Post-Quantum Cryptography (PQC) Migration Roadmap

May 2025

The Post-Quantum Cryptography Coalition (PQCC) is a community of technologists, researchers, and expert practitioners with a mission to drive progress toward broader understanding and public adoption of post-quantum cryptography (PQC) and associated National Institute of Standards and Technology (NIST) standards. The PQCC emphasizes classical cryptosystems with quantum-safe security to enable information security in an era of cryptographically-relevant quantum computers.

Table of Contents

Background

Breakthroughs in the race to develop advanced quantum computing threaten our current systems which secure communications, ensure authenticity, and protect sensitive data at rest and in transit, necessitating the migration to post-quantum cryptography (PQC). While it may take another 10 to 20 years to develop a cryptographically-relevant quantum computer (CRQC) that can penetrate current cryptographic security, it is necessary to begin the migration process now to ensure successful planning and implementation timeframes. Initiating the migration to PQC also mitigates the threat of data being collected now for an adversary to decrypt later.

This migration roadmap is written as a guide for your organization to plan and implement its post-quantum journey, providing an overview of four key categories to progress the migration to PQC: (1) Preparation, (2) Baseline Understanding, (3) Planning and Execution, and (4) Monitoring and Evaluation. Additionally, desired outcomes are listed for each category and their associated activities, giving organizations an idea of where they should be throughout the process outlined in this roadmap.

Migration Overview

The migration to PQC across your organization can be broken down into four main categories. Accompanying these categories are activities your organization may take to progress and sustain their PQC migration. The implementation of categories and activities will look different organization-to-organization, and as seen in Figure 1, components of this roadmap can take place concurrently or in a staggered order.

Category 1: Preparation

Your organization sets up its migration to PQC by obtaining an overview of its PQC migration aims, assigning a migration lead, identifying necessary stakeholders, and aligning stakeholders through strategic messaging.

Category 2: Baseline Understanding

Your organization gathers a baseline understanding of its data inventory, the prioritized assets to be updated, and the required resources and available budget.

Category 3: Planning and Execution

Your organization collaborates with system vendors and internal system owners to ensure that post-quantum solutions are acquired externally or developed internally and implemented effectively.

Category 4: Monitoring and Evaluation

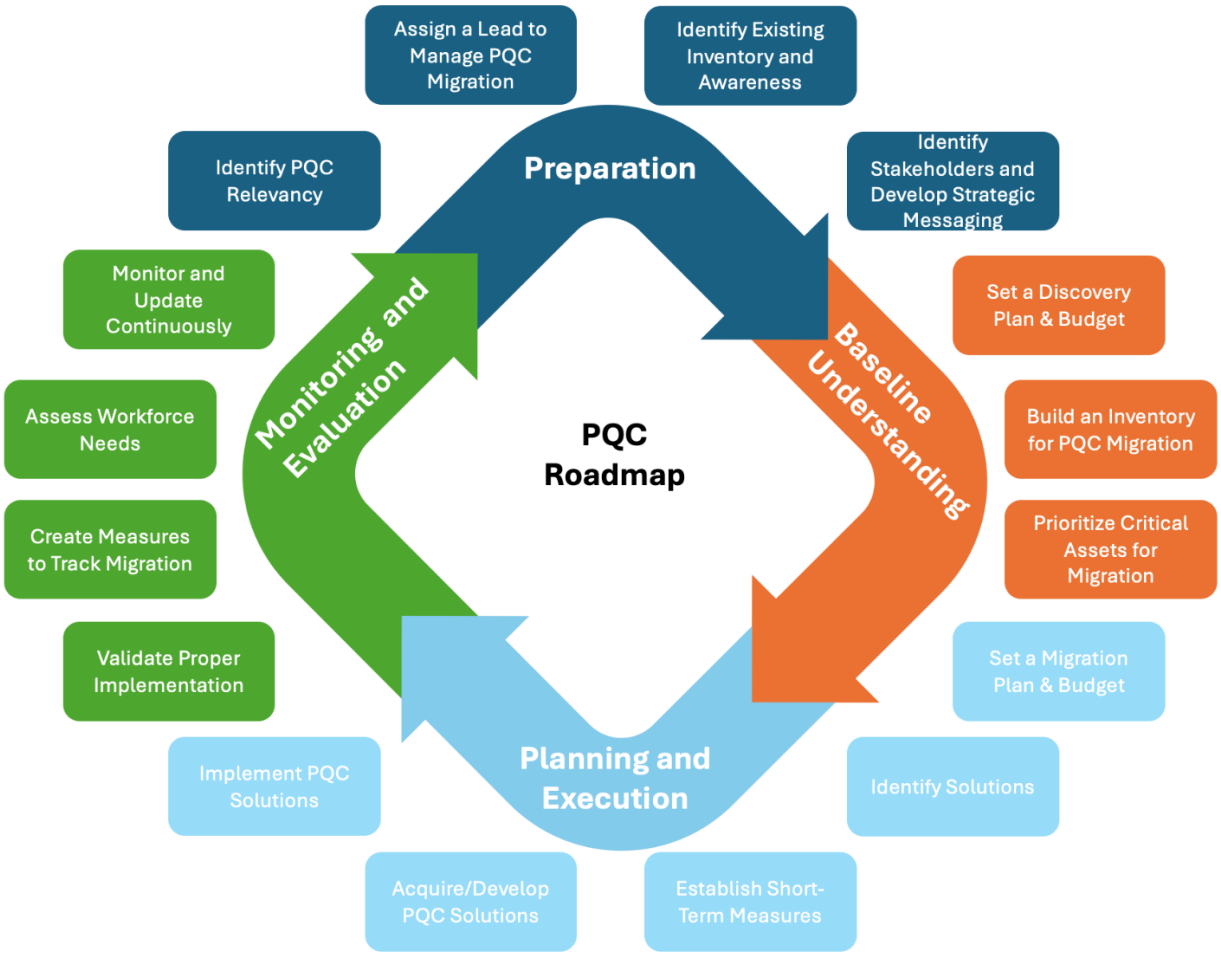
Your organization develops measures to track migration process and formulates a process for reassessing cryptographic security as quantum capabilities evolve.

Recommended Roadmap Implementation

How an organization applies this roadmap depends on the shelf-life and volume of its critical data, the amount of available information about its assets, its budget for potentially significant software and hardware updates, and numerous other influencing factors. The implementation of

categories and activities vary by organization, and may occur concurrently, consecutively, or individually.

Figure 1. PQC Roadmap Categories.



Category 1: Preparation

In the preparation category of PQC migration, your organization readies itself by obtaining an overview of its PQC migration aims, assigning a migration lead, identifying necessary stakeholders, and aligning stakeholders through strategic messaging.

Category 1 Outcomes:

- Organization familiarizes itself with its vulnerabilities and their level of urgency, determining an appropriate timeline to begin PQC migration.
- Organization assigns a migration lead responsible for progressing PQC migration.
- Organization identifies existing inventories and PQC awareness.
- Organization identifies and aligns its key stakeholders to PQC migration needs, leveraging strategic messaging.
- Organization begins initial vendor engagement for PQC solutions.

Activity 1.1: Identify PQC Relevancy

Before starting the journey towards PQC migration, your organization needs to assess whether it should begin this process now or follow a later timeline. Determining the appropriate timeline for your organization's PQC migration involves estimating migration, information shelf-life, and threat timelines. As seen in Figure 2 below, the shelf-life of sensitive information can impact the urgency of PQC adoption as adversaries may harvest present-day information to decrypt later with the help of a CRQC. Regardless of whether your organization faces the harvest-now-decrypt-later threat, it must be prepared to secure critical information against integrity and authenticity threats that will exist with the arrival of CRQCs.

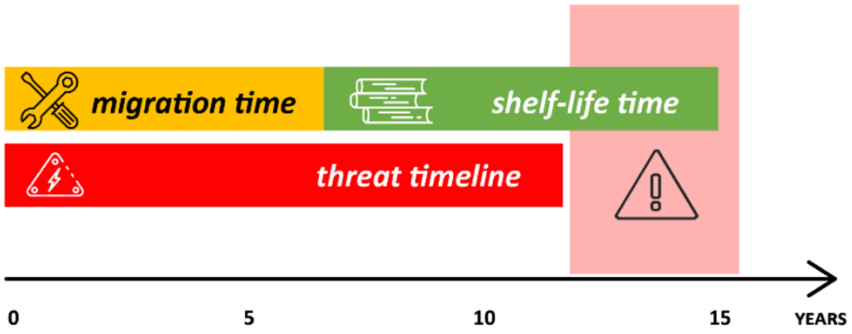


Figure 2. Model timeline for determining the urgency of PQC migration (Quantum Readiness Working Group).

To understand the general level of engagement your organization needs in its PQC journey, you should determine its PQC migration aims. This will initially clarify how much risk your organization is willing to take when it comes to protecting its data and assets. To determine your organization's migration aims, you may consider characteristics such as:

- Your organization's attack surface

- The types of systems and their potential malfunctions
- The criticality and sensitivity of data handled
- The urgency of migration needed
- The expected life span of replaced or migrated assets
- Interdependencies with other organizations

Your organization will either be an urgent adopter or a regular adopter. Urgent adopters handle highly sensitive data or assets, where a security breach could compromise critical infrastructure or expose sensitive personal or organizational data. Regular adopters are organizations that do not fall under the urgent adopter category. While regular adopters may store data or operate systems, they are at lower risk for store-now-decrypt-later schemes.

Activity 1.1 Outcomes:

- Organization clarifies its PQC migration aims and determines an appropriate timeline to begin PQC migration.
- Organization familiarizes itself with its vulnerabilities and their level of urgency.

Activity 1.2: Assign a Lead to Manage PQC Migration

When your organization decides to begin its PQC migration timeline, it should appoint an individual or team (a "migration lead") to monitor and progress its PQC migration. The responsibilities of this role will be specific to your individual organization, but may include setting timeframes, contacting vendors, and other migration implementation duties. In the end, PQC migration involves interfacing actively with a variety of leadership and technical roles, so the migration lead should be well positioned to cut across different areas within and outside your organization.

Activity 1.2 Outcomes:

- Organization defines the role and outcomes expected from its migration lead.
- Organization assigns a migration lead responsible for progressing PQC migration.

Activity 1.3: Identify Existing Inventory and Awareness

In this activity, the migration lead sets a plan for gathering a baseline understanding of its organization's cryptographic needs. This can include identifying what inventories are already available, determining what current migration efforts exist, and gaining a holistic view of your organization's migration posture. Your organization will want to check what inventories, risk assessments, and cryptographic bills of materials (CBOMs) it already has. Organizations may have multiple inventories and risk assessments that were designed to meet specific requirements at different points in time. When examining your existing inventories and risk assessments, document the location of the data and assets, who owns and operates them, why they were made, and how they are being used. Documenting the information your organization currently has —

and doesn't have — will help the migration lead clarify its needs early on and avoid unnecessary costs and efforts.

Activity 1.3 Outcomes:

- Migration lead has evaluated and documented any existing inventories, risk assessments, and awareness related to PQC migration.

Related Activities: 2.2, 2.3

Activity 1.4: Identify Stakeholders and Develop Strategic Messaging

Critical to achieving the activities in this roadmap is aligning your organization's leaders and key stakeholders to the value and purpose of PQC migration. Because of this, the migration lead should develop a communications plan specific to your organization which (1) identifies and aligns stakeholders and (2) communicates the process and need for PQC migration. This activity may include initial engagement with system operators and vendors to determine your organization's current migration context. Some questions to consider when developing strategic messaging include:

- What is the value/return on investment (ROI) of migrating our organization to PQC?
- How urgently do we need to begin PQC migration?
- How can we measure the impact of adopting PQC?
- What does PQC migration require from us financially and operationally?

Stakeholders are those that depend upon, support, or can benefit from your organization's PQC migration. Understanding stakeholder expectations includes understanding how they can—and do—influence other stakeholders. Listening to stakeholders and leveraging their input to drive continuous improvement and satisfaction is how your organization will continue to increase stakeholder commitment to progressing PQC migration.

In its strategic messaging, your organization may want to consider a positioning statement that provides an overview of the purpose and scope of your PQC migration. Your organization may also want to anticipate concerns stakeholders may have to migrating to PQC and draft response messaging that can help increase stakeholders' understanding and alignment to your organization's PQC goals. Additionally, your organization may draft elevator pitches to briefly communicate the value of PQC migration to stakeholders internal and external to your organization. Since stakeholder engagement and strategic messaging will span the entirety of your organization's PQC migration, you will also want to establish measures to track the impact of your strategic messaging on stakeholder activities.

Activity 1.4 Outcomes:

- Organization identifies and aligns its key stakeholders to the categories and activities of PQC migration.
- Organization can decisively communicate the value and purpose of PQC migration across an ecosystem of stakeholders.

Activity 1.4 a: Begin Engagement with System Vendors and Operators

Your organization's key stakeholder engagement will include initial conversations with its vendors and internal system operators to scope migration needs. Preliminary questions your organization will want to ask include:

- When will PQC solutions from the vendor be available?
- When will PQC solutions for internally developed systems be available?
- Will PQC updates necessitate hardware or software implementations?
- What is the cost of new solutions?
- What is the anticipated business impact of implementation efforts?
- Will a CBOM be included alongside solutions?
- What is the status of cryptographically agile solutions?

Activity 1.4 (a) Outcomes:

- Organization establishes a cadence with its vendors if it has not already.
- Vendor(s) and internal operator(s) help provide estimated timelines for PQC solution availability as well as implementation costs and impacts.

Category 2: Baseline Understanding

In the second category, the migration lead gathers a baseline understanding of its data inventory, the prioritized assets to be updated, and the required resources and available budget for discovery initiatives.

Category 2 Outcomes:

- Organization determines necessity for additional inventory and prioritization efforts.
- Organization has identified and documented all cryptographic assets necessary to achieve its desired level of PQC resiliency.
- Organization prioritizes assets in its inventory list based on sensitivity and lifespan.

Activity 2.1: Set a Discovery Plan and Budget

In this activity, the migration lead uses the initial information gathered (Activity 1.3) to determine whether the organization should proceed with additional measures to develop its inventory and asset prioritization. Utilizing information that is already available, the migration lead determines if additional inventorying initiatives are necessary (Activity 2.2) or if the organization can proceed directly to asset prioritization (Activity 2.3). The migration lead may also determine the available budget for inventorying, asset prioritization, and other discovery initiatives.

Activity 2.1 Outcomes:

- Migration lead identifies what inventorying and prioritization efforts need to be conducted for PQC migration.
- Migration lead identifies a budget for discovery initiatives.

Related Activities: 1.3, 2.2, 2.3

Activity 2.2: Build an Inventory for PQC Migration

Centralized inventories are essential for tracking enterprise-level migration timelines and ensuring comprehensive planning to address all security gaps. By building a clear inventory of assets and cryptographic use, your organization can proactively identify challenges and assure agility in planning PQC requirements. To effectively plan for PQC migration, the migration lead collaborates with system operators to:

- Determine what tools and methods to use in inventorying
- Document information about your most important assets
- Categorize your inventory(ies)

The following sub-activities (Activities 2.2 (a) and (b)) are not chronological but serve as considerations to make throughout the process of inventorying.

Activity 2.2 Outcomes:

- Organization documents its inventory of assets and cryptographic use.

Related Activities: 2.2 (a), 2.2 (b)

Activity 2.2 a: Consider Tooling and Methods to Use for Inventory

Your organization may want to consider using automated tools for identifying cryptographic algorithms across various components of an enterprise's infrastructure, including hardware, software modules, libraries, and embedded code. These tools should also pinpoint the algorithms used for cryptographic key establishment and management, which are crucial for securing cryptographically protected information and managing access. Additionally, automated tools should identify algorithms that ensure the integrity of data at rest, in transit, and in use, safeguarding both the source and content of the data. Consider your organization's level of accepted risk when choosing tools and methods, as some offer more granularity than others.

Activity 2.2 (a) Outcomes:

- The migration lead and technical teams identify which methods and tools will work best for gathering your organization’s inventory.

Activity 2.2 b: Collect and Categorize Information on Cryptographic Assets

In this activity, your organization’s migration lead and system operators document detailed technical information about your most important assets, including who operates them, what data they protect, and what architectural designs, design protocols, and interfaces they use. It is also crucial to document what your organization doesn’t know and to be aware of potential blind spots within your inventory, such as offline keys, keys in file structure inaccessible to automated tools, or keys with an unknown format. As your organization builds its inventory list, organize products by supplier to ensure you know who to contact in Activity 3.2 (a).

Activity 2.2 (b) Outcomes:

- Organization has a categorized list of all cryptographic assets that touch information of value.
- Organization has identified blind spots and information it does not know about its assets.
- Organization knows who to contact regarding each asset and is aware of what updates it will need to implement itself and what updates will need to be carried out by its suppliers.

Related Activities: 3.2 (a)

Activity 2.3: Prioritize Critical Assets for Migration

In this activity, the migration lead prioritizes critical assets and determines their migration timelines. This activity involves reviewing the inventory of assets and cryptographic use gathered in Activity 2.2 and evaluating its sensitivity and lifespan. This foundational understanding helps prioritize which systems require immediate attention and planning for future security needs. The migration lead will continue to consult relevant vendors and system operators to guide the outcomes of this activity.

Your organization may opt to conduct a detailed risk assessment for critical systems to further identify potential security, operational, and compliance risks. A key aspect of an assessment is evaluating risks in scenarios where adversaries possess large-scale quantum computers, and some cryptographic algorithms are rendered ineffective. This requires a reassessment of threats and prioritization of systems for migration to maintain security. Conducting a quantum risk assessment can produce a comprehensive list of all risks, the controls in place to mitigate those risks, and any further actions that need to be taken for mitigation.

Regardless of whether your organization decides to conduct a risk assessment, it will want to reference and utilize its migration, shelf-life, and threat timelines (see Figure 2) identified in Activity 1.1. Your final prioritized asset list will have considered estimated migration times, the urgency of migrating assets, and viable risk mitigation strategies.

Activity 2.3 Outcomes:

- Organization assesses its inventory and creates a prioritized asset list based on sensitivity and lifespan.
- If opting for a risk assessment, organization develops a comprehensive list of all risks, the controls in place to mitigate those risks, and any further actions that need to be taken for mitigation.

Related Activities: 1.1, 2.2

Category 3: Planning and Execution

Category 3 of this roadmap focuses on high-level activities that your organization should consider at the beginning of the migration processes. Your organization will determine which post-quantum solutions can be acquired from vendors or developed internally. Near- and long-term risk is mitigated through out-of-band mechanisms and PQC solution implementation. This section is purposefully less prescriptive due to the lack of information available on organizational migration processes.

Category 3 Outcomes:

- Organization develops a plan to manage the migration to PQC, determining what systems must be acquired or developed.
- Organization has implemented, acquired, or developed PQC solutions across their infrastructure.
- Organization implements short-term measures to mitigate the exposure of sensitive data.

Activity 3.1: Set a Migration Plan and Budget

Using your prioritized asset list from Activity 2.3, determine the appropriate course of action for each prioritized asset—whether to mitigate risk, start migration to PQC, or manage exceptions by accepting quantum risk. You may also want to engage with your organization's vendors to fully understand an asset's risk level (Activity 3.2 (a)). Additionally, you will want to get an idea of what workforce changes your organization will need to implement in order to execute its PQC migration (Activity 4.3).

The migration lead, in coordination with your organization's financial team and system operators, will then estimate the costs of migrating those assets to PQC. For this activity, you'll want to understand the work breakdown structure of migrating your prioritized assets, which could include scheduled tasks and the estimated costs of each task.

Activity 3.1 Outcomes:

- Organization estimates the cost of migrating its prioritized assets to PQC and builds a budgeting plan.

Related Activities: 2.3, 3.2 (a), 4.3

Activity 3.2: Identify Solutions

In this activity, the migration lead identifies the solutions specific to your organization's migration needs. The migration lead uses the prioritized asset list created in Activity 2.3 to coordinate with internal system operators and/or maintainers. During initial coordination efforts, the migration lead should attempt to identify and document what system updates must be acquired and what systems must be updated internally. Additionally, the migration lead should seek to identify what systems are able to be migrated to PQC via software updates and what systems will necessitate hardware upgrades.

Additionally, prior to selecting migration products that best suit your organization, it is important to verify whether they are compliant with current PQC standards. Check whether your vendors or systems align with NIST's standards and guidelines on cryptographic algorithms, currently outlined in FIPS 203, 204, and 205. Organizations should also be aware of NIST's Cryptographic Module Validation Program, which validates cryptographic algorithms using a set of testable cryptographic and security requirements to provide agencies with a metric to assess security. Finally, throughout this activity, your organization should document its compliance. Documentation will enable ease of access for future reference and prevent duplicative efforts.

Optional: During this period, the migration lead should assess the viability of hybrid and/or agile cryptographic implementations. Hybrid cryptographic implementations may help alleviate some cost in the migration processes and assist in ensuring backwards and forwards compatibility. Investing in and implementing agile cryptographic systems/methods will help enhance your organization's ability to quickly adjust to new security threats in a cost and time efficient manner. Adopting agile solutions now will reduce the cost of future cryptographic updates, support long term maintenance of systems, and mitigate risks associated with vendor lock-in or outdated cryptography.

Activity 3.2 Outcomes:

- Organization creates system/solution implementation plan.
- Organization determines what vulnerable systems must be upgraded to reduce risk and meet compliance requirements.
- Organization determines if available solutions are compliant with current PQC standards.
- Organization determines necessity and desire for agile cryptographic implementations/solutions.
- Organization assesses the implementation methods of PQC solutions and projected organizational impacts.

Related Activities: 2.3

Activity 3.2 a: Confirm Migration Needs with Vendors

Using the prioritized asset list, the migration lead, in coordination with relevant organizational acquisition authorities, should continue engagement with system vendors to determine the availability of post-quantum solutions. The migration lead should confirm and reassess the following questions from Activity 1.4 (a):

- When will PQC solutions from the vendor be available?
- Will PQC updates necessitate hardware or software implementations?
- What is the cost of new solutions?
- What is the anticipated business impact of implementation efforts?

- Will a CBOM be included alongside solutions?

Activity 3.2 (a) Outcomes:

- Organization identifies what PQC solutions are available from commercial vendors.
- Organization updates acquisition language and contracts to ensure newly acquired systems meet PQC standards.
- Organization determines timeline for PQC solution availability and cost of solutions.
- Organization coordinates with vendors to determine extent of organization disruption during implementation processes.

Related Activities: 1.4 (a), 2.3

Activity 3.2 b: Build Solutions

Using the prioritized asset list, the migration lead should coordinate with the system operators of custom systems or systems that do not yet have a commercial update available to begin the development process. The migration lead should consider:

- What is the timeline for developing post-quantum solutions?
- Will PQC updates necessitate hardware or software implementations?
- What is the cost to develop solutions?
- Are there commercial solutions available?

Activity 3.2 (b) Outcomes:

- Organizations determine the timeline, costs, and resources needed to develop solutions for niche or custom applications.
- Organizations determine if commercial solutions are available that offer comparable performance.

Related Activities: 2.3

Activity 3.3: Establish Short-Term Measures

Using the timeline for solution availability and the prioritization assessment, the migration lead must determine what measures should be taken to ensure that sensitive systems and information is protected. Additionally, for systems and data that is at risk for "harvest now, decrypt later" attacks, the migration lead should coordinate with the system operators/maintainers to assess what short-term solutions can be implemented to help mitigate risk. These measures may include:

- Decrease life of new certificates
- Increase length of newly certified keys
- Plan for revoking overly long-lived certificates
- Modernize to support TLS 1.3
- Re-examine physical security procedures and data-at-rest protections for long-lived data
- Consider adding extra security layers to systems that protect data (VPN)

While these security measures may be helpful in mitigating some of the risk associated with the quantum computing threat, they **are not** a substitute for migration to PQC.

Activity 3.3 Outcomes:

- Organization determines necessity for short-term measures to mitigate risk to quantum threat.
- Organization creates and implements risk mitigation strategies to reduce data exposure.

Related Activities: 3.2 (a), 3.2 (b)

Activity 3.4: Acquire/Develop PQC Solutions

In coordination with organizational acquisition authorities, the migration lead begins acquiring post quantum solutions and distributing resources for the internal development of solutions. These acquisition and development processes occur in the order of prioritized assets determined in Activity 2.3.

Activity 3.4 Outcomes:

- Organization distributes resources for acquisition and development.
- Organization purchases PQC solutions from vendors.
- Organization begins internal development of PQC solutions.

Related Activities: 2.3

Activity 3.5: Implement PQC Solutions

Your organization installs short-term and long-term mitigations and solutions. The migration lead determines the extent of organizational disruptions and creates contingency plans in the case of extended disruption. If your organization is incrementally deploying systems, the migration lead facilitates coordination to ensure forward and backward compatibility.

Activity 3.5 Outcomes:

- Organization implements acquired or developed PQC solutions.
- Organization updates inventory to reflect new system status.

Category 4: Monitoring and Evaluation

Your organization tracks the migration process and formulates a process for reassessing cryptographic security as quantum capabilities evolve. During this category, the migration lead should also ensure that all documentation from migration efforts is maintained and creates processes for continuous evaluation to assist in potential future technology migrations.

Category 4 Outcomes:

- Organization validates implementations of solutions and compliance with standards.
- Organization has prepared its workforce to utilize/implement PQC solutions.
- Organization tracks its migration progress and validates its desired outcomes.
- Organization creates processes to continuously monitor its security against technological developments.

Activity 4.1: Validate Proper Implementation

The migration lead, in collaboration with the system implementors, evaluates the effectiveness of the implemented PQC systems. During this activity, the system operators ensure the implemented solution meets the system cryptographic and operational requirements (i.e., backwards and forwards compatibility). Following successful verification of implementation, the migration lead should ensure that the inventory has been updated to reflect the new system status.

Optional: Dependent on your organization's size and structure, the migration lead and organizational leadership may choose to implement an enforcement mechanism to encourage and expedite the organization's migration processes.

Activity 4.1 Outcomes:

- Migration lead has evaluated PQC effectiveness in securing priority assets.
- Interoperability and operational requirements are verified and documented.
- Inventory is updated to reflect new system status.

Activity 4.1 a: Ensure Alignment with Industry Standards

Depending on the type of data your organization handles, it must ensure that its PQC migration considers existing industry regulations. For instance, a health sector organization may evaluate their PQC migration against HIPAA standards, or an organization operating within the EU will certify NIS2 compliance. Additionally, these standards may already require PQC-adjacent activities such as future-proofing and regular risk assessments, offering more of a compelling reason to begin planning for PQC migration. Overall, assessing current standards while also

anticipating future changes to them will better enable your organization to stay ahead of regulatory developments as well as the threat landscape.

Activity 4.1 (a) Outcomes:

- Organization integrates existing industry standards into its PQC migration planning.
- Organization documents how its PQC migration adheres to industry standards.

Activity 4.2: Create Measures to Track PQC Migration Success

Critical to knowing the impact of your organization's PQC migration is determining the amount of sensitive information that has been cryptographically updated. For this activity, the migration lead may use the prioritized asset list identified in Activity 2.3 to track the cryptographic state of the inventory.

When designing a performance measurement plan, remember that "you get what you measure." Choose measures that effectively indicate performance and can be practically gathered. Measures should be data-driven, progress-focused, decision-oriented, and limited to a few critical inquiries. Finally, measures will address different categories of your organization's PQC migration. For instance, for the preparation category, you may want to identify measures to track the impact of your strategic messaging on stakeholder alignment. For planning and execution, you will want to track the number of systems that have migrated to PQC.

There is still extensive research to be made on how to best measure the security of PQC migration. In the meantime, organizations should reference NIST and NSA standards to ensure the most up-to-date measurement methods are employed.

Activity 4.2 Outcomes:

- Organization identifies measures that allow it to track PQC migration success.
- Organization can determine the amount of sensitive information that is protected by new PQC solutions.

Related Activities: 2.3

Activity 4.3: Assess Workforce Needs

The migration lead will assess how to optimize your organization's current workforce to implement and maintain newly acquired/developed PQC solutions. This could include coordinating with system owners/operators to identify gaps within current workflows, distributing necessary training, and/or determining if additional talent is needed to execute the migration processes. Necessary changes made to your organization's workforce may impact how your organization budgets for (Activity 3.1) and continues to implement (Activity 3.5) its PQC migration.

Activity 4.3 Outcomes:

- Organization determines if additional security trainings are needed for new PQC security implementations.
- Organization determines if additional workforce is needed to assist in the operation/migration of systems to PQC.

Related Activities: 3.1, 3.5

Activity 4.4: Monitor and Update Continuously

The migration lead will continue to monitor and measure developments in your organization's security, updating inventory lists, tracking compliance with new standards, and assessing your organization's risk environment. As mentioned in previous activities, documenting these changes and updates will be integral to sustaining your organization's security resilience.

Activity 4.4 Outcomes:

- Organization continues to update inventory of cryptographic algorithms.
- Organization continuously measures migration progress against organizational goals.
- Organization maintains preparedness by creating a process to monitor technological developments and risk status.

Related Activities: All

Conclusion

For many organizations, migrating to PQC is crucial to safeguard their data against future quantum threats. This roadmap provides a tailorable guide through the four critical categories of this transition: (1) Preparation, (2) Baseline Understanding, (3) Planning and Execution, and (4) Monitoring and Evaluation. Each category is designed to equip organizations with the necessary tools and strategies to effectively manage the complexities of PQC migration. The process outlined in this roadmap underscores the importance of strategic planning, stakeholder alignment, and continuous monitoring and documentation to adapt to technological advancements and maintain robust security postures. As the quantum computing landscape continues to evolve, organizations must remain adaptable, tracking updates in guidance to maintain a secure PQC transition.

References

Attema T, Duarte J, Dunning V, Lequesne M, van der Schoot W, Stevens M (2023) The PQC Migration Handbook. (Applied Cryptography and Quantum Algorithms, Cryptology Group, and Netherlands National Communications Security Agency). https://publications.tno.nl/publication/34641918/oicFLj/attema-2023-pqc.pdf

Cybersecurity and Infrastructure Security Agency (2023) Quantum Readiness: Migration to Post-Quantum Cryptography. https://www.nccoe.nist.gov/sites/default/files/2023-08/quantum-readiness-fact-sheet.pdf

FS-ISAC (2023) PQC Working Group Infrastructure Inventory Technical Paper. https://www.fsisac.com/hubfs/Knowledge/PQC/InfrastructureInventory.pdf

FS-ISAC (2023) PQC Working Group Risk Model Technical Paper. https://www.fsisac.com/hubfs/Knowledge/PQC/RiskModel.pdf

Moody D, Perlner R, Regenscheid A, Robinson A, Cooper D (2024) Transition to Post-Quantum Cryptography Standards. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST IR 8547 ipd. https://doi.org/10.6028/NIST.IR.8547.ipd

National Institute of Standards and Technology (2024) Module-Lattice-Based Key-Encapsulation Mechanism Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 203. https://doi.org/10.6028/NIST.FIPS.203

National Institute of Standards and Technology (2024) Module-Lattice-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 204. https://doi.org/10.6028/NIST.FIPS.204

National Institute of Standards and Technology (2024) Stateless Hash-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 205. https://doi.org/10.6028/NIST.FIPS.205

Quantum Readiness Working Group of the Canadian Forum for Digital Infrastructure Resilience (2024) Canadian National Quantum-Readiness Best Practices and Guidelines. https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/documents/Quantum-Readiness%20Best%20Practices%20-%20v04%20-%2010%20July%202024.pdf