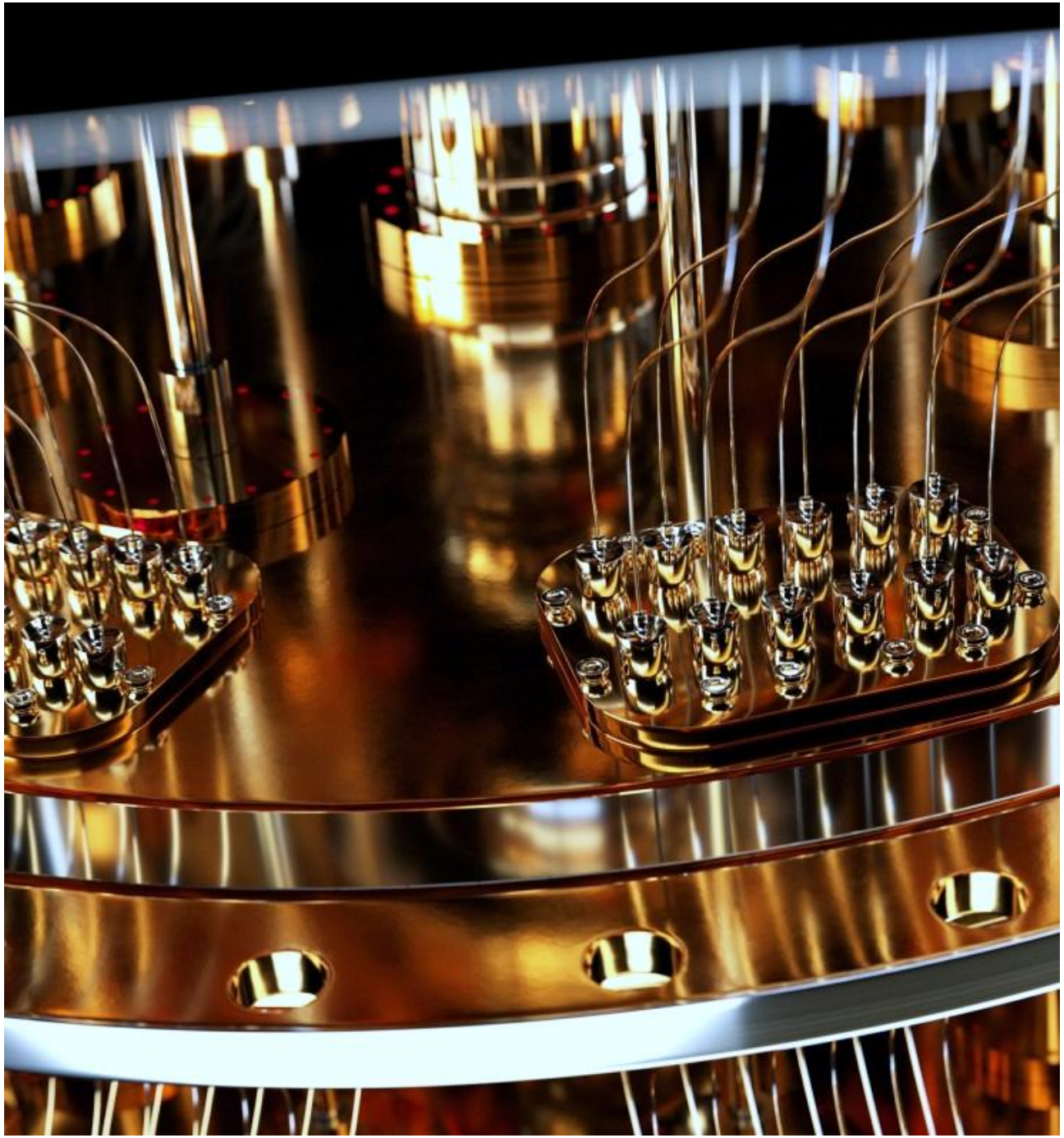


PQC Call to Action

William Gee, Vice Chair, Asia PKI Consortium

Hong Kong | Nov 2025

Q-Day fast Approaching

Google
Quantum Echoes: step towards real-world applications

IBM 2025-2029 Deliveries
Loon (2025) → Kookaburra (2026) → Full fault-tolerant (2029)

Quantinuum (Honeywell)
New version within 2025 will be 1 billion times faster

Microsoft
"Majorana 1" topological core in Feb 2025

Google
Willow achieved a major breakthrough in Dec 2024

©2025 Asia PKI Consortium

The two algorithms

Prof. Peter Shor

Dr. Lov Grover

©2025 Asia PKI Consortium

Transition timeframe: US NIST Recommendations

Note:

- **112 bits security strength equals 2048 bits, and 128 bits equals 3072 bits**
- **Typical key length for digital certificates is currently 2048 bits (3072 bits for code signing)**
- **The NIST recommendations effectively render today's cryptographic algorithms obsolete by 2035**

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Table 4: Quantum-vulnerable key-establishment schemes

Key Establishment Scheme	Parameters	Transition
Finite Field DH and MQV [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [SP80056B]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Check for updates

NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

ble free of charge from:
).6028/NIST.IR.8547.ipd

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

Source:
https://www.quantum.gov/nist-draft-report-on-pqc-transition/

Symmetric and hash algorithms

Cryptographic Construction	Primitive	Problem Family	Post-Quantum Security		
Public-Key Encryption	RSA	Integer Factorization	✗	Shor:	~0 bit
Digital Signature Scheme	ECDSA	EC Discrete Logarithm	✗	Shor:	~0 bit
Key Establishment Scheme	(EC)DH	(EC) Discrete Logarithm	✗	Shor:	~0 bit
Symmetric-Key Encryption	AES-128	Block Cipher	✓	Grover:	~64 bit
	AES-256	Block Cipher	✓	Grover:	~128 bit
Hash Function	SHA2-256	Merkle-Damgård	✓	Grover:	~128 bit
	SHA3-256	Keccak	✓	Grover:	~128 bit

Table 4: Security strength time frames

Security Strength		Through 2030	2031 and Beyond
< 112	Applying protection	Disallowed	
	Processing	Legacy use	
112	Applying protection	Acceptable	Disallowed
	Processing		Legacy use
128	Applying protection and processing information that is already protected	Acceptable	Acceptable
192		Acceptable	Acceptable
256		Acceptable	Acceptable

Source:
https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final
https://www.bosch.com/stories/quantum-computing-threat-how-to-prepare-for-a-smooth-transition-to-post-quantum-cryptography/

NIST Standardisation Status

NIST Standards

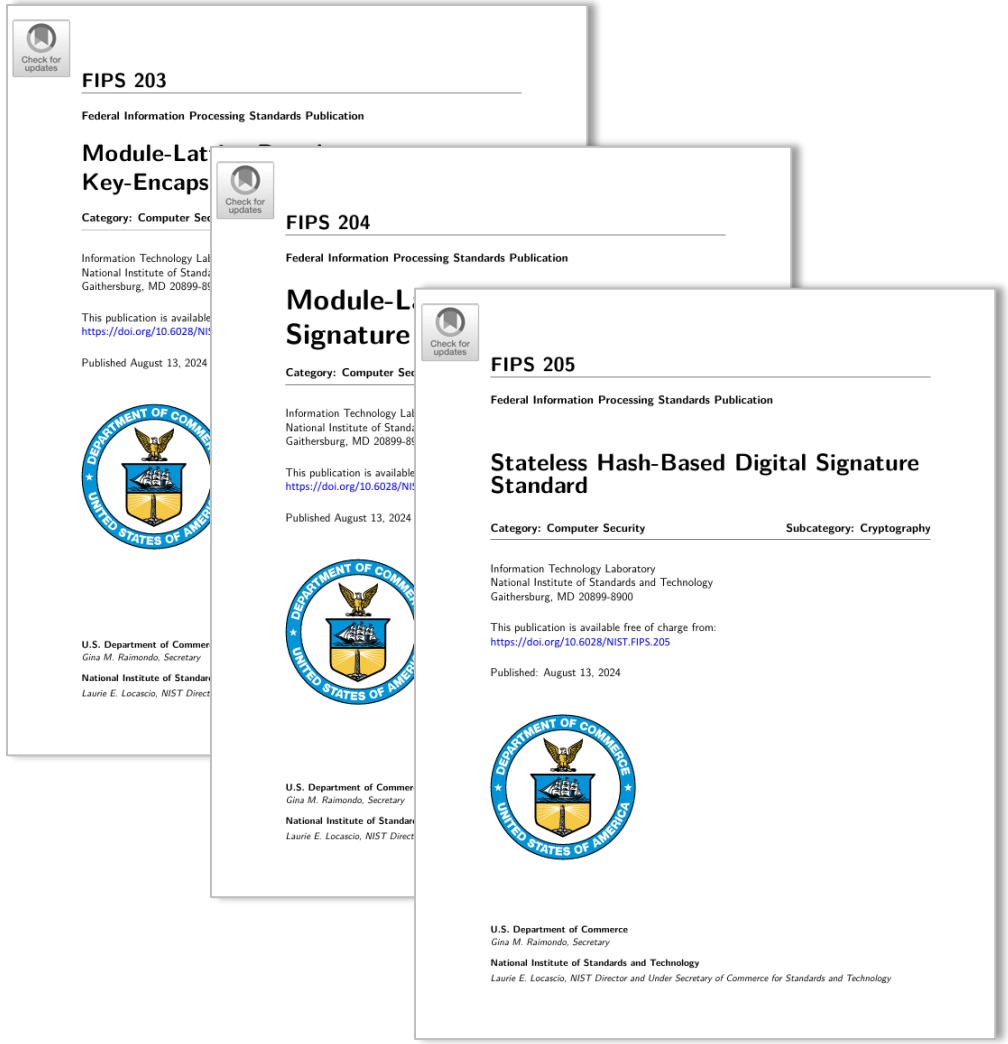
Key-Encapsulation Mechanisms:
CRYSTALS-KYBER (2022) | FIPS 203
HQC (2025) | FIPS under development

Digital Signature Algorithms:
CRYSTALS-DILITHIUM (2022) | FIPS 204
SPHINCS+ (2022) | FIPS 205
FALCON (2022) | FIPS under development

NIST Ongoing Activities

Digital Signatures Algorithms:
CROSS , FAEST, LESS, SQsign, HAWK, MAYO, Mirath, MQOM, Perk, RYDE, SDitH, QR-UOV, SNOVA, UOV

Encryption:
BIKE, CLASSIC McEliece

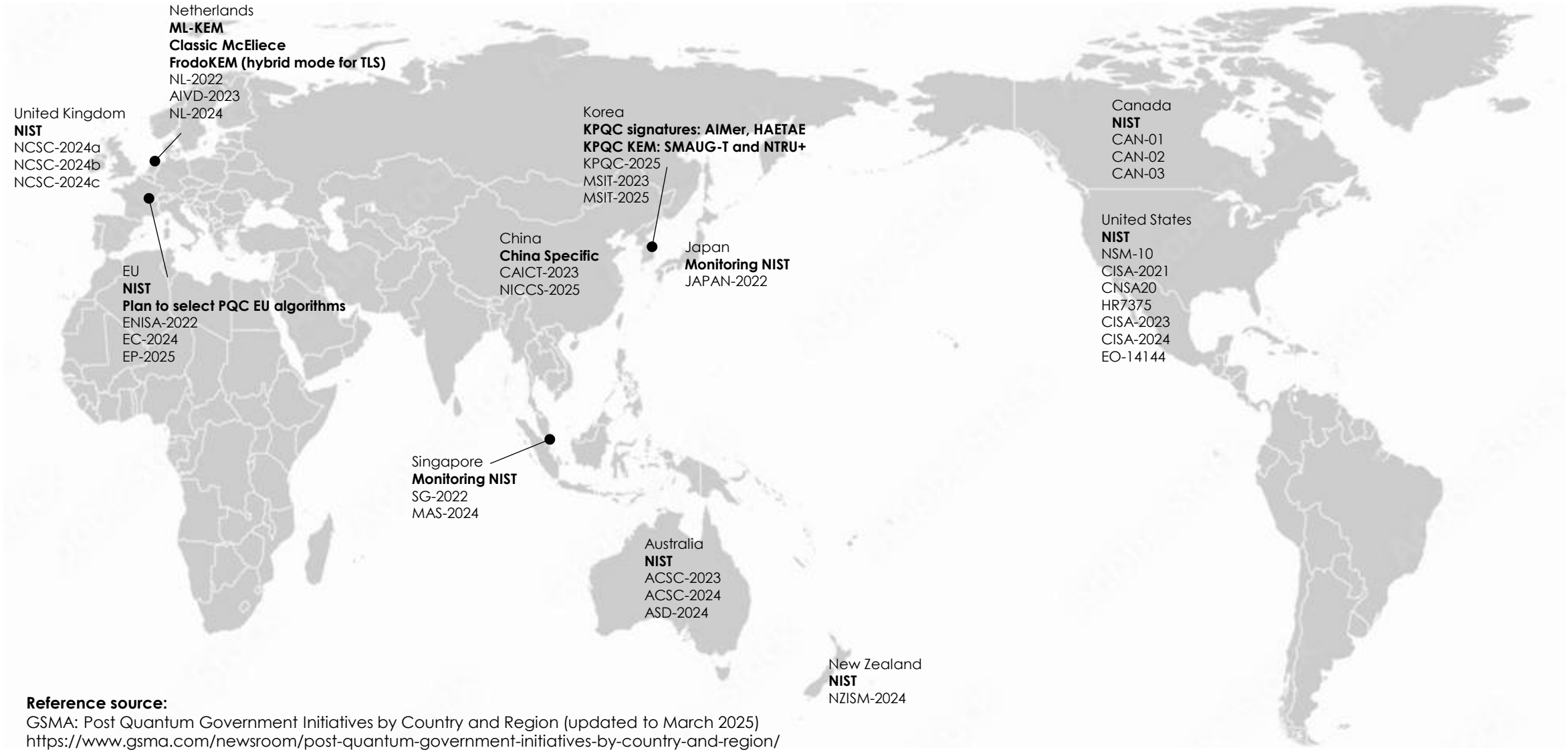


Examples of other enabling standards

- **OpenSSL 3.5: support for ML-KEM, ML-DSA, SLH-DSA**
- **IETF/ISO:**
  - Broad alignment with NIST recommendations
  - Instances of selective adoption, e.g. LMS/XMSS for IETF/ISO 14888-4
  - Ongoing work for: IPSec, IKEv2, TLS 1.3, X.509
  - Non-NIST algorithm also expected, e.g. FrodoKEM
- **IEEE:**
  - IEEE 802.11 (work ongoing)
- **ETSI:**
  - TS 104 015 Quantum-Safe Hybrid Key Exchange
- **Quantum secure smart cards**

©2025 Asia PKI Consortium

Divergent national and regional strategies



Reference source:
GSMA: Post Quantum Government Initiatives by Country and Region (updated to March 2025)
https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/

Threat vectors…

HNDL vs. TNFL

Harvest Now, Decrypt Later **Trust Now, Forge Later**

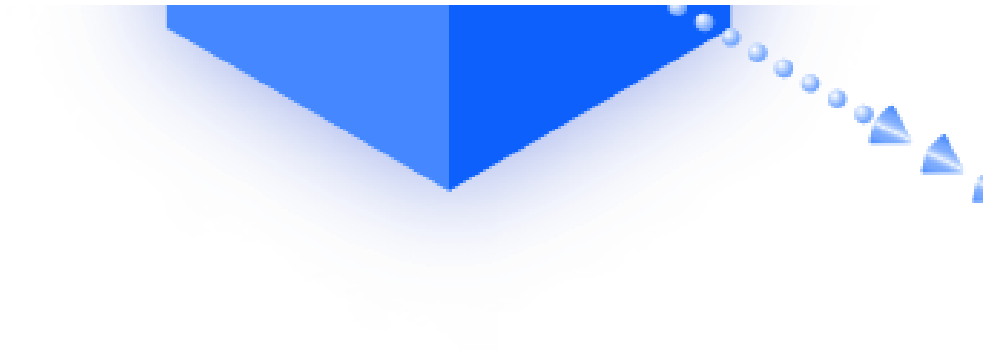
Beyond cybersecurity…

Cryptography impacts every aspect of our digital architecture

Reference source:
IBM: Secure the post-quantum future (published 3 October 2025)
https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-quantum-safe-readiness

Remediation…

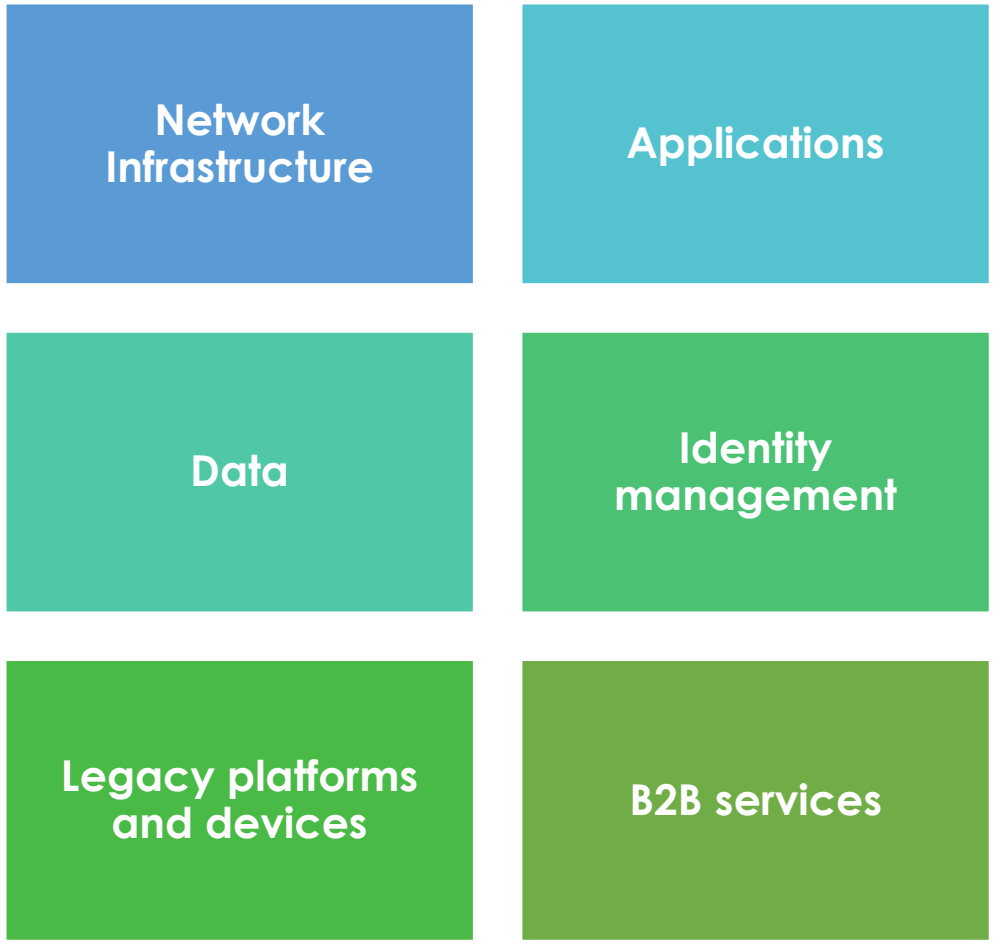
Balancing internal ownership with vendor dependency



Compounding this uncertainty is an overestimation of the role of external vendors in solving quantum-safe remediation issues. 62% of respondents believe vendors will handle quantum-safe transition requirements for them, while 56% continue to view quantum safety as purely a technical issue.

Reference source:
IBM: Secure the post-quantum future (published 3 October 2025)
https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-quantum-safe-readiness

Resilience



> … Reframe quantum-safe preparation not as insurance against a specific future risk, but as a capability that delivers business value and transformational benefits regardless of when quantum computing capabilities mature

Reference source:
IBM: Secure the post-quantum future (published 3 October 2025)
https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-quantum-safe-readiness

©2025 Asia PKI Consortium

Cryptographic agility

Algorithmic	Operational	Automation	Governance	Ecosystem
Ability to select and switch algorithms	Rollout processes and deployment	Enabling architecture and configuration, and consensus on standards and protocols	Policies, rules, compliance and regulatory frameworks	Coordination with vendors, suppliers, and regulators

EASY

PKI certificate issuance solution

Validity checks for trust root; quantum-safe trusted time; public key size; dependencies…

DIFFICULT

Process and People

Technology

Meaning of Quantum-Safe for HSMs: What is NOT

- HSMs without quantum-safe roots of trust (RoT) injected at manufacturing time are not quantum-safe and will never become quantum-safe
- Classic HSM providing PQC algorithm support does not make it quantum-safe
- Adding QRNG (Quantum Random Number Generator) to a classic HSM does not make it quantum-safe
- Classic HSM to HSM communications are subject to Harvest Now/Decrypt Later attacks so this need to be quantum-safe also
- Obtaining FIPS 140-3 validation of a classic HSM does not make it quantum-safe

©2025 Asia PKI Consortium

Call to Action

Discovery

Inventory

Demos and Pilots

Cryptographic Library

Discussions and Sharing

Asia PKI Consortium

THANK YOU