

Session VII – NIST 6th PQC Standardization Conference

NIST Cybersecurity Whitepaper 39 Considerations for Achieving Cryptographic Agility: Strategies and Practices

NIST National Cybersecurity Center of Excellence Migration to Post-Quantum Cryptography Project

NIST Cybersecurity White Paper 39: Considerations for Achieving Cryptographic Agility: Strategies and Practices (2nd Public Draft)

Cryptographic (crypto) agility describes the capabilities needed to replace and adapt cryptographic algorithms for protocols, applications, software, hardware, and infrastructures without interrupting the flow of a running system in order to achieve resiliency.

Public Comment Period Ended August 15, 2025

2025 April Online Workshop after 1st draft - <https://csrc.nist.gov/events/2025/crypto-agility-workshop> - session videos posted (worth a watch)

Updated CSWP Draft to be published this fall.

Crypto Agility Paper Timeline

April 2024

Initial Discussions and Presentations from **NIST NCCoE PQC Migration Project Collaborators** from over 40 different organizations

August 2024

One-on-One Discussion with Various Collaborators on Specific Topics (e.g, Hardware)

April 2025

NIST Workshop on Crypto Agility with Presentations and Panels from 32 different organizations

Fall 2025

Will Publish **Final Version of CSWP 39** Informed by Comments Received for the Second Draft

Draft Outline of a White Paper Informed by Discussion with Collaborators

June 2024

Published **CSWP 39 Considerations for Achieving Cryptographic Agility: Strategies and Practices Initial Draft** Informed by All Previous Discussions for Public Comment

March 2025

Published **CSWP 39 Second Draft** Informed by the Workshop Discussions and Written Feedback for Another Round of Public Comment

July 2025

CSWP 39 Considerations for Achieving Cryptographic Agility: Strategies and Practices

NIST Cybersecurity White Paper
NIST CSWP 39

Considerations for Achieving Crypto Agility

Strategies and Practices

Elaine Barker*
Lily Chen

David Cooper*

Dustin Moody

Andrew Regenscheid

Murugiah Souppaya

Computer Security Division

Information Technology Laboratory

Bill Newhouse

Applied Cybersecurity Division

Information Technology Laboratory

Russ Housley
Vigil Security

Sean Turner
sn3rd

William Barker
Dakota Consulting

Karen Scarfone
Scarfone Cybersecurity

**Former NIST employee; all work for this publication was done while at NIST.*

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.CSWP.39.2pd>

Fall 2025

- Provide in-depth survey of current approaches for achieving crypto agility and discusses their challenges and trade-offs
- Present crypto agility considerations in technical detail and may be of interest to protocol designers, implementers, operators, IT and cybersecurity architects, software and standards developers, and hardware designers
- Examine strategic planning for crypto agility, which should be beneficial for organizational risk management, governance, and policy professionals
- Assist with development of a comprehensive strategic and tactical plan that integrates crypto agility into the organization's overall risk management framework, ensuring that employees, business partners, and technology suppliers involved in cryptographic design, implementation, acquisition, deployment, and use consider and adopt these practices

CSWP 39 Considerations for Achieving Cryptographic Agility: Strategies and Practices

Executive Summary

1. Introduction

2. Historic Transitions and Challenges

2.1. Long Period for a Transition

2.2. Backward Compatibility and Interoperability Challenges

2.3. Constant Needs of Transition

2.4. Resource and Performance Challenges

3. Crypto Agility for Security Protocols

3.1. Algorithm Identification

3.1.1. Mandatory-to-Implement Algorithms

3.1.2. Dependent Specifications

3.2. Algorithm Transitions

3.2.1. Preserving Protocol Interoperability

3.2.2. Providing Notices of Expected Changes

3.2.3. Integrity for Algorithm Negotiation

3.2.4. Hybrid Cryptographic Algorithms

3.3. Cryptographic Key Establishment

3.4. Balancing Security Strength and Protocol Complexity

3.4.1. Balancing the Security Strength of Algorithms in a Cipher Suite

3.4.2. Balancing Protocol Complexity

4. Crypto Agility in System Implementations

4.1. Using an API in a Crypto Library Application

4.2. Using APIs in the Operating System Kernel

4.3. Using Service Mesh in Cloud Native Environments

4.4. Embedded Systems

4.5. Hardware

4.6. Using Crypto-Gateway for Legacy Systems

5. Crypto Agility Strategic Plan for Managing Organizations' Crypto Risks

5.1. Cryptographic Standards, Regulations, and Mandates

5.2. Crypto Security Policy Enforcement

5.3. Technology Supply Chains

5.4. Cryptographic Architecture

6. Considerations for Future Works

6.1. Resource Considerations

6.2. Agility-Aware Design

6.3. Complexity and Security

6.4. Crypto Agility in the Cloud

6.5. Maturity Assessment for Crypto Agility

6.6. Common Crypto API

7. Conclusion

References

Appendix A. List of Symbols, Abbreviations, and Acronyms

Appendix B. Definition of Crypto Agility in Other Literature

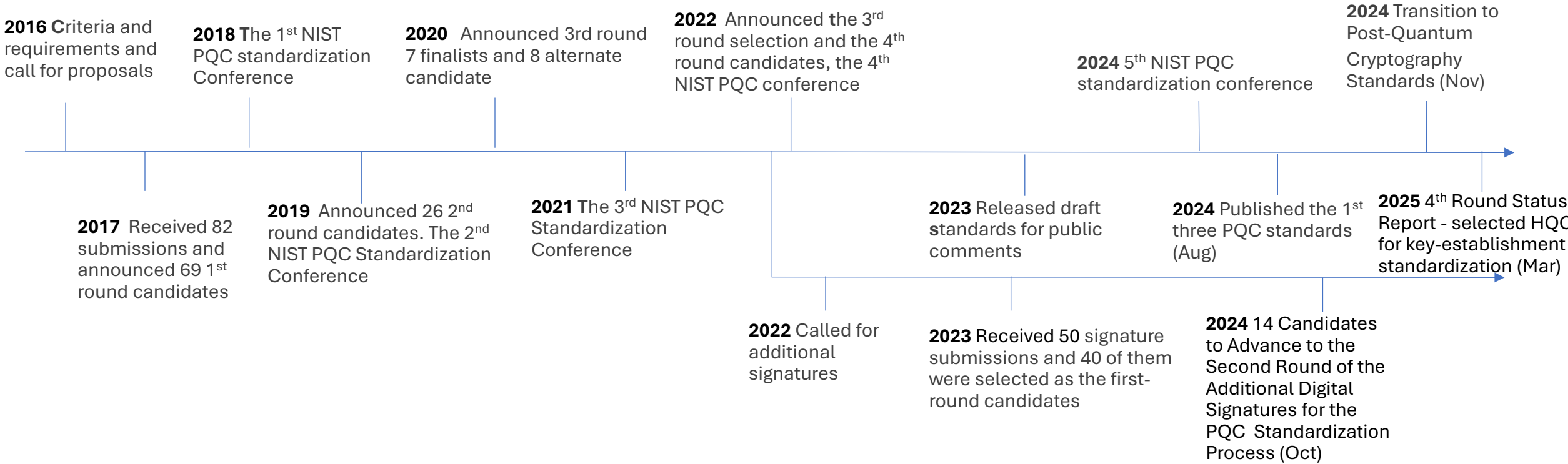
Crypto Agility References

- **NIST CSWP 39 (Initial Draft) Considerations for Achieving Cryptographic Agility: Strategies and Practices**
<https://csrc.nist.gov/pubs/cswp/39/considerations-for-achieving-cryptographic-agility/ipd>
- **NIST CSWP 39 (2nd Public Draft) Considerations for Achieving Cryptographic Agility: Strategies and Practices**
<https://csrc.nist.gov/pubs/cswp/39/considerations-for-achieving-cryptographic-agility/2pd>
- **Crypto Agility Workshop**
<https://csrc.nist.gov/Events/2025/crypto-agility-workshop>
- **NIST NCCoE PQC Migration Project**
<https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms>

Post Quantum Cryptography Milestones and Timeline



POST-QUANTUM CRYPTOGRAPHY Standardization



NIST NCCOE Migration to POST-QUANTUM CRYPTOGRAPHY Project

The development of practices to ease migration from the current set of public-key cryptographic algorithms to standardized PQC algorithms that are resistant to quantum computer-based attacks



NIST Post-Quantum Cryptography Standards

- **NIST Standards – Federal Information Processing Standards (FIPS) for PQC**
 - FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)* (Approved August 2024)
 - FIPS 204, *Module-Lattice-Based Digital Signature Standard (ML-DSA)* (Approved August 2024)
 - FIPS 205, *Stateless Hash-Based Digital Signature Standard (SLH-DSA)* (Approved August 2024)
 - Fourth PQC Standard, FIPS 206, *FFT over NTRU-Lattice-Based Digital Signature Algorithm* (draft expected soon)
- **Ongoing public evaluation of additional algorithms continues**
 - *Key Encapsulation Mechanisms*: HQC (non-lattice, code-based) KEM selected for standardization to complement ML-KEM announced March 11, 2025
 - *Digital Signature Algorithms*: 14 2nd round candidates announced October 24, 2024
- **International/Industry Standards**
 - ISO/IEC: ML-KEM including in SC27 WG2 standard under development with other PQC KEMs
 - IETF: Critical network protocols, including TLS and IPsec, being revised to support NIST PQC algorithms
 - 3GPP: Cellular Technology Specifications including 5G and 6G being defined to support PQC algorithms
 - EU: Coordinating through TTC and with individual EU member state IT security authorities
- **NIST to provide transition guidelines for the PQC standards**
 - National Security Memorandum (NSM) 10: “*within 90 days of the PQC standards, NIST shall release a proposed timeline for the deprecation of quantum-vulnerable cryptography in standards*”
 - [NCCoE Migration to PQC](#) project to accelerate adoption of quantum-resistant algorithms

The NCCoE – Migration to PQC project - An applied Research Project



- Complement NIST PQC standardization effort
 - Support **US Government PQC initiatives** (White House NSM-10, Memo M-23-02, June 2025 Cybersecurity Executive Order)
 - Tackle challenges with **adoption, implementation, and deployment** of PQC
 - Engage with the community including **industry collaborators and across government** to bring **awareness and education** to the issues involved in migrating to post-quantum algorithms
 - Coordinate with **standard developing organizations** and government and industry sectors community to develop guidance to accelerate the migration
- **Leverage automated tools to discover use of quantum vulnerable cryptography within an organization in hardware, firmware, software, protocols, and services and use a risk-based approach to prioritize their replacement**
 - Perform **interoperability and performance demonstrations** across different technology and protocols to include **TLS, QUIC, SSH, code signing, public key certificates, hardware security modules, etc.**

The fact sheet is titled "MIGRATION TO POST-QUANTUM CRYPTOGRAPHY" and is published by NIST and NCCoE. It provides an overview of the project, including its goals, background, challenges, and benefits. The document is structured with clear headings and bullet points, and includes a QR code and contact information for further details.

MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

The National Cybersecurity Center of Excellence (NCCoE) is collaborating with stakeholders in the public and private sectors to bring awareness to the challenges involved in migrating from the current set of public-key cryptographic algorithms to quantum-resistant algorithms. This fact sheet provides an overview of the Migration to Post-Quantum Cryptography project, including background, goal, challenges, and potential benefits.

BACKGROUND

The advent of quantum computing technology will render many of the current cryptographic algorithms ineffective, especially public-key cryptography, which is widely used to protect digital information. Most algorithms in which we depend are used worldwide in components of many different communications, processing, and storage systems. Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to adversaries. It is essential to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

GOAL

The initial scope of this project will include engaging industry to demonstrate the use of automated discovery tools to identify instances of quantum-vulnerable public-key algorithm use, where they are used in dependent systems, and for what purposes. Once the public-key cryptography components and associated assets in the enterprise are identified, the next project element is prioritizing those applications that need to be considered first in migration planning. Finally, the project will describe systematic approaches for migrating from vulnerable algorithms to quantum-resistant algorithms across different types of organizations, assets, and supporting technologies.

CHALLENGES

- Organizations are often unaware of the breadth and scope of application and function dependencies on public-key cryptography.
- Many, or most, of the cryptographic products, protocols, and services on which we depend will need to be replaced or significantly altered when post-quantum replacements become available. Information systems are not typically designed to encourage supporting rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure—requiring intense manual effort.
- The migration to post-quantum cryptography will likely create many operational challenges for organizations. The new algorithms may not have the same performance or reliability characteristics as legacy algorithms due to differences in key size, signature size, error handling properties, number of execution steps required to perform the algorithm, key establishment process complexity, etc. A truly significant challenge will be to maintain connectivity and interoperability among organizations and organizational elements during the transition from quantum-vulnerable algorithms to quantum-resistant algorithms.


BENEFITS

The potential business benefits of the solution explored by this project include:

- helping organizations identify where, and how, public-key algorithms are being used on their information systems
- mitigating enterprise risk by providing tools, guidelines, and practices that can be used by organizations in planning for replacement/updating hardware, software, and services that use PQC-vulnerable public-key algorithms
- protecting the confidentiality and integrity of sensitive enterprise data
- supporting developers of products that use PQC-vulnerable public-key cryptographic algorithms to help them understand protocols and constraints that may affect use of their products

DOWNLOAD PROJECT DESCRIPTION

This fact sheet provides a high-level overview of the project. To learn more, visit the project page: <https://www.nccoe.nist.gov/crypto-ability-considerations/migrating-post-quantum-cryptographic-algorithms>



HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or would like to join the project's Community of Interest, please email applied.crypto-pqc@nist.gov.

Migration to PQC Project Collaborators



- Amazon Web Services, Inc.
- ATIS
- AvinyaSQ
- Cisco Systems, Inc.
- Cloudflare, Inc.
- Comcast
- Crypto4A Technologies, Inc.
- CryptoNext Security
- Cyberzero
- US Gov't: Cybersecurity and Infrastructure Security Agency
- Data-Warehouse GbmH
- Dell Technologies
- DigiCert
- Entrust
- GDIT
- Google
- HP, Inc.
- HSBC
- IDEMIA Secure Transactions
- IBM
- Information Security Corporation
- InfoSec Global
- ISARA Corporation
- JPMorgan Chase Bank, N.A.
- Keyfactor
- Kudelski IoT
- M&T Bank
- Microsoft
- US Gov't: NSA
- NTT Data
- NXP Semiconductors
- Palo Alto Networks
- Post-Quantum
- PQSecure
- PQShield
- QuantumXChange
- Qinvicta
- SafeLogic, Inc.
- Samsung SDS Co., Ltd.
- SandboxAQ
- Santander
- SEALSQ
- Siemens
- SSH Communications Security Corp
- SWIFT
- Thales DIS CPL USA, Inc.
- Thales Trusted Cyber Technologies
- Tychon
- U.S. Army DEVCOM C5ISR Ctr
- Utimaco
- Verizon
- Wells Fargo
- wolfSSL

Initial Public Draft NIST SP 1800-38B (Dec 2023) *Quantum Readiness: Cryptographic Discovery*

- Demonstration of collaborator cryptographic discovery and inventory tools

Initial Public Draft NIST SP 1800-38C (Dec 2023) *Quantum Readiness: Testing Draft and Final Standards for Interoperability and Performance*

- Explore interoperability issues in a controlled, non-production environment
- Reduction of time spent by individual organizations performing similar interoperability testing for their own PQC migration efforts

Frequently Asked Questions (July 2025)

- <https://pages.nist.gov/nccoe-migration-post-quantum-cryptography/FAQ/index.html>



NIST SPECIAL PUBLICATION 1800-38B
*Migration to Post-Quantum Cryptography
Quantum Readiness: Cryptographic Discovery*

Volume B:
Approach, Architecture, and Implementation

William Newhouse
Murugiah Souppaya
National Institute of Standards and Technology
Rockville, Maryland

William Barker
Dakota Consulting
Silver Spring, Maryland

Chris Brown
The MITRE Corporation
McLean, Virginia

Panos Kampanakis
Amazon Web Services (AWS)
Arlington, Virginia

Marc Manzano
SandboxAQ
Palo Alto, California

December 2023
PRELIMINARY DRAFT

This publication is available free of charge from <https://www.nccoe.nist.gov>

NIST

NIST SPECIAL PUBLICATION 1800-38C
*Migration to Post-Quantum Cryptography
Quantum Readiness: Testing Draft Standards*

Volume C:
Quantum-Resistant Cryptography Technology Interoperability and Performance Report

William Newhouse Murugiah Souppaya National Institute of Standards and Technology Rockville, Maryland	Julien Prat Robin Larrieu CryptoNext Security Paris, France	Robert Burns Thales DIS CPL USA, Inc. Austin, Texas
William Barker Dakota Consulting Silver Spring, Maryland	John Gray Mike Ounsworth Cleandro Viana Entrust Minneapolis, Minnesota	Christian Paquin Microsoft Redmond, Washington
Chris Brown The MITRE Corporation McLean, Virginia	Hubert Le Van Gong JPMorgan Chase Bank, N.A. Jersey City, New Jersey	Jane Gilbert Gina Scinta Thales Trusted Cyber Technologies Abingdon, MD
Panos Kampanakis Amazon Web Services, Inc. (AWS) Arlington, Virginia	Kris Kwiatkowski PQShield Oxford, United Kingdom	Eunhyung Kim Samsung SDS Co., Ltd. Seoul, Republic of South Korea
Jim Goodman Crypto4A Technologies, Inc. Ontario, Canada	Anthony Hu wolfSSL Seattle, Washington	Volker Krummel Ultimeco Nordrhein-Westfalen, Germany

December 2023
PRELIMINARY DRAFT

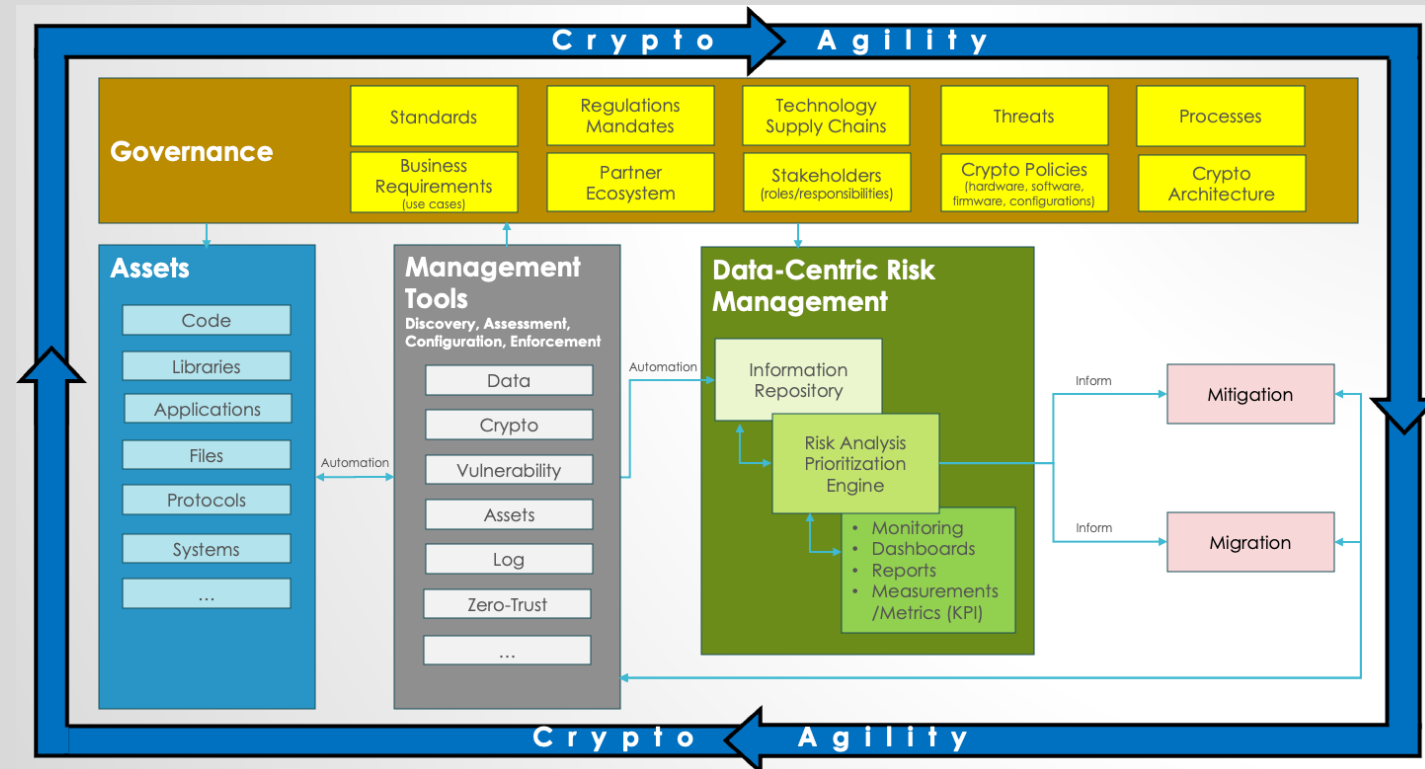
This publication is available free of charge from <https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms>

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

WORKSTREAMS -

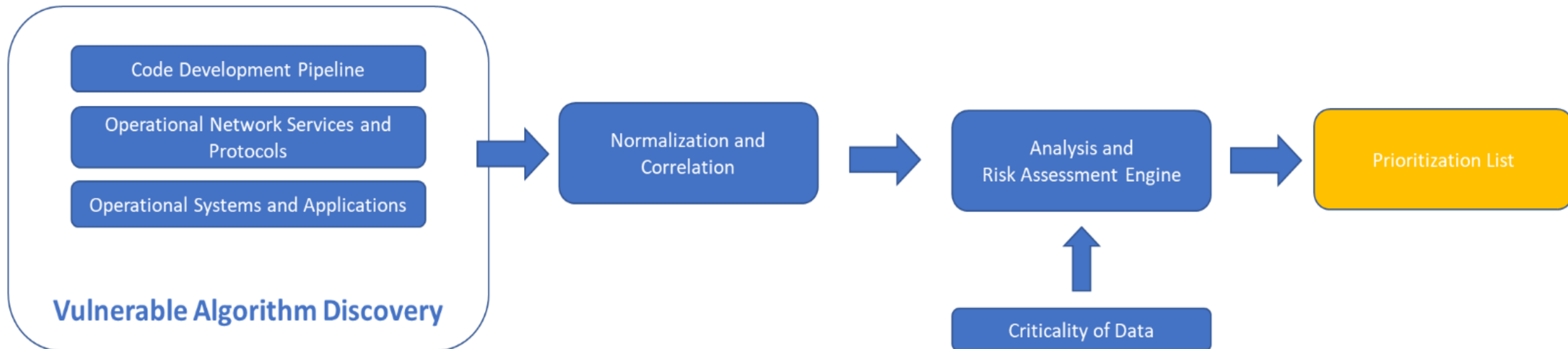
- Interop Demonstrations with PQC standards
- Internet Communication Protocols, HSMs
- Public Key Infrastructures
 - Smart Card- chip-based payment cards/chip-based payment cards...

Data centric risk management to prioritize mitigation and migration with crypto agility

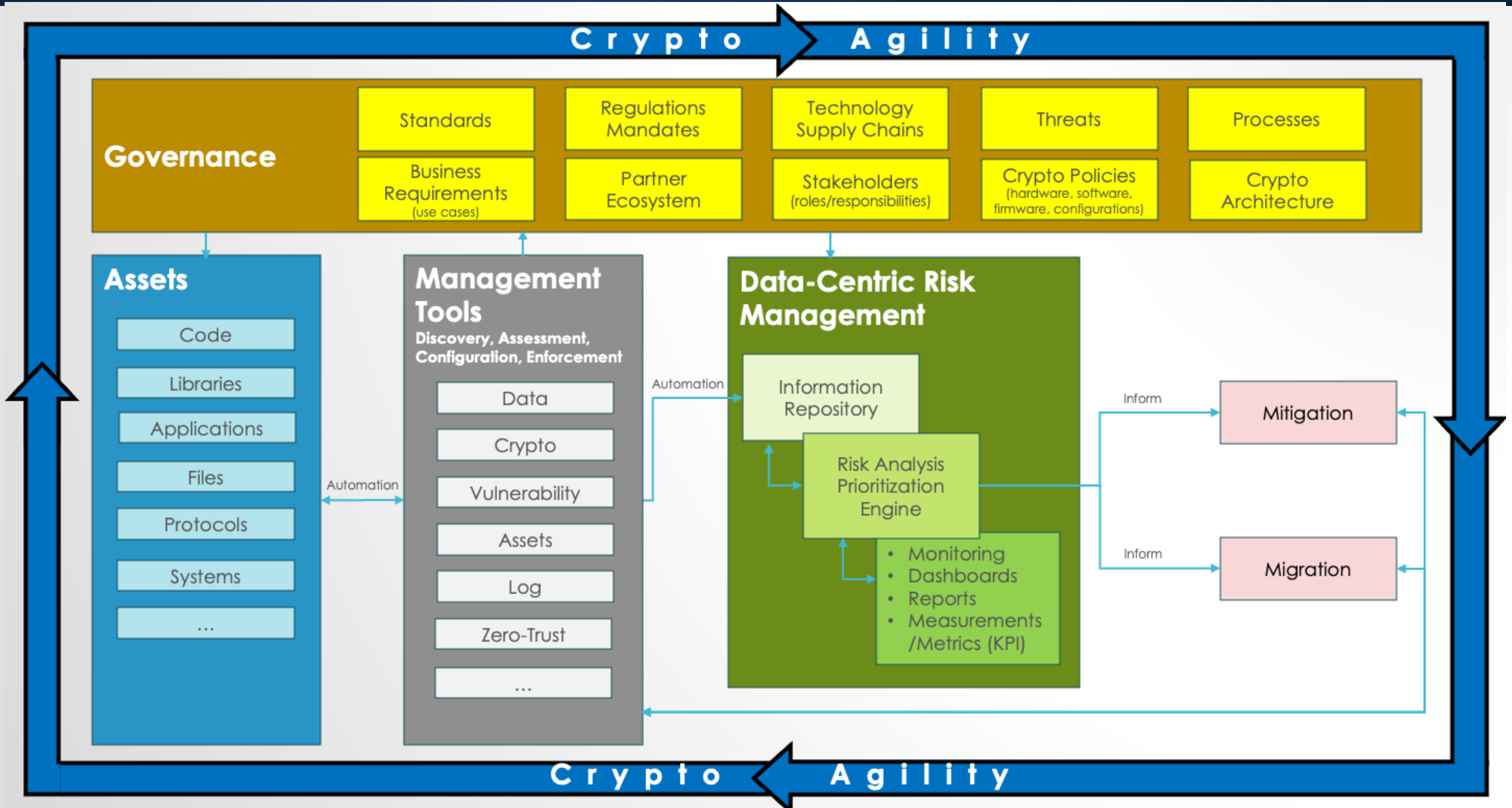


Migration to Post-Quantum Cryptography Discovery Workstream

- Exploring the use of discovery tools to detect and report the presence and use of quantum vulnerable (and quantum resistant) cryptography in systems and services
- Use of output from the tools to inform risk analysis for prioritizing actions to implement quantum-resistant cryptography



DATA CENTRIC CRYPTO RISK MANAGEMENT APPROACH



MIGRATION TO PQC

CAPABILITIES MAPPED TO CSF AND 800-53



NIST Cybersecurity White Paper 48: 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)**

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.

Public Comment Period Ends October 20, 2025

<https://csrc.nist.gov/pubs/cswp/48/mapping-migration-to-pqc-project-capabilities-to-r/ipd>

NIST AND NCCOE URLS AND EMAILS

- NCCoE Migration to PQC Project website
 - <https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms>
- NCCoE Migration to PQC Project Community of Interest (COI)
 - Request to Join Email: applied-crypto-pqc@nist.gov
- Email for NCCoE Migration to PQC project team
 - applied-crypto-pqc@nist.gov
- NIST Post-Quantum Cryptography
 - <https://csrc.nist.gov/Projects/post-quantum-cryptography>
- Post-Quantum Cryptography Technical Inquiries
 - pqc-comments@nist.gov