

# NIST CSWP 39 CONSIDERATIONS FOR ACHIEVING CRYPTOGRAPHIC AGILITY: STRATEGIES AND PRACTICES

March 17, 2026

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*

Russ Housley  
*Vigil Security*

Sean Turner  
*sn3rd*

William Barkert†  
*Stratavia LLC*

Karen Kent  
*Trusted Cyber Annex*

Bill Newhouse  
*Applied Cybersecurity Division  
Information Technology Laboratory*

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

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

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.CSWP.39>

December 19, 2025

### Table of Contents

<b>Executive Summary</b> .....	1
<b>1. Introduction</b> .....	2
<b>2. Historic Transitions and Challenges</b> .....	4
2.1. Long Period for a Transition.....	4
2.2. Backward Compatibility and Interoperability Challenges.....	4
2.3. Constant Needs of Transition.....	5
2.4. Resource and Performance Challenges.....	5
<b>3. Crypto Agility for Security Protocols</b> .....	7
3.1. Algorithm Identification.....	7
3.1.1. Mandatory-to-Implement Algorithms.....	8
3.1.2. Dependent Specifications.....	9
3.2. Algorithm Transitions.....	9
3.2.1. Preserving Protocol Interoperability.....	10
3.2.2. Providing Notices of Expected Changes.....	11
3.2.3. Integrity for Algorithm Negotiation.....	11
3.2.4. Hybrid Cryptographic Algorithms.....	12
3.3. Cryptographic Key Establishment.....	13
3.4. Balancing Security Strength and Protocol Complexity.....	14
3.4.1. Balancing the Security Strength of Algorithms in a Cipher Suite.....	14
3.4.2. Balancing Protocol Complexity.....	14
<b>4. Crypto Agility in System Implementations</b> .....	16
4.1. Using an API in a Crypto Library Application.....	16
4.2. Using APIs in the Operating System Kernel.....	17
4.3. Using Service Mesh in Cloud-Native Environments.....	18
4.4. Embedded Systems.....	18
4.5. Hardware.....	19
4.6. Using a Crypto Gateway for Legacy Systems.....	20
<b>5. Crypto Agility Strategic Plan for Managing Organizations' Crypto Risks</b> .....	22
5.1. Cryptographic Standards, Regulations, and Mandates.....	24
5.2. Crypto Security Policy Enforcement.....	24
5.3. Technology Supply Chains.....	25
5.4. Cryptographic Architecture.....	25
<b>6. Considerations for Future Works</b> .....	27
6.1. Resource Considerations.....	27

6.2. Agility-Aware Design.....	27
6.3. Complexity and Security.....	28
6.4. Crypto Agility in the Cloud.....	28
6.5. Maturity Assessment for Crypto Agility.....	29
6.6. Common Crypto API.....	31
<b>7. Conclusion</b> .....	33
<b>References</b> .....	34
<b>Appendix A. List of Symbols, Abbreviations, and Acronyms</b> .....	38
<b>Appendix B. Definition of Crypto Agility in Other Literature</b> .....	41

### List of Figures

<b>Fig. 1. Using a hybrid algorithm to transition to PQC</b> .....	12
<b>Fig. 2. Functional diagram of applications using a crypto API</b> .....	17
<b>Fig. 3. Crypto agility strategic plan for managing an organization's cryptographic risks</b> .....	22



CWSP 39

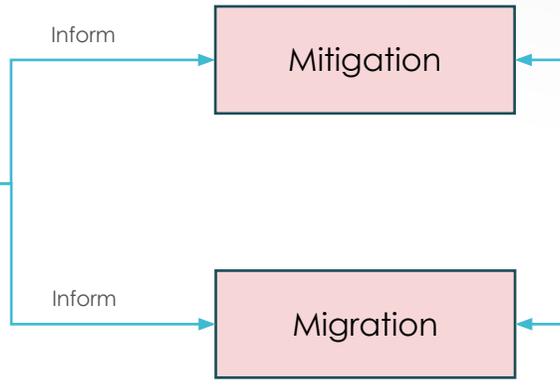
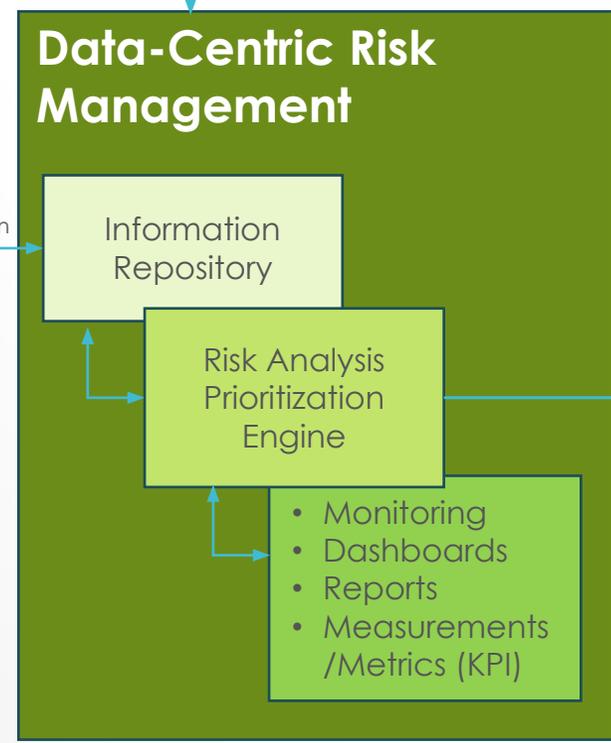
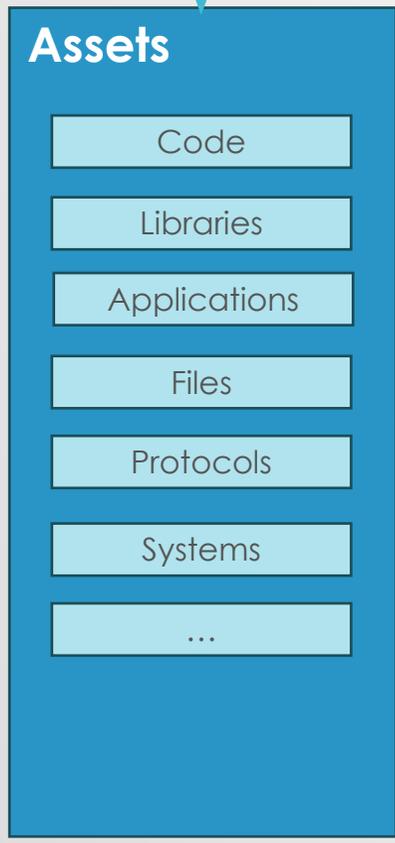
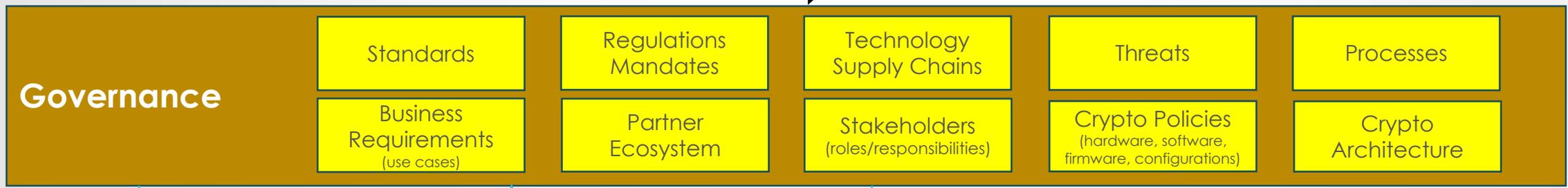


Questions



Questions

Crypto Agility



Crypto Agility

