

Post-Quantum

Cryptography Conference

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

As organizations prepare for the transition to post-quantum cryptography (PQC), the NIST National Cybersecurity Center of Excellence (NCCoE) and its industry collaborators are researching practical approaches for migration to standardized post-quantum cryptography. This presentation by Bill Newhouse, Cybersecurity Engineer and Project Lead at NCCoE, will focus on what the collaboration has learned as it has explored cryptographic discovery and inventory tools and the interoperability of the PQC algorithms being standardized by NIST in the communication protocols and systems that rely on public-key encryption. The session will explore the real-world challenges of transitioning to PQC enabling organizations to safeguard their critical systems against quantum threats. The presentation will highlight NIST Special Publication 1800-38 which is being used to document the insights and findings of this collaborative project.



Bill Newhouse

Cybersecurity Engineer & Project Lead, National Cybersecurity Center of Excellence (NCCoE) at NIST



KEYFACTOR



January 15 and 16, 2025 - Austin, TX (US) | Online

PKI Consortium Inc. is registered as a 501(c)(6) non-profit entity ("business league") under Utah law (10462204-0140) | pkic.org



PKI
Consortium

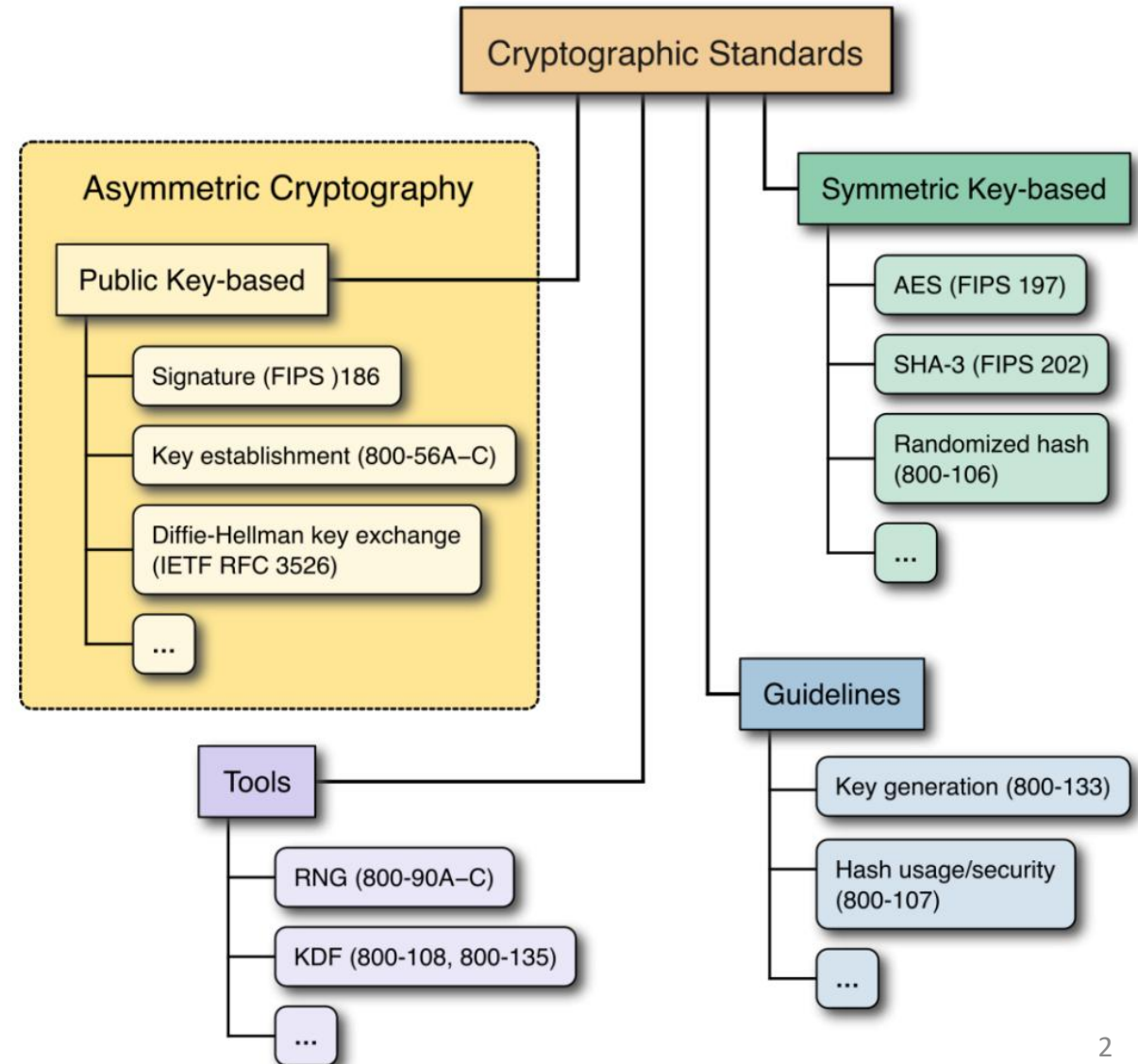
Updates on the Migration to Post-Quantum Cryptography Project

Bill Newhouse – NCCoE Cybersecurity Engineer
william.newhouse@nist.gov

January 16, 2024

Need for Post-Quantum Cryptography (PQC)

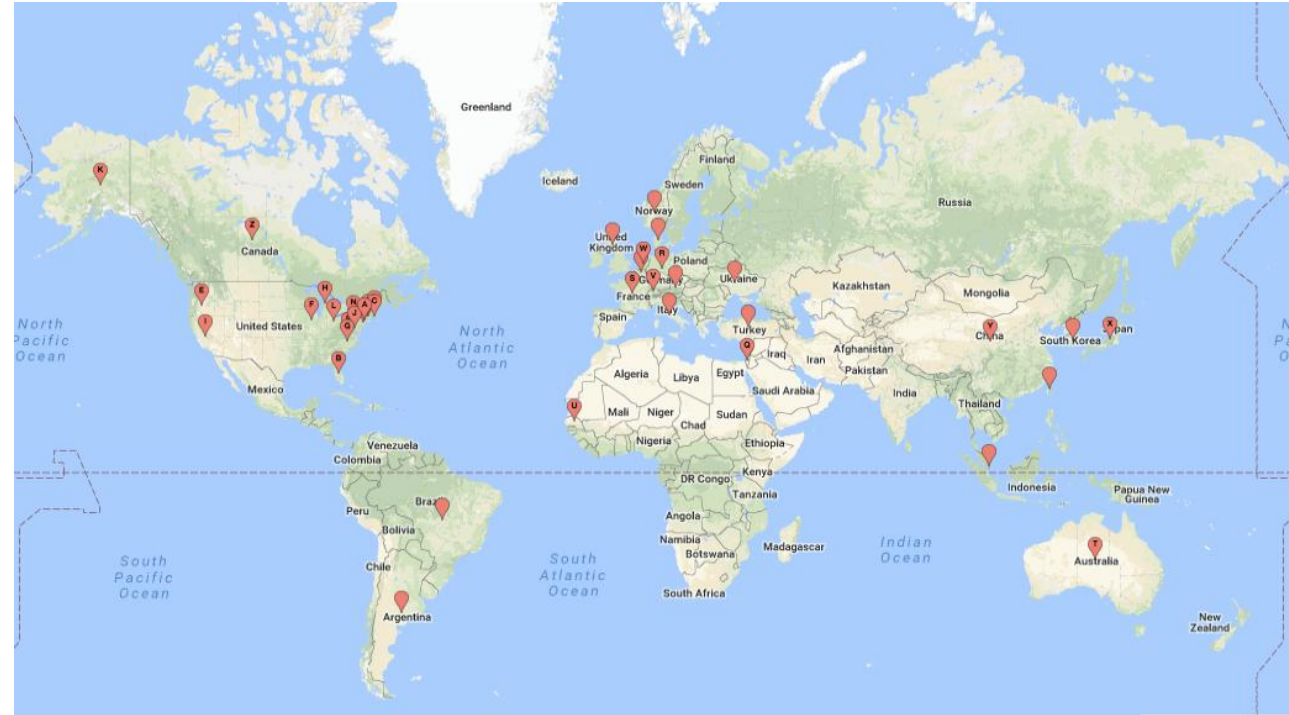
- **Quantum computers threaten the security of current, widely-deployed public key cryptosystems**
 - *Signatures*– ECDSA, RSA
 - *Key Establishment*–Diffie-Hellman, RSA
- Quantum computers changed what we have believed about the hardness
 - By Shor’s algorithm, factorization and discrete logarithm problems can be solved by quantum computers in polynomial time
- Quantum computing also impacts security strength of symmetric key based cryptography algorithms – manageable by increasing key size
 - Grover’s algorithm provides quadratic speedup



NIST PQC Standardization – Milestones and Timeline



- 2010 – 2015** – NIST PQC project team builds & First PQC Conference
- 2015** – [Workshop on Cybersecurity in a Post-Quantum World](#)
- 2016** – Determined criteria and requirements, [Call for proposals](#)
- 2017** – Received 82 submissions, **69 First Round candidates**
- 2018** – [1st NIST PQC Standardization Conference](#)
- 2019** – Announced **26 Second Round candidates**
Released [NIST IR 8240](#)
[2nd NIST PQC Standardization Conference](#)
- 2020** – Announced **7 finalists & 8 alternate candidates**
Released [NIST IR 8309](#)
- 2021** – [3rd NIST PQC Standardization Conference](#)
Released [NIST IR 8413](#)
- 2022** – **Announced Initial Selections for Standardization & 4th Round Candidates**
[4th NIST PQC Standardization Conference](#)
- 2023** – [Release draft standards and call for public comments](#)
- 2024** – [5th NIST PQC Standardization Conference](#)
Approval of 3 Federal Information Processing Standards ([FIPS](#)) for Post-Quantum Cryptography (August)
[NIST IR 8528](#) Status Report 1st Round of the Additional Digital Signature Schemes
[NIST IR 8547](#) Transition to Post-Quantum Cryptography Standards (Initial Public Draft)



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* (still under development)
- **Ongoing public evaluation of additional algorithms continues**
 - *Key Encapsulation Mechanisms*: One or two (non-lattice) KEMs to be selected for standardization to complement ML-KEM
 - BIKE, Classic McEliece, HQC – all based on code-based cryptography
 - *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
 - 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

Milestones and Timeline



NIST POST-QUANTUM CRYPTOGRAPHIC Standardization

2016 Criteria and requirements and call for proposals

2018 The 1st NIST PQC standardization Conference

2020 Announced 3rd round 7 finalists and 8 alternate candidate

2022 Announced the 3rd round selection and the 4th round candidates, the 4th NIST PQC conference

2024 5th NIST PQC standardization conference

2017 Received 82 submissions and announced 69 1st round candidates

2019 Announced 26 2nd round candidates. The 2nd NIST PQC Standardization Conference

2021 The 3rd NIST PQC Standardization Conference

2023 Released draft standards for public comments

2024 Published the 1st three PQC standards (Aug 2024)

2022 Called for additional signatures

2023 Received 50 signature submissions and 40 of them were selected as the first-round candidates

2024 14 Candidates to Advance to the Second Round of the Additional Digital Signatures for the PQC Standardization Process

2021 NCCoE begins Migration to Post-Quantum Cryptography Project calling for collaborators (Oct)

2022 Kickoff with 14 CRADA Collaborators (July)

2023 Published initial public drafts for discovery and interoperability/performance workstreams (Dec)

2024 Demonstrating how to use inventory for prioritization decisions, expanding interoperability and performance testing into additional communication protocols (over 40 collaborators)

NCCoE Migration to Post Quantum Cryptography Project
Practices to ease migration from the current set of public-key cryptographic algorithms to NIST standardized PQC algorithms



The NCCoE – Migration to PQC - AN applied Research Project



- Complement NIST PQC standardization effort
- Support **US Government PQC initiatives** (White House NSM-10, M-23-02, '23 National Cybersecurity Strategy)
- 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.**

A fact sheet titled "MIGRATION TO POST-QUANTUM CRYPTOGRAPHY" from NIST and NCCoE. The document is structured with sections: BACKGROUND, CHALLENGES, GOAL, and BENEFITS. It provides an overview of the project, including background, goal, challenges, and potential benefits. At the bottom, there are sections for "DOWNLOAD PROJECT DESCRIPTION" and "HOW TO PARTICIPATE".

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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 on 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.

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.

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.

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-agility-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
- Cisco Systems, Inc.
- Comcast
- Crypto4A Technologies, Inc.
- CryptoNext Security
- Federal: Cybersecurity and Infrastructure Security Agency (CISA)
- Data-Warehouse GbmH
- Dell Technologies
- DigiCert
- Entrust
- GDIT
- Gutsy
- HP, Inc.
- HSBC
- IDEMIA Secure Transactions
- IBM
- Information Security Corporation
- InfoSec Global
- ISARA Corporation
- JPMorgan Chase Bank, N.A.
- Keyfactor
- Kudelski IoT
- Microsoft
- M&T Bank
- Federal: National Security Agency (NSA)
- NXP Semiconductors
- Palo Alto Networks
- Post-Quantum
- PQShield
- QuantumXChange
- SafeLogic, Inc.
- Samsung SDS Co., Ltd.
- SandboxAQ
- Santander
- Siemens
- SSH Communications Security Corp
- Thales DIS CPL USA, Inc.
- Thales Trusted Cyber Technologies
- Utimaco
- Verizon
- Wells Fargo
- wolfSSL

Moving volumes into one NIST Special Publication 1800-38 to be hosted on pages.nist.gov

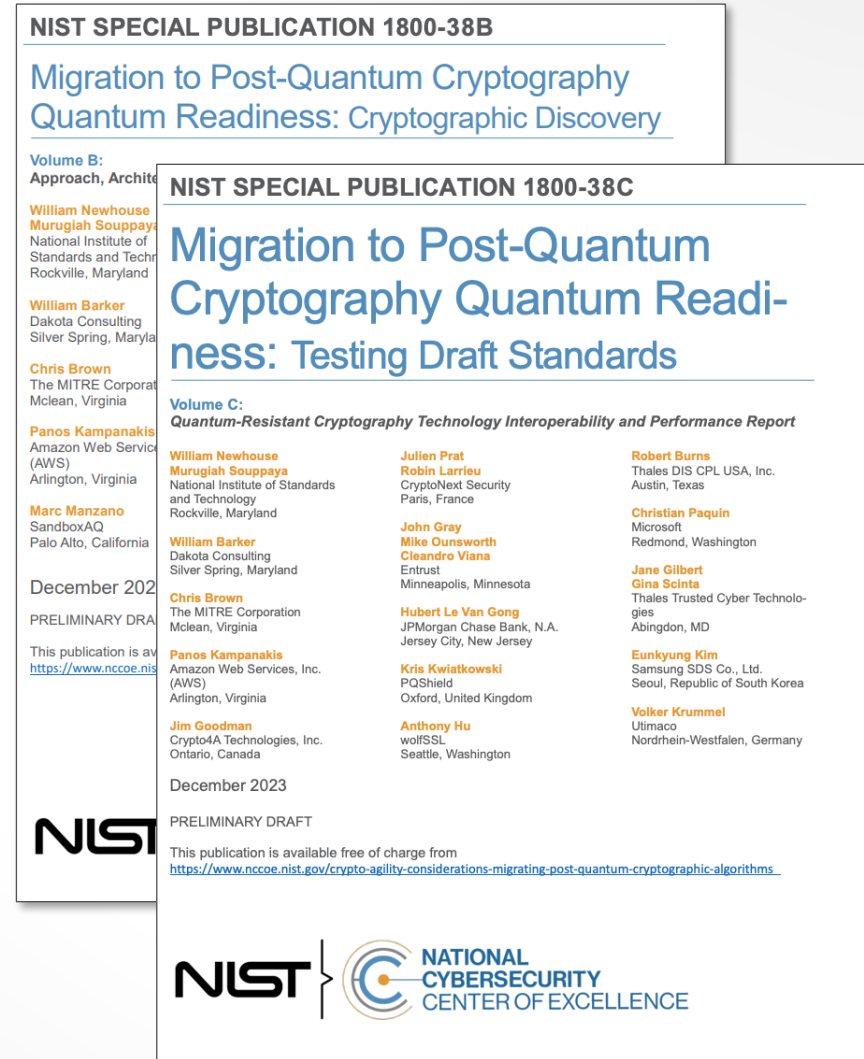
- Example: NIST SP 1800-35 <https://pages.nist.gov/zero-trust-architecture/>

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



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>

Julien Prat
Robin Larrieu
CryptoNext Security
Paris, France

John Gray
Mike Ounsworth
Cleandro Viana
Entrust
Minneapolis, Minnesota

Hubert Le Van Gong
JPMorgan Chase Bank, N.A.
Jersey City, New Jersey

Kris Kwiatkowski
PQShield
Oxford, United Kingdom

Anthony Hu
wolfSSL
Seattle, Washington

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>


Robert Burns
Thales DIS CPL USA, Inc.
Austin, Texas

Christian Paquin
Microsoft
Redmond, Washington

Jane Gilbert
Gina Scinta
Thales Trusted Cyber Technologies
Abingdon, MD

Eunkyoung Kim
Samsung SDS Co., Ltd.
Seoul, Republic of South Korea

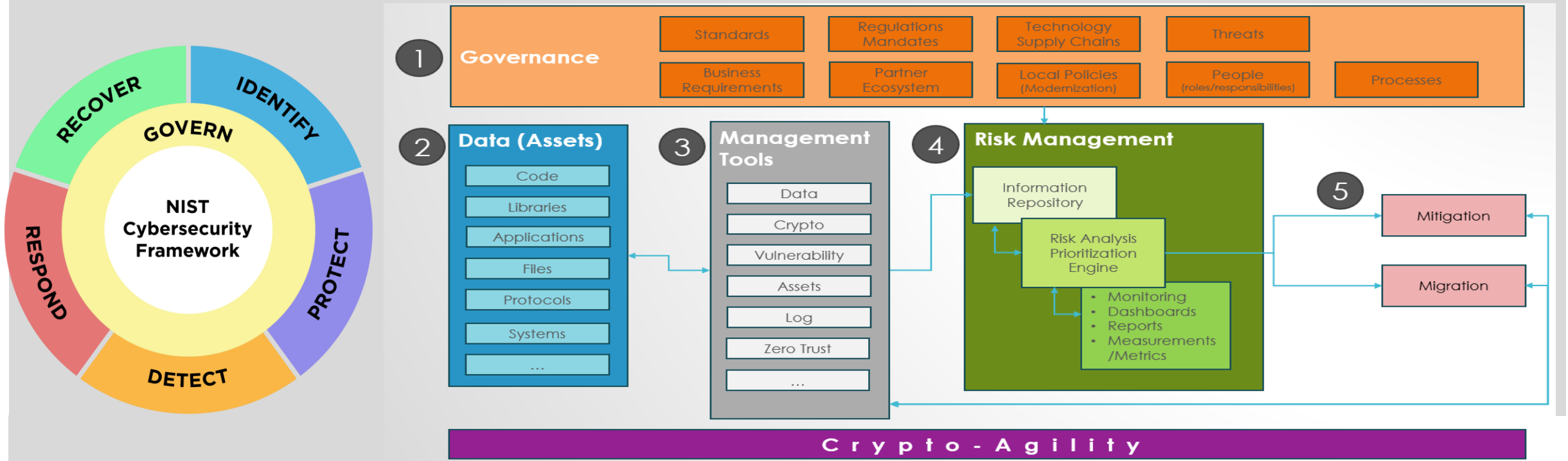
Volker Krummel
Ultimaco
Nordrhein-Westfalen, Germany



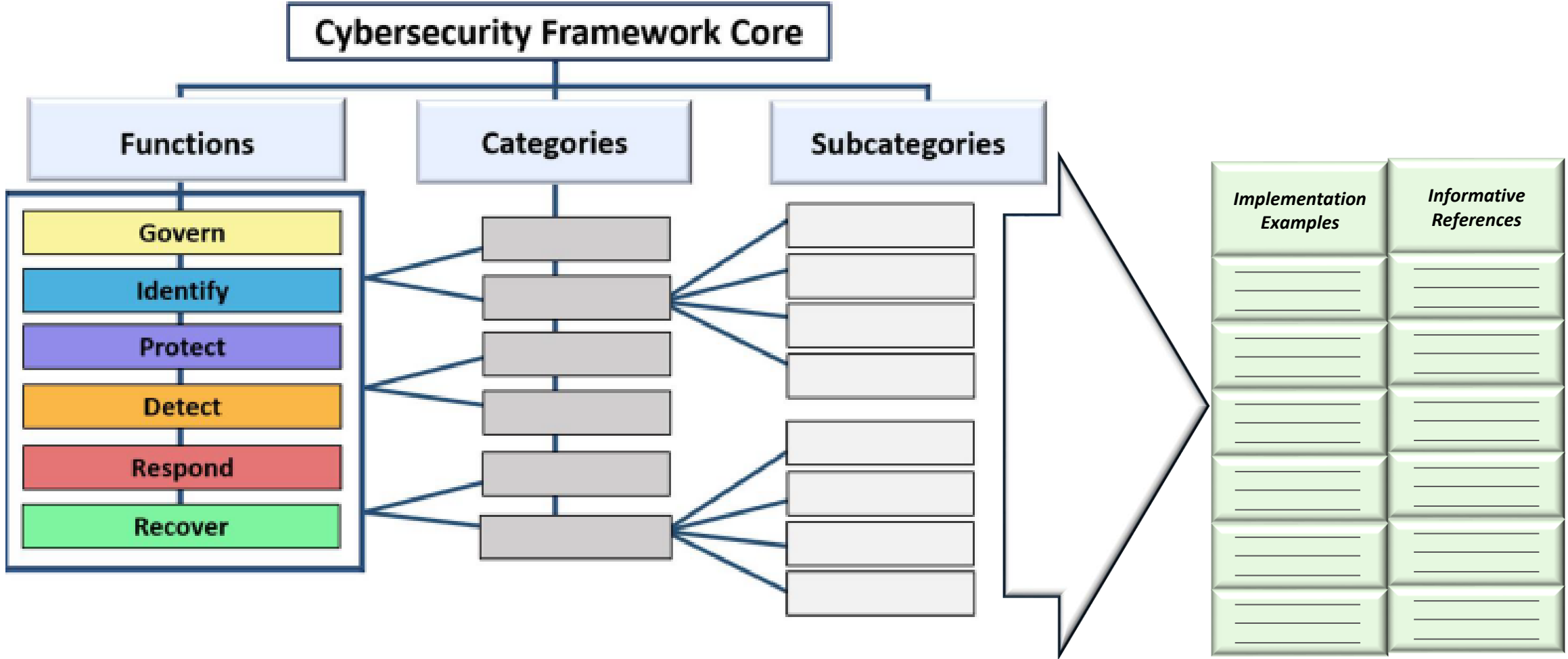
- NIST is actively working on Special Publications to provide recommendations for the usage of PQC standards in applications, e.g.,
 - The initial public draft of NIST Special Publication (SP) 800-227, Recommendations for Key-Encapsulation Mechanisms, is now available for public comment.
<https://csrc.nist.gov/pubs/sp/800/227/ipd>
 - NIST will also hold a [virtual Workshop on Guidance for KEMs](#) on February 25-26, 2025, to gather additional feedback on SP 800-227
- NIST provided guidance for transition in the past (NIST SP 800-131A Rev. 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths) and will provide PQC transition guidance
- NIST CAVP is already testing new PQC algorithms for FIPS 140 validation - <https://pages.nist.gov/ACVP/#module-lattice-algorithms>
- CAVP has finished work on ML-DSA external interface testing. A complete set of test vectors, and a set of intermediate values for FIPS 204 ML-DSA SigGen were posted on Nov 25 to the PQC-Forum

- Update earlier tests with standardized PQC algorithms parameters (X.509, HSMs, TLS, SSH)
- VPN (PQC -only and hybrid modes of the IKEv2 Key Exchange)
- IPsec
- DNSSEC
- Smart Card/PIV...

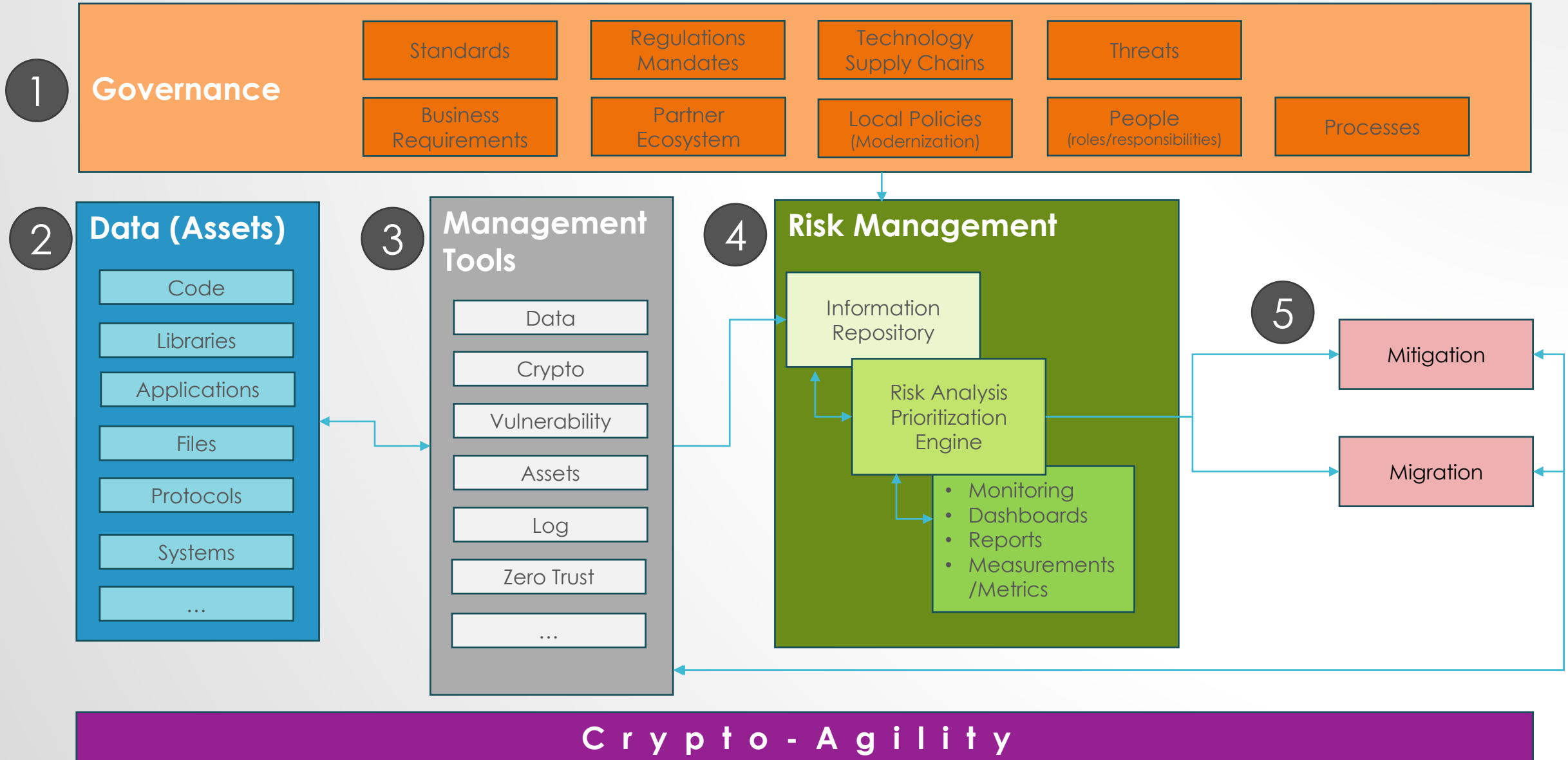
Data centric risk management to prioritize mitigation and migration with crypto agility



a risk management framework Cybersecurity Framework (CSF) 2.0



DATA CENTRIC CRYPTO RISK MANAGEMENT APPROACH



CONSIDERATIONS FOR ACHIEVING CRYPTO AGILITY

Initial Public Draft NIST Cybersecurity Whitepaper (CWSP 39) Considerations for Achieving Crypto Agility

Crypto agility refers to the capabilities needed to replace and adapt cryptographic schemes in protocols, applications, software, hardware, and infrastructures.

This white paper provides an in-depth survey of current approaches to achieving crypto agility. It discusses challenges and tradeoffs and identifies some approaches for providing operational mechanisms to achieve crypto agility while maintaining interoperability.

- Transition Challenges
- Crypto Agility for Security Protocols
- Crypto Agility in Systems for Applications
- Governance
- Discussions:
 - Resource Considerations
 - Agility Awareness Designs
 - Crypto Agility in the Cloud
 - Maturity Assessment for Crypto Agility
 - Strategic Planning
 - Security Policy Enforcement
 - Complexity and Security
 - Environment Specific Agility Requirements

NIST AND NCCOE URLS AND EMAILS

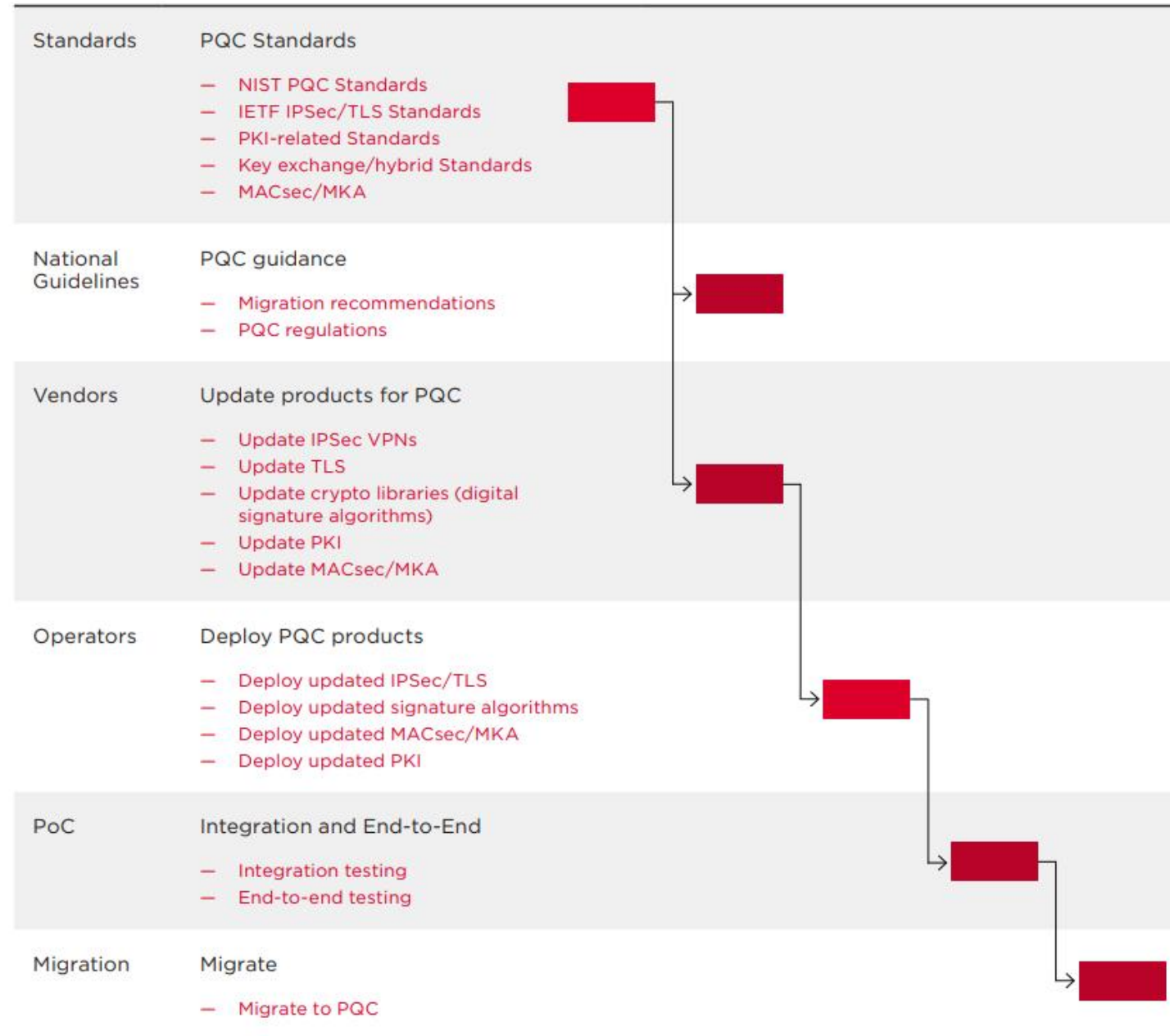
- **NIST Post-Quantum Cryptography**
 - <https://csrc.nist.gov/Projects/post-quantum-cryptography>
- **PQC Crypto Technical Inquiries**
 - pqc-comments@nist.gov
- **NCCoE Migration to PQC Project website**
 - <https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms>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

EXTRA Slides

SECTOR SPECIFIC EXAMPLE
 POST QUANTUM CRYPTOGRAPHY – GUIDELINES
 FOR TELECOM USE CASES VERSION 2.0

• https://www.gsma.com/newsroom/gsma_resources/pq-03-post-quantum-cryptography-guidelines-for-telecom-use-cases/

Figure 2
 Gantt chart for VPN PQC migration



Network operator use cases	Actions Identified	Customer impacting use cases	Actions Identified
Protection of interface between base stations & security gateway	Yes	Virtual Private Network services	Yes
Virtualized network functions	Yes	SD-WAN services	Yes
Cloud Infrastructure	To be determined	IoT Smart Meters	Yes
SIM (physical)	To be determined	IoT Automotive	Yes
eSIM Provisioning (remote)	Yes	Lawful Intercept	To be determined
Devices and firmware upgrade	Yes	Privacy of customer data	Yes
Concealment of the Subscriber Public Identifier	Yes		
Authentication and transport security in 4G and 5G	Yes		

Table 1: Summary of actions for Telco Use Cases