NIST Cybersecurity White Paper
NIST CSWP 48 ipd

Mappings of Migration to PQC Project Capabilities to NIST Cybersecurity Framework 2.0 and to Security and Privacy Controls for Information Systems and Organizations

Initial Public Draft

William Newhouse
Applied Cybersecurity Division
Information Technology Laboratory

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

William Barker
Stratvia LLC

Karen Scarfone
Scarfone Cybersecurity

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.48.ipd

September 18, 2025

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

Publication History
Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]

How to Cite this NIST Technical Series Publication:

Newhouse W, Souppaya M, Barker W, Scarfone K (2025) Mappings of Migration to PQC Project Capabilities to Risk Framework Documents. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 38.ipd. https://doi.org/10.6028/NIST.CSWP.48.ipd

Author ORCID iDs
Murugiah Souppaya: 0000-0002-8055-8527
Bill Newhouse: 0000-0002-4873-7648
William Barker: 0000-0002-4113-8861
Karen Scarfone: 0000-0001-6334-9486

Public Comment Period

September 18, 2025 - October 20, 2025

Submit Comments

applied-crypto-pqc@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/publications/cswp, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

The capabilities demonstrated by the NCCoE Migration to Post-Quantum Cryptography project support several security objectives and controls identified by the NIST Cybersecurity Framework 2.0 (CSWP 29) and Security and Privacy Controls for Information Systems and Organizations (SP 800-53), respectively. A responsible implementation of the demonstrated capabilities depends on adherence to several security objectives and controls identified in these risk framework documents.

This paper identifies the supported and dependent characteristics of capabilities functions that are part of the Migration to Post-Quantum Cryptography project at NIST's National Cybersecurity Center of Excellence and maps those functions to elements of both the NIST Cybersecurity Framework 2.0 and Special Publication 800-53 Revision 5.

The NCCoE Migration to Post-Quantum Cryptography project demonstrates practices to ease migration from the current set of public-key cryptographic algorithms to replacement algorithms resistant to quantum computer-based attacks. Project collaborators demonstrate using cryptographic discovery and inventory tools to allow an organization to learn where and how cryptography protects the confidentiality and integrity of the organization's important data and digital systems. Project collaborators are also exploring interoperability of the NIST PQC algorithms for key establishment and digital signature schemes in internet communication protocols and hardware security modules (HSMs).

Keywords

algorithm; cryptography; encryption; identity management; key establishment and management; post-quantum cryptography; public key cryptography; quantum-resistant; vulnerable cryptography discovery.

Audience

The primary audience for this report is security program managers and architects, as well as IT professionals, especially those involved with planning migration to quantum-safe algorithms, and risk management staff at companies that produce security software and hardware.

Table of Contents

List of Tables

1. Overview

1.1. Introduction

The National Institute of Standards and Technology's (NIST's) National Cybersecurity Center of Excellence (NCCoE) is engaging with industry collaborators, industry sectors, and the U.S. Federal Government to bring awareness to the challenges involved in migrating information technology systems from cryptographic algorithms vulnerable to attacks from a cryptanalytically-relevant quantum computer.

The NCCoE Migration to Post-Quantum Cryptography project [1] demonstrates practices to ease migration from the current set of public-key cryptographic algorithms to replacement algorithms resistant to quantum computer-based attacks.

The project's Cryptographic Discovery workstream focuses on the use of cryptographic discovery and inventory tools to allow an organization to learn where and how cryptography is being used to protect the confidentiality and integrity of the organization's important data and digital systems. The discovery workstream also looks at how cryptographic inventories can support risk management and prioritization decisions about where to implement technologies that leverage the NIST standardized post-quantum cryptographic algorithms.

The project's Interoperability and Performance workstream explores how the NIST PQC algorithms for key establishment and digital signature schemes will operate in communication protocols such as the Transport Layer Security (TLS) protocol, the Secure Shell (SSH) protocol, and with hardware security modules (HSMs).

The project's outputs are described in publications posted to the NCCoE Migration to Post-Quantum Cryptography webpage, which has an associated frequently asked questions resource available at https://pages.nist.gov/nccoe-migration-post-quantum-cryptography.

The capabilities demonstrated in the project **support** several security objectives and controls identified by the NIST *Cybersecurity Framework 2.0* [2] and *Security and Privacy Controls for Information Systems and Organizations* (SP 800-53) [3], respectively.

At the same time, responsible implementation of the demonstrated capabilities is **dependent** on adherence to several security objectives and controls security objectives and controls identified in these risk framework documents.

This paper identifies the supported and dependent characteristics from the NIST Cybersecurity Framework 2.0 and NIST Special Publication 800-53 Revision 5 for demonstrated *Discovery and Inventory* and *Interoperability and Performance capabilities*.

1.2. Migration to Post-Quantum Cryptography (PQC) Capability Demonstrations

1.2.1. Quantum-Vulnerable Cryptography Discovery

The Migration to PQC Project's Quantum-Vulnerable Cryptography Discovery Workstream demonstrates tools for discovering quantum-vulnerable cryptographic algorithms used in code development pipelines, software development lifecycle, and repository components; network services and protocols; and end-user systems and servers that include applications and associated libraries. The project will offer insights for planning a migration roadmap using a risk-based approach.

The discovery workstream's identification of assets such as hardware and software as part of an inventory is a core function of the Cybersecurity Framework (CSF) and a basic precondition for any organization to manage cybersecurity risk effectively. This project aims to extend existing inventory capabilities when identifying *cryptographic* assets with discovery and inventory tools and subsequently correlating their output to previously (and hopefully continuously) inventoried hardware, software, and services. This project demonstrates a combination of active and passive cryptographic discovery and inventory technologies.

1.2.2. Interoperability and Performance of implemented PQC Algorithms

Interoperability testing of NIST pre-standardized PQ cryptographic algorithms was identified as a core focus area to support the ability of technology vendors and standards bodies to migrate and develop new products that utilize PQC. Benchmarking performance metrics from the interoperability tests performed in our lab will assist our consortium members and any technology vendors in optimizing their implementations as they move toward production-grade status. Understanding the performance metrics of PQ-ready algorithms plays a crucial role in motivating technology providers to offer technologies that enable organizations' migrations and provide initial data on which PQ cryptographic algorithm is best suited for specific use cases.

The Interoperability and Performance Workstream's consortium members contributed working implementations of selected NIST standardized PQC algorithms in a variety of testing scenarios for the Transport Layer Security (TLS) protocol, QUIC (Quick UDP Internet Connections), Secure Shell (SSH) protocol, and hardware security modules (HSMs). The project's collaborators implemented NIST's pre-standardized post-quantum cryptographic algorithms in a lab environment to gain experience using PQC algorithms and have moved to using the three NIST PQC standards published in August 2024. Interoperability testing examples include successful communication between collaborator server implementations of lab versions of TLS and SSH using PQC. A performance measurement example documented the maximum TLS 1.3 handshake rate for testing profiles.

The NCCoE Migration to PQC project collaboration also leverages and highlights the outcomes from our consortium members participating in standardizing the use of PQC in standard bodies such as the Internet Engineering Task Force (IETF).

2. Mapping Process

This section provides mappings between cybersecurity functions of the logical architecture components demonstrated in the project's lab to security characteristics enumerated in relevant cybersecurity documents. These mappings are intended for any organization interested in implementing PQC migration tools and components or for organizations already implementing PQC.

Logical Architecture Components for Discovery and Inventory Tools include Cryptographic Data Collection Tools, Cryptographic Inventory Tools, Cryptographic Analytics Tools, and Certificate Discovery and Management Tools.

Logical Architecture Components for Post-Quantum Cryptography Implementations in the interoperability and performance workstream include Quantum-Ready Algorithm Implementations, Quantum-ready Cryptographic Service Implementations, Quantum-ready Integration Tools and Application Plugins, Quantum-ready Certificate Authority Implementations, and Quantum-ready Hardware Security Modules (HSMs).

The mappings provide information on how cybersecurity functions from the project's reference design are related to NIST-recommended security outcomes and controls: the security outcome subcategories from the NIST *Cybersecurity Framework 2.0* [2] and Security and Privacy Controls for Information Systems and Organizations (SP 800-53) [3]. All elements in these mappings—the PQC demonstrated capabilities described as Logical Architecture Components and Component's Functions, CSF Subcategories, and SP 800-53 controls—involve ways to reduce cybersecurity risk.

2.1. Use Cases

There are two primary use cases for this mapping. They are not intended to be comprehensive.

1. **Why should organizations implement discovery, interoperability, and performance capabilities?** This use-case identifies how implementing discovery and inventory functions and interoperability and performance demonstration capabilities can support organizations in achieving CSF Subcategory outcomes and SP 800-53 security controls. This helps communicate to an organization's chief information security officer, chief data officer, security team, and senior management that expending resources to implement discovery, interoperability, and performance capabilities can also aid in fulfilling other security requirements.

2. **How can organizations implement discovery, interoperability, and performance capabilities?** This use case identifies how an organization's existing implementations of CSF Subcategories and SP 800-53 controls can help support the trusted implementation of discovery and inventory functions and interoperability and performance demonstration capabilities. An organization wanting to migrate to quantum-resistant cryptography might first assess its current security capabilities so that it can plan how to

establish and implement a migration roadmap while adding missing capabilities and enhancing existing capabilities. Organizations can leverage their existing security investments and prioritize future security technology deployment to address the gaps.

2.2. Mapping Terminology

In this publication, we use the following relationship types from NIST IR 8477 Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings [4] to describe how the functions in project demonstrations relate to the NIST reference documents. In NIST IR 8477, this is called a supportive relationship mapping.

The "Supports" relationship applies only to use case 1 which focuses on why organizations should implement discovery, interoperability, and performance capabilities. The "Is Supported By" relationship applies only to use case 2 which focuses on how organizations can implement discovery, interoperability, and performance capabilities.

3. **Supports:** Demonstration component function X supports security control/Subcategory Y when X can be applied alone or in combination with one or more other component functions to achieve Y in whole or in part.
4. **Is Supported By:** A demonstration component function X is supported by security control/Subcategory Y when Y can be applied alone or in combination with one or more other security controls/Subcategories to achieve X in whole or in part.

Each *Supports* and *Is Supported By* relationship have one of the following properties assigned to them:

5. **Example of:** The supporting concept X is one way (an example) of achieving the supported concept Y in whole or in part. However, Y could also be achieved without applying X.
6. **Integral to:** The supporting concept X is integral to, and a component of the supported concept Y. X must be applied as part of achieving Y.
7. **Precedes:** The supporting concept X precedes the supported concept Y when X must be achieved before applying Y. In other words, X is a prerequisite for Y.

When determining whether a demonstration component function's support for a given CSF Subcategory or SP 800-53 control is integral to that support versus an example of that support, we do not consider how that function may, in general, be used to support the Subcategory or control. Rather, we consider only how that function is intended to support that Subcategory or control within the reference design.

Also, when determining whether a function is supported by a CSF Subcategory outcome or SP 800-53 control with the relationship property of precedes, we do not consider whether applying the function without first achieving the Subcategory or control is possible. Instead, we consider whether, according to our reference design, the Subcategory or control will be achieved prior to applying that function.

3. Cybersecurity Framework Mapping

Table 1 provides a mapping of tools supporting migration to quantum-resistant algorithms to the CSF. It includes both CSF outcomes that need to be met for secure operation of the tools and CSF outcomes that the platform supports. Note that the current PQC migration project does not involve operational use of cryptographic systems; it only addresses laboratory demonstration and measurement in a controlled environment. As a result, many of the organizational and operational security objectives do not apply to this paper's mappings.

Table 1 Architecture Mapping to CSF

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Discovery and Inventory Tools			
Cryptographic Data Collection Tools	Sensors that are used to scan technologies and systems deployed within a digital footprint for cryptography. Technologies scanned include hosts (for filesystem, binary data, running processes, certificate stores, etc.), network interfaces, CI/CD pipelines, application repositories, key management systems, PKI systems, and HSM systems.	Supports (precedes) ID.AM-01: Inventories of hardware managed by the organization are maintained	Crypto data collection is a first step in developing a cryptographic inventory. The inventory is necessary to understand the continuing adequacy of the PQC security services on which the organization depends.
		Supports (precedes) ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.	
		Supports (precedes) ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	
Cryptographic Inventory Tools	Products that enable an organization to build comprehensive centralized inventories of all cryptographic	Supports (integral to) ID.AM-01: Inventories of hardware	Cryptographic inventory tools enable an organization to build comprehensive centralized inventories of all cryptographic

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	assets, including cryptographic keys, keystores, X.509 certificates, cryptographic libraries, cryptographic algorithms, and cryptographic protocols deployed across their digital footprint.	managed by the organization are maintained	assets, including HSMs and cryptographic hardware modules.
		Supports (integral to) ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.	Cryptographic inventory tools enable an organization to build comprehensive centralized inventories of cryptographic assets for all software, services, and systems managed by the organization, including cryptographic keys, keystores, X.509 certificates, cryptographic libraries, and cryptographic algorithms and protocols.
		Supports (integral to) ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	Cryptographic inventory tools enable an organization to build and maintain comprehensive centralized inventories of all cryptographic data and corresponding metadata.
Cryptographic Analytics Tools	Products that review a cryptographic inventory and identify cryptographic weaknesses, compliance gaps, and quantum-vulnerable objects based on a policy; provide snapshots of the processing environments by extracting security and cryptographic information based on configurable policies; provide details on keys managed by processors and applications; and help identify insecure keys, algorithms, and enabled services.	Is supported by (integral to) GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.	Cryptographic analytics tools review cryptographic inventories and identify cryptographic weaknesses, compliance gaps, and/or quantum-vulnerable objects based on the organization's cybersecurity policies. The security and cryptographic information extraction processes are based on configurable policies.
		Supports (example of) ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded	Cryptographic analytics tools review cryptographic inventories and identify cryptographic weaknesses, compliance gaps, and/or quantum-vulnerable objects.

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Is supported by (example of) ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	Threats, vulnerabilities, likelihoods, and impacts inherent in post-quantum risk assessment are informed by outputs from cryptographic analytics tools.
		Supports (example of) PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	Cryptographic analytics tools identify cryptographic weaknesses, compliance gaps, and/or quantum-vulnerable objects that could, if implemented operationally, degrade the integrity of credentials for authorized users, services, and hardware are managed by the organization
		Supports (example of) PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	Cryptographic analytics tools identify cryptographic weaknesses, compliance gaps, and/or quantum-vulnerable objects that could, if implemented operationally, degrade the integrity of the binding of identities to credentials.
		Supports (example of) PR.AA-03: Users, services, and hardware are authenticated	Cryptographic analytics tools identify cryptographic weaknesses and compliance gaps in authentication mechanisms that could, if implemented operationally, degrade the integrity of the authentication process.
		Supports (example of) PR.AA-04: Identity assertions are protected, conveyed, and verified	Cryptographic analytics tools identify cryptographic weaknesses, compliance gaps, and/or quantum-vulnerable objects that could, if implemented operationally, degrade the integrity of identity assertions.

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (example of) PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Cryptographic analytics tools identify cryptographic weaknesses, compliance gaps, and/or quantum-vulnerable objects that could, if implemented operationally, degrade the enforcement of authorizations as defined in policy.
		Supports (example of) PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	Cryptographic analytics tools identify cryptographic weaknesses, compliance gaps, and/or quantum-vulnerable objects that could, if implemented operationally, degrade the confidentiality, integrity, and/or availability of data-at-rest.
		Supports (example of) PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	Cryptographic analytics tools identify cryptographic weaknesses, compliance gaps, and/or quantum-vulnerable objects that could, if implemented operationally, degrade the confidentiality, integrity, and/or availability of data-in-transit.
		PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	Cryptographic analytics tools identify cryptographic weaknesses, compliance gaps, and/or quantum-vulnerable objects that could, if implemented operationally, degrade the confidentiality, integrity, and/or availability of data in use.
		PR.DS-11: Backups of data are created, protected,	Cryptographic analytics tools identify cryptographic weaknesses, compliance gaps, and/or quantum-vulnerable

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		maintained, and tested	objects that could, if implemented operationally, degrade the protection of data backups.
Certificate Discovery and Management Tools	Certificate discovery and lifecycle automation tools that provide centralized visibility, governance, and lifecycle automation for digital certificates to identify weak and non-compliant certificates.	Is supported by (integral to) GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.	Certificate discovery and lifecycle automation tools identify weak and non-compliant certificates according to organizational policies.
		Is supported by (example of) ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	Threats, vulnerabilities, likelihoods, and impacts inherent in post-quantum risk assessment are informed by outputs from certificate discovery tools that identify weak and non-compliant certificates.
		Is supported by (integral to) PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	The integrity of analytic results is dependent on control of access to project facilities and networks. Unauthorized access to programs and processes can result in incorrect findings.
Post-Quantum Cryptography Implementations			
Quantum-Ready Algorithm Implementations	PQC applications and libraries.	Is supported by (integral to) GV.PO-01: Policy for managing	Selection and implementation of cryptographic algorithms and libraries is constrained by policies based on organizational context,

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	cybersecurity strategy, and priorities.
		Supports (example of) PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	Successful demonstrations of quantum-ready algorithm implementations show the feasibility of implementation of alternatives to quantum-vulnerable algorithms, the use of which can endanger the integrity of credentials for authorized users, services, and hardware are managed by the organization.
		Supports (example of) PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	Successful demonstrations of quantum-ready algorithm implementations show the feasibility of implementation of alternatives to quantum-vulnerable algorithms, the use of which can endanger the integrity of binding of identities to credentials.
		Supports (example of) PR.AA-03: Users, services, and hardware are authenticated	Successful demonstrations of quantum-ready algorithm implementations show the feasibility of implementation of alternatives to quantum-vulnerable algorithms for authentication purposes.
		Supports (example of) PR.AA-04: Identity assertions are protected, conveyed, and verified	Successful demonstrations of quantum-ready algorithm implementations show the feasibility of implementation of alternatives to quantum-vulnerable algorithms, the use of which can endanger the integrity of identity assertions.
		Supports (example of)	Successful demonstrations of quantum-ready algorithm

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	implementations show the feasibility of implementation of alternatives to quantum-vulnerable algorithms, the use of which can endanger the integrity of access permissions and authorizations.
		Supports (precedes) PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	Successful demonstrations of quantum-ready algorithm implementations show the feasibility of implementation of alternatives to quantum-vulnerable algorithms, the use of which can endanger the confidentiality, integrity, and availability of data-at-rest.
		Supports (precedes) PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	Successful demonstrations of quantum-ready algorithm implementations show the feasibility of implementation of alternatives to quantum-vulnerable algorithms, the use of which can endanger the confidentiality, integrity, and availability of data-in-transit.
		PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	Successful demonstrations of quantum-ready algorithm implementations show the feasibility of implementation of alternatives to quantum-vulnerable algorithms, the use of which can endanger the confidentiality, integrity, and availability of data-in-use.
		PR.DS-11: Backups of data are created, protected, maintained, and tested	Successful demonstrations of PQC, quantum-ready algorithm, implementations show the feasibility of implementation of alternatives to quantum-vulnerable algorithms, the use of

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			which can endanger the confidentiality and integrity of data and program backups.
		Is supported by (integral to) PR.PS-01: Configuration management practices are established and applied	Configuration management is necessary to the effectiveness and temporal validity of algorithm implementation interoperability testing and of the temporal validity of algorithm implementation performance testing.
		Is supported by (integral to) PR.PS-05: Installation and execution of unauthorized software are prevented	Continuing accuracy of algorithm implementation performance test results rely on preventing execution of unauthorized software.
		Is supported by (integral to) PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	The integrity of analytic results is dependent on control of access to project facilities and networks. Unauthorized access to programs and processes can result in incorrect interoperability or performance findings.
		Is supported by (integral to) GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	Selection and implementation of protocols including communication protocols, protocol programming interfaces, and identity management protocols are constrained by organizational cybersecurity policies.
Quantum-Ready Cryptographic Service Implementations	Post-quantum crypto implementations and/or implementations of protocols supporting PQC, including communication protocols,	Supports (example of) PR.AA-01: Identities and credentials for	Successful demonstrations of quantum-ready cryptographic service implementations can show the feasibility of implementing alternatives to

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	protocol programming interfaces, and identity management protocols.	authorized users, services, and hardware are managed by the organization	quantum-vulnerable services that employ public-key cryptography in providing credentials for authorized users, services, and hardware.
		Supports (example of) PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	Successful demonstrations of quantum-ready cryptographic service implementations can show the feasibility of implementing alternatives to quantum-vulnerable services that bind identities to credentials using public-key cryptography in post-quantum environments.
		Supports (example of) PR.AA-03: Users, services, and hardware are authenticated	Successful demonstrations of quantum-ready cryptographic service implementations where public-key cryptography is used in authentication processes can show the feasibility of implementing quantum-resistant alternatives to quantum-vulnerable authentication services.
		Supports (example of) PR.AA-04:: Identity assertions are protected, conveyed, and verified	Successful demonstrations of quantum-ready cryptographic service implementations can show the feasibility of implementing alternatives to quantum-vulnerable services that use public-key cryptography in protecting identity assertions.
		Supports (example of) PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and	Successful demonstrations of quantum-ready cryptographic service implementations can show the feasibility of implementing alternatives to quantum-vulnerable services that employ public-key cryptography in enforcing access permissions, entitlements, and authorizations.

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		separation of duties	
		Supports (precedes) PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	Successful demonstration of quantum-ready cryptographic service implementations shows the feasibility of implementation of alternatives to quantum-vulnerable services, the use of which can endanger the confidentiality, integrity, and availability of data-at-rest. Affected services can include programming interfaces, and file encryption, key variable storage, and file encryption.
		Supports (precedes) PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	Successful demonstration of quantum-ready cryptographic service implementations shows the feasibility of implementation of alternatives to quantum-vulnerable services, the use of which can endanger the confidentiality, integrity, and availability of data-in-transit. Affected services can include protocols including communication protocols, key establishment protocols, protocol programming interfaces, and identity management protocols.
		Supports (precedes) PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	Successful demonstration of quantum-ready cryptographic service implementations shows the feasibility of implementation of alternatives to quantum-vulnerable services, the use of which can endanger the confidentiality, integrity, and availability of data-in-use.
		Supports (precedes) PR.DS-11: Backups of data are created, protected,	Successful demonstration of quantum-ready cryptographic service implementations shows the feasibility of implementation of alternatives to quantum-vulnerable services, the use of

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		maintained, and tested	which can endanger the confidentiality and integrity of data and program backups.
		Is supported by (integral to) PR.PS-01: Configuration management practices are established and applied	Configuration management is necessary to the effectiveness and temporal validity of interoperability testing and of the temporal validity of performance testing of quantum-ready cryptographic service implementations.
		Is supported by (integral to) PR.PS-05: Installation and execution of unauthorized software are prevented	Continuing accuracy of cryptographic service implementation performance test results relies on preventing execution of unauthorized software.
		Is supported by (integral to) PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	The integrity of analytic results is dependent on control of access to project facilities and networks. Unauthorized access to programs and processes can result in incorrect interoperability or performance findings.
Quantum-Ready Integration Tools and Application Plugins	Post-quantum and/or post-quantum hybridization-capable integration tools and application plugins for cryptographic toolkits, network infrastructures, security infrastructures (PKI, HSM, blockchain), proxies/connectors, messaging tools, and web application servers and clients.	Is supported by (integral to) GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	Selection and implementation of post-quantum and/or post-quantum hybridization-capable integration tools and application plugins for cryptographic toolkits, network infrastructures, security infrastructures (PKI, HSM, blockchain), proxies/connectors, messaging tools, and web application servers and clients are constrained by organizational cybersecurity policies.
		Supports (example of) PR.AA-01: Identities and	Successful demonstration of quantum-ready integration tools and application plugins can show the feasibility of implementing

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		credentials for authorized users, services, and hardware are managed by the organization	alternatives to quantum-vulnerable cryptography, the use of which can endanger the integrity of identity credentials.
		Supports (example of) PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	Successful demonstration of quantum-ready integration tools and application plugins can show the feasibility of implementing alternatives to quantum-vulnerable cryptography where public-key cryptography is used in protecting the binding of identities to credentials.
		Supports (example of) PR.AA-03: Users, services, and hardware are authenticated	Successful demonstration of quantum-ready integration tools and application plugins can show the feasibility of implementing alternatives to quantum-vulnerable cryptography where public-key cryptography is used in authentication.
		Supports (example of) PR.AA-04: Identity assertions are protected, conveyed, and verified	Successful demonstration of quantum-ready integration tools and application plugins can show the feasibility of implementing alternatives to quantum-vulnerable cryptography where public-key cryptography is used in protecting identity assertions.
		Supports (example of) PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Successful demonstration of quantum-ready integration tools and application plugins can show the feasibility of implementing alternatives to quantum-vulnerable cryptography where public-key cryptography is used in protecting access permissions, entitlements, and authorizations.

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (precedes) PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	Successful demonstration of quantum-ready integration tools and application plugins shows the feasibility of implementation of alternatives to quantum-vulnerable cryptography, the use of which can endanger the confidentiality, integrity, and availability of data-at-rest.
		Supports (precedes) PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	Successful demonstration of quantum-ready integration tools and application plugins shows the feasibility of implementation of alternatives to quantum-vulnerable services, the use of which can endanger the confidentiality, integrity, and availability of data-in-transit.
		PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	Successful demonstration of quantum-ready integration tools and application plugins shows the feasibility of implementation of alternatives to quantum-vulnerable services, the use of which can endanger the confidentiality, integrity, and availability of data-in-use.
		PR.DS-11: Backups of data are created, protected, maintained, and tested	Successful demonstration of quantum-ready integration tools and application plugins shows the feasibility of implementation of alternatives to quantum-vulnerable services, the use of which can endanger the confidentiality and integrity of backups.
		Is supported by (integral to) PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	The integrity of analytic results is dependent on control of access to project facilities and networks. Unauthorized access to programs and processes can result in incorrect interoperability or performance findings.
Quantum-Ready Certificate Authority Implementations	Post-quantum and/or post-quantum hybridization-	Is supported by (integral to)	Selection of post-quantum and/or post-quantum hybridization-

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	enabled X.509 certificate authorities.	GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	enabled X.509 certificate authorities are constrained by organizational cybersecurity policies.
Quantum-Ready Hardware Security Modules (HSMs)	Post-quantum and/or post-quantum hybridization-capable key establishment and storage mechanisms that provide built-in quantum-safe cryptographic functionality.	Is supported by (example of) ID.RA-03: Internal and external threats to the organization are identified and recorded	Identification of internal and external threats to quantum-ready algorithm implementations can inform requirements for and selection of HSMs.
		Supports (example of) PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	Successful demonstration of quantum-ready HSMs shows the feasibility of physically protecting quantum-vulnerable cryptographic information and processes, the compromise of which can endanger the integrity of identity credentials.
		Supports (example of) PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	Successful demonstration of quantum-ready HSMs shows the feasibility of physically protecting quantum-vulnerable information associated with public-key mechanisms used in binding identities to credentials – and potentially the processes themselves.
		Supports (example of) PR.AA-03: Users, services, and hardware are authenticated	Successful demonstration of quantum-ready HSMs shows the feasibility of physically protecting information used in authentication and potentially processes that use that information.

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (example of) PR.AA-04: Identity assertions are protected, conveyed, and verified	Successful demonstration of quantum-ready HSMs shows the feasibility of physically protecting information employed in or by authentication mechanisms.
		Supports (example of) PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Successful demonstration of quantum-ready HSMs shows the feasibility of physically protecting information employed in access and authorization enforcement.
		Supports (precedes) PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	Successful demonstration of quantum-ready HSMs shows the feasibility of physically protecting quantum-vulnerable cryptographic components, the exposure of which can endanger the confidentiality, integrity, and availability of data-at-rest.
		Supports (precedes) PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	Successful demonstration of quantum-ready HSMs shows the feasibility of physically protecting quantum-vulnerable cryptographic information and processes, the exposure of which can endanger the confidentiality, integrity, and availability of data-in-transit.
		PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	Successful demonstration of quantum-ready HSMs shows the feasibility of physically protecting quantum-vulnerable cryptographic information and processes, the exposure of which can endanger the confidentiality,

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			integrity, and availability of data-in-use.
		PR.DS-11: Backups of data are created, protected, maintained, and tested	Successful demonstration of quantum-ready HSMs shows the feasibility of physically protecting quantum-vulnerable cryptographic information and processes, the exposure of which can endanger the confidentiality and integrity of backups.

229

4. SP 800-53 Mapping

Table 2 provides a mapping of tools and products supporting migration to quantum-resistant algorithms to the SP 800-53 controls. It includes both controls that need to be met for secure operation of the tools and controls that the platform supports. As in the case for CSF mappings, note that the current PQC migration project does not involve operational use of cryptographic systems; it only addresses laboratory demonstration and measurement in a controlled environment. As a result, many of the organizational and operational security controls do not apply.

Table 2 Architecture Mapping to NIST Special Publication 800-53

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Discovery and Inventory Tools			
Cryptographic Data Collection Tools	Sensors that are used to scan technologies and systems deployed within a digital footprint for cryptography. Technologies scanned include hosts (for filesystem, binary data, running processes, certificate stores, etc.), network interfaces, CI/CD pipelines, application repositories, key management systems, PKI systems, and HSM systems.	Supports (integral to) CM-8: System Component Inventory	Crypto data collection is integral to developing a cryptographic inventory. The cryptographic data collection tools support identification of cryptographic components, particularly in complex subsystems, systems, and infrastructures.
		Supports (integral to) CM-8: System Component Inventory	
		Supports (precedes) CM-12: Information Location	Discovery of cryptographic components is prerequisite to locating the components.
		Supports (precedes) CP-2 (Enhancement 08): Contingency Plan - Identify critical system assets supporting essential mission and business functions.	Discovery of cryptographic components is necessary for identification of critical cryptographic assets that support essential mission and business functions and inform contingency plan development.

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Cryptographic Inventory Tools	Products that enable an organization to build comprehensive centralized inventories of all cryptographic assets, including cryptographic keys, keystores, X.509 certificates, cryptographic libraries, cryptographic algorithms, and cryptographic protocols deployed across their digital footprint.	Supports (integral to) CM-8: System Component Inventory	Cryptographic inventory tools enable an organization to build comprehensive centralized inventories of all cryptographic assets, including HSMs and cryptographic hardware modules. The inventory is necessary to establishing an understanding of the enterprise's cryptographic components and evaluating the continuing adequacy of the post-quantum cryptographic security services on which the enterprise and its external stakeholders depend.
		Supports (precedes) CP-2 (Enhancement 08): Contingency Plan - Identify critical system assets supporting essential mission and business functions.	Cryptographic inventory tools enable an organization to build comprehensive centralized inventories of all cryptographic assets, including HSMs and cryptographic hardware modules and the mission and business functions that they support. This supports prioritization of replacement of quantum-vulnerable components and contingency planning for response to compromises due to vulnerabilities of remaining legacy cryptography.
Cryptographic Analytics Tools	Products that review a cryptographic inventory and identify cryptographic weaknesses, compliance gaps, and quantum-vulnerable objects based on a policy; provide snapshots of the processing environments by extracting security and cryptographic information based on configurable policies; provide details on keys managed by processors and applications; and help identify insecure keys, algorithms, and enabled services.	Supports (example of) CA-2: Control Assessments	Cryptographic analytics tools can identify cryptographic weaknesses, compliance gaps, or quantum-vulnerable objects, details regarding keys managed by processors and applications, and identification of insecure keys, algorithms, and enabled services. This is necessary for assessment of cryptographic controls.
		Is supported by (precedes) CM-8: System Component Inventory	Cryptographic components must be identified before they can be analyzed.
		Supports (example of) RA-3: Risk Assessment	Cryptographic analytics tools can identify cryptographic vulnerabilities in systems and

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			hosted applications that inform risk assessments.
		Is supported by (example of) RA-3: Risk Assessment	Risk assessment provides the basis for determination of what the cryptographic analytics tools are looking for and for identification and prioritization of vulnerabilities.
		Supports (example of) RA-5: Vulnerability Monitoring and Scanning	Cryptographic analytics tools can identify cryptographic vulnerabilities in systems and hosted applications.
		Supports (example of) RA-7: Risk Response	Analytics results enable response and recovery. For example, inventory of certificates enables certificate replacement and recovery from consequences of vulnerable cryptographic components.
		Supports (example of) SA-11: Developer Testing and Evaluation	Cryptographic analytics tools can support developer testing and evaluation by identifying vulnerable algorithms and cryptographic components.
		Supports (example of) SA-15: Development Process, Standards, and Tools	Cryptographic analytics tools can support system and application development processes by identifying vulnerable algorithms and cryptographic components.
		Supports (example of) SC-8: Transmission Confidentiality and Integrity	Understanding cryptographic weaknesses, compliance gaps, or quantum-vulnerable objects, details regarding keys managed by processors and applications, and identification of insecure keys, algorithms, and enabled services is necessary to understanding the adequacy of the post-quantum cryptographic security services on which external stakeholders depend and the prioritization of migration actions.
		Supports (example of) SC-12: Cryptographic Key Establishment and Management	Understanding instances of use of cryptographic functions for cryptographic key establishment and management supports identification of cases where

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			vulnerable algorithms and key establishment mechanisms are being used or have the potential of being used due to configuration choices. This includes details on keys managed by processors and applications, and help identify insecure keys, algorithms, and enabled services.
		Is supported by (integral to) SC-13: Cryptographic Protection	Cryptographic analytics tools review cryptographic inventories and identify cryptographic weaknesses, compliance gaps, and/or quantum-vulnerable objects based on the organization's cybersecurity policies. The security and cryptographic information extraction processes are based on configurable policies.
		Supports (example of) SC-28: Protection of Information at Rest	Cryptographic analytics tools review cryptographic components used to protect information at rest and identify cryptographic weaknesses, compliance gaps, and/or quantum-vulnerable objects that may compromise that protection.
		Is supported by (example of) SI-7 (Enhancement 06): Software, Firmware, and Information Integrity – Cryptographic Protection	The effectiveness of cryptographic analytics tools in identifying cryptographic weaknesses, compliance gaps, and/or quantum-vulnerable objects that can enable or represent internal or external threats to the organization is dependent on the integrity of the tools and their input data.
Certificate Discovery and Management Tools	Certificate discovery and lifecycle automation tools that provide centralized visibility, governance, and lifecycle automation for digital certificates to identify weak and non-compliant certificates.	Supports (precedes) CM-8: System Component Inventory	Visibility into digital certificates is necessary for inventory purposes since they are critical components of enterprise cryptographic security.
		Supports (example of) CP-2 (Enhancement 08) Contingency Plan – identify Critical Assets	Digital certificates are critical system assets, and discovery and inventory of the certificates is an element of contingency planning for certificate replacement and

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			recovery – particularly in large data center environments.
		Supports (example of) RA-3: Risk Assessment	The tool can provide information on vulnerabilities that are useful for risk assessment purposes.
		Supports (example of) RA-7: Risk Response	Inventory of certificates enables certificate replacement and recovery.
		Is supported by (integral to) SC-17: Public Key Infrastructure Certificates	Certificate discovery and lifecycle automation tools identify weak and non-compliant certificates. Centralized visibility into, governance of, and lifecycle automation for digital certificates to identify weak and non-compliant certificates is necessary to implementation of post-quantum cryptographic security services on which the organization depends.
Post-Quantum Cryptography Implementations			
Quantum-Ready Algorithm Implementations	PQC applications and libraries.	Supports (example of) AC-3: Access Enforcement	Post-quantum cryptographic applications and libraries provide cryptographic mechanisms for access enforcement.
		Is supported by (integral to) CM-1: Configuration Management Policies and Procedures	Configuration management is necessary to the effectiveness and temporal validity of algorithm implementation interoperability testing and of the temporal validity of algorithm implementation performance testing.
		Is supported by (example of) CM-3: Configuration Change Control	Configuration change control supports modifications to and management of cryptographic libraries in establishing and maintaining quantum-resistant capabilities.
		Is supported by (example of) CM-6: Configuration Settings	Management of configuration settings can prevent unintended insecure implementation of PQC applications and libraries.
		Is supported by (precedes) CM-8: System Component Inventory	The component inventory facilitates identification and selection of PQC implementations.

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Is supported by (example of) CM-9: Configuration Management Plan	Implementation of PQC applications and library elements requires management. This includes identifying cryptographic configuration items throughout the system or subsystem development life cycle and managing the configuration of the configuration items. The configuration management plan defines the cryptographic configuration items for the system and places the configuration items under configuration management.
		Supports example of) CM-11: User-Installed Software	Identities of approved software are used to restrict user-installed software.
		Is supported by (example of) CM-11: User-Installed Software	If provided the necessary privileges, users can install cryptographic software in enterprise systems. To support cryptographic security policies and maintain control over the cryptography being installed, the organization needs to identify permitted and prohibited library components and cryptographic applications and actions taken in software installation.
		Is supported by (example of) IA-7: Cryptographic Module Authentication	When using cryptographic applications and library elements, implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.
		Is supported by (example of) RA-3: Risk Assessment	Selection and implementation of cryptographic applications and components are constrained by organizational cybersecurity policies that are informed by risk assessment.
		Supports (integral to) SC-8: Transmission	Successful demonstration of quantum-ready algorithm

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Confidentiality and Integrity	implementations shows the feasibility of implementation of alternatives to quantum-vulnerable algorithms, the use of which can endanger the confidentiality, integrity, and availability of data-in-transit.
		Supports (integral to) SC-12: Cryptographic Key Establishment and Management	Post-quantum cryptographic applications and libraries are used in secure key transport and other methods employed in key establishment.
		Supports (integral to) SC-13: Cryptographic Protection	Post-quantum cryptographic applications and libraries will be needed for many forms of cryptographic protection once quantum computers capable of executing Shor's algorithm become available to adversaries.
		Is supported by (example of) SC-17: Public Key Infrastructure Certificates	Many PQC implementations will require PKI certificates issued by a recognized certificate authority.
		Supports (integral to) SC-28: Protection of Information at Rest	Successful demonstration of quantum-ready algorithm implementations shows the feasibility of implementation of alternatives to quantum-vulnerable algorithms, the use of which can endanger the confidentiality, integrity, and availability of data-at-rest.
		Supports (example of) SC-40: Wireless Link Protection	Post-quantum cryptographic implementations can be used to protect wireless links that may be visible to individuals who are not authorized system users.
		Is supported by (integral to) PR.PS-05: Installation and execution of unauthorized software are prevented	Continuing accuracy of algorithm implementation performance test results relies on preventing execution of unauthorized software.
		Supports (integral to) SI-7: Software, Firmware, and Information Integrity	Quantum-ready cryptographic functions can be used to detect unauthorized changes to software, firmware, and information. Mechanisms include code signing, digital signature of

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			messages, and non-repudiation of transactions.
Quantum-ready Cryptographic Service Implementations	Post-quantum crypto implementations and/or implementations of protocols supporting PQC, including communication protocols, protocol programming interfaces, and identity management protocols.	Is supported by (integral to) CM-1: Configuration Management Policies and Procedures	Configuration management is necessary to the continuing effectiveness of operational implementations but also to the temporal validity of interoperability testing and of the temporal validity of performance testing of quantum-ready cryptographic service implementations.
		Is supported by (example of) IA-9: Service Identification and Authentication	Services that may require identification and authentication include cryptographic services and other applications using digital signatures. Identification and authentication methods for system services and applications include information or code signing, provenance graphs, and electronic signatures that indicate the sources of services.
		Is supported by (example of) RA-3: Risk Assessment	Identification of internal and external threats to quantum-ready algorithm implementations and of use restrictions and potential implementation vulnerabilities can inform cryptographic service selection.
		Is supported by (precedes) SA-2: Allocation of Resources	Service acquisition includes determining the high-level cryptographic security requirements for the quantum-resistant system service in mission and business process planning; determining, documenting, and allocating the resources required to protect the system service as part of the organizational capital planning and investment control process; and establishing a discrete line item for information security and privacy in organizational programming and budgeting documentation.

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Is supported by (integral to) SA-4: Acquisition Process	in the acquisition contract for the secure processing service, include post-quantum security functional requirements; strength of mechanism requirements; security assurance requirements; controls needed to satisfy the security and privacy requirements; security documentation requirements; requirements for protecting security documentation; description of the environment in which the system is intended to operate; and allocation of responsibility or identification of parties responsible for information security and supply chain risk management.
		Is supported by (example of) SA-9: External System Services	External system services are provided by an external provider, and the organization has no direct control over the implementation of the required controls. Require that providers of external system services comply with organizational post-quantum cryptographic security requirements; define and document organizational oversight and user roles and responsibilities associated with external system services; and employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	Successful demonstration of quantum-ready cryptographic service implementations shows the feasibility of implementation of alternatives to quantum-vulnerable services, the use of which can endanger the confidentiality, integrity, and availability of data-in-transit. Affected services can include

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			protocols including communication protocols, key establishment protocols, protocol programming interfaces, and identity management protocols.
		Supports (integral to) SC-13: Protection of Information at Rest	Successful demonstration of quantum-ready cryptographic service implementations shows the feasibility of implementation of alternatives to quantum-vulnerable services use of which can endanger the confidentiality, integrity, and availability of data-at-rest. Affected services can include programming interfaces, key variable storage, and file encryption.
Quantum-ready Integration Tools and Application Plugins	Post-quantum and/or post-quantum hybridization-capable integration tools and application plugins for cryptographic toolkits, network infrastructures, security infrastructures (PKI, HSM, blockchain), proxies/connectors, messaging tools, and web application servers and clients.	Is supported by (example of) AC-3: Access Enforcement	The integrity of analytic results is dependent on control of access to project facilities and networks. Unauthorized access to programs and processes can result in incorrect interoperability or performance findings.
		Is supported by (example of) CM-4: Impact Analysis	Analysis of potential security and privacy impacts prior to installation and implementation of application plugins for cryptographic toolkits, network infrastructures, and security infrastructures can help avoid operational and security failures.
		Is supported by (precedes) CM-5: Access Restrictions for Change	Defining, documenting, approving, and enforcing access restrictions associated with changes to the system discourages unauthorized or erroneous installation of cryptographic application plug-ins.
		Supports (example of) CM-11: User-Installed Software	Identities of approved plug-ins can be used as a basis for restricting user-installed software to an approved set.

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Is supported by (example of) CM-11: User-Installed Software	If provided the necessary privileges, users can install cryptographic plugins in enterprise systems. To support cryptographic security policies and maintain control over the cryptography being installed, the organization needs to identify permitted and prohibited cryptographic applications and plugins.
		Is supported by (example of) RA-3: Risk Assessment	Identification of internal and external threats to quantum-ready algorithm implementations can inform cryptographic tools and application plugin selection.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	Successful demonstration of quantum-ready integration tools and application plugins show the feasibility of implementation of alternatives to quantum-vulnerable services, the use of which can endanger the confidentiality, integrity, and availability of data-in-transit.
		Supports (example of) SC-12: Cryptographic Key Establishment and Management	Quantum-ready application plugins may be used in secure key transport and other methods employed in key establishment.
		Supports (integral to) SC-13: Cryptographic Protection	Post-quantum cryptographic applications and libraries will be needed for many forms of cryptographic protection once quantum computers capable of executing Shor's algorithm become available to adversaries.
		Supports (integral to) SC-28: Protection of Information at Rest	Successful demonstration of quantum-ready integration tools and application plugins show the feasibility of implementation of alternatives to quantum-vulnerable cryptography, the use of which can endanger the confidentiality, integrity, and availability of data-at-rest.
Quantum-ready Certificate Authority Implementations	Post-quantum and/or post quantum hybridization-	Is supported by (example of) CM-3 (Enhancement 06):	Ensure that cryptographic mechanisms are under configuration management. For

Logical Architecture Component (PQC demonstrated capabilities)	Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	enabled X.509 certificate authorities.	Configuration Management – Cryptography Management	example, if system components use certificates for identification and authentication, a process is implemented to address the expiration of those certificates.
		Supports (example of) SC-12: Cryptographic Key Establishment and Management	Quantum-ready certificate authorities are needed to implement secure key establishment in an environment in which quantum computing capable of practically executing Shor's algorithm is available to adversaries.
		Supports (integral to) SC-17: Public Key Infrastructure Certificates	Many PQC implementations will require PKI certificates issued by a recognized certificate authority.
		Supports (example of) SC-23 (Enhancement 05): Session Authenticity – Allowed Certificate Authorities	The organization may restrict the set of certificate authorities that it will accept/use (e.g., a U.S. immigration enforcement organization may not accept certificates from some foreign sources).
Quantum-ready Hardware Security Modules (HSMs)	Post-quantum and/or post-quantum hybridization-capable key establishment and storage mechanisms that provide built-in quantum-safe cryptographic functionality.	Is supported by (example of) RA-3: Risk Assessment	Identification of vulnerabilities to internal and external threats to quantum-ready algorithm implementations can inform requirements for and selection of HSMs.
		Supports (example of) SC-12: Cryptographic Key Establishment and Management	HSMs often perform key establishment functions and provide management support.
		Supports (Example of) SC-28: Protection of Information at Rest	Successful demonstration of quantum-ready HSMs show the feasibility of physically protecting quantum-vulnerable cryptographic components, the exposure of which can endanger the confidentiality, integrity, and availability of data-at-rest.

5. CSF 2.0 Community Profiles

Since the NIST Cybersecurity Framework (CSF) was first released in 2014, the CSF has been used by communities with shared interests in cybersecurity risk management. They developed what CSF 2.0 terms "Community Profiles" to describe how various organizations have used CSF Profiles to develop cybersecurity risk management guidance that applies to multiple organizations and differentiate them from Organizational Profiles that are not shared publicly. A Community Profile can be thought of as guidance for a specific community that is organized around the common taxonomy of the CSF.

The NCCoE has a guide that describes Community Profiles, provides a template and guidance for the content that may be conveyed through a Community Profile, and offers a Community Profile Lifecycle (Plan, Develop, Use, Maintain). Communities can build on the ideas in this guide to create a Community Profile that supports their needs where they share common priorities. Visit https://www.nccoe.nist.gov/projects/guide-creating-community-profiles to see the guide. Visit https://www.nccoe.nist.gov/examples-community-profiles to see a few examples.

For Migration to Post-Quantum Cryptography, we encourage communities to come together to develop a community profile that will allow the community to use consistent language and build relationships to share practices that ease the community's migration to PQC.

One organization has created a cryptographic resilience community profile [5]; your organization could reference that to develop its plan for migration to post-quantum cryptography or quantum readiness efforts to reduce the risk from the threat of a cryptanalytically relevant quantum computer.

References

[1] Barker W, Souppaya M, Newhouse W (2021) Migration to Post-Quantum Cryptography Project Description. (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://csrc.nist.gov/pubs/pd/2021/08/04/migration-to-postquantum-cryptography/final

[2] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[3] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 658 (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[4] Scarfone K, Souppaya M, Fagan M (2024) Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8477. https://csrc.nist.gov/pubs/ir/8477/final

[5] Deloitte (2025) Cryptographic Resilience: A Cyber Security Framework (CSF) 2.0 Community Profile. Available at https://www.deloitte.com/content/dam/assets-shared/docs/services/consulting/2025/deloitte-cryptographic-resilience-community-profile-april-2025.pdf

Appendix A. List of Symbols, Abbreviations, and Acronyms

AA
Identity Management, Authentication, and Access Control

AC
Access Control

AM
Asset Management

CA
Continuous Monitoring

CM
Configuration Management

CP
Contingency Planning

CSF
Cybersecurity Framework

CSWP
Cybersecurity White Paper

DS
Data Security

GV
Govern

HSM
Hardware Security Module

IA
Identification and Authentication

IR
Technology Infrastructure Resilience

ID
Identify

IETF
Internet Engineering Task Force

NCCoE
National Cybersecurity Center of Excellence

NIST
National Institute of Standards and Technology

NIST IR
NIST Interagency Report

PO
Policy

PQC
Post-Quantum Cryptography

PR
Protect

PS
Platform Security

RA
Risk Assessment

SA
System and Services Acquisition

SC
System and Communication Protection

SI
System and Information Integrity

SP
Special Publication

SSH
Secure Shell

TLS
Transport Layer Security