7] CARAF: Crypto Agility Risk Assessment Framework
[8] Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR) paper on BEST PRACTICES AND GUIDELINES v2.0

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