Building a PQC Center of Excellence

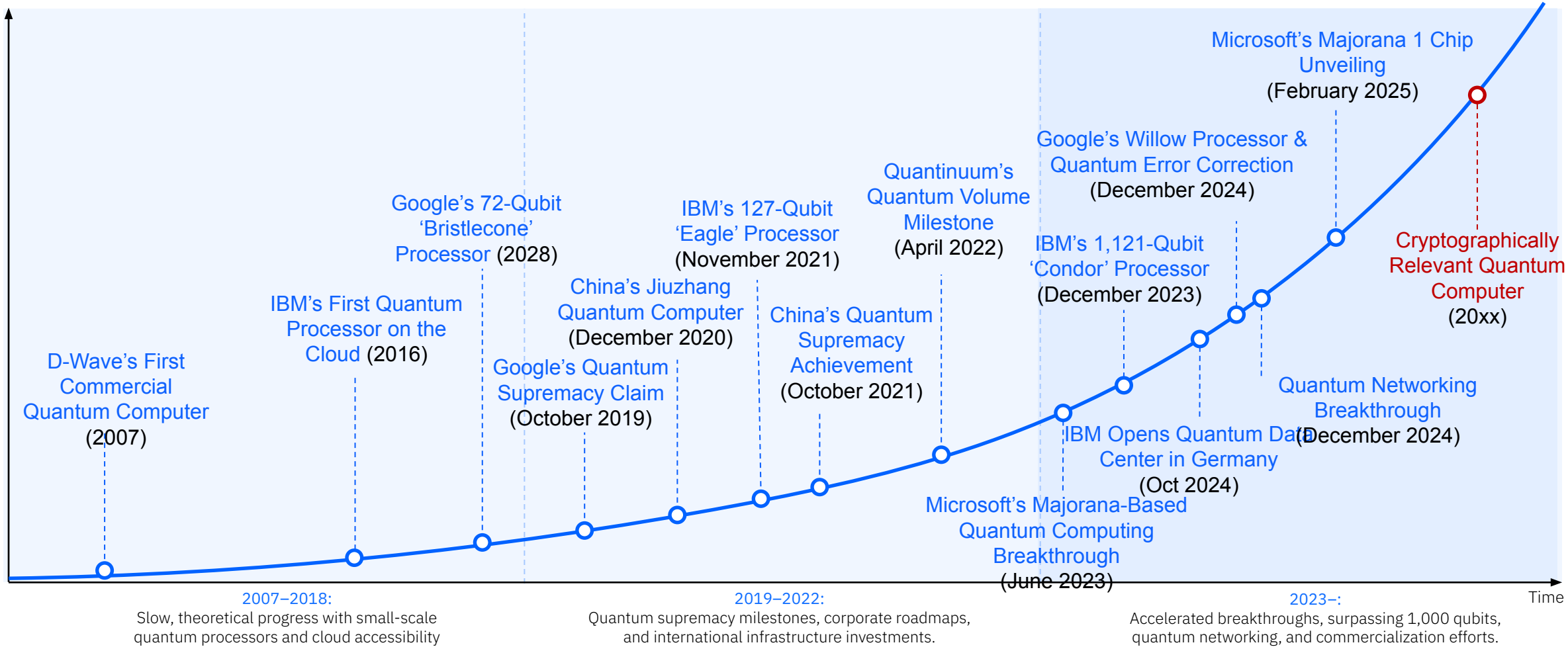
Understand the methods to overcome the hurdles

J.R. Rao
IBM Fellow and CTO, Security Research
IBM Research

March 17, 2026

IBM

The Quantum Risk:
What's Happening, and Why It Matters



There is increasing urgency to build quantum resilience from governments and institutions worldwide

NIST, NSA and CISA

All recommend organizations create cryptographic inventories and integrate them into risk assessment processes to prioritize quantum-safe cryptography adoption as soon as possible.[3]

US National Cyber Strategy & EO

Signed in March 2026, accelerates the modernization and resilience of PQC adoption by directing agencies to have visibility into cryptographic inventory in the next 2 years.

EU Members

Guidance from 18 EU member states requires preparation for quantum threats be integrated into cybersecurity risk management.

Early protection of sensitive data is critical to avoid leaving key assets exposed.[2]

Singapore Financial Institutions

The Monetary Authority of Singapore issued an advisory to urging financial institutions to prepare for the transition to post-quantum cryptography.[4]

India Telecommunications

India's Telecommunication Engineering Centre (TEC) published a technical report on migration to post-quantum cryptography.[5]

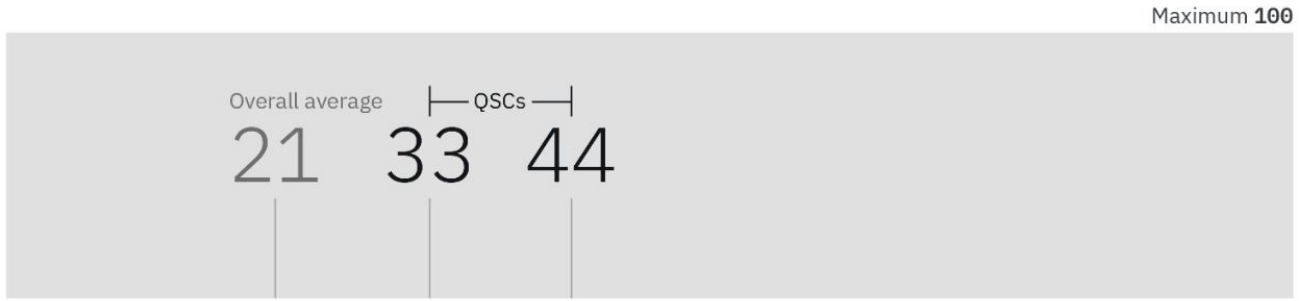
Indonesia Defense University

The university's Center for Quantum Security Ecosystem (CQSE) introduced a roadmap for the development of a national quantum security system.[6]

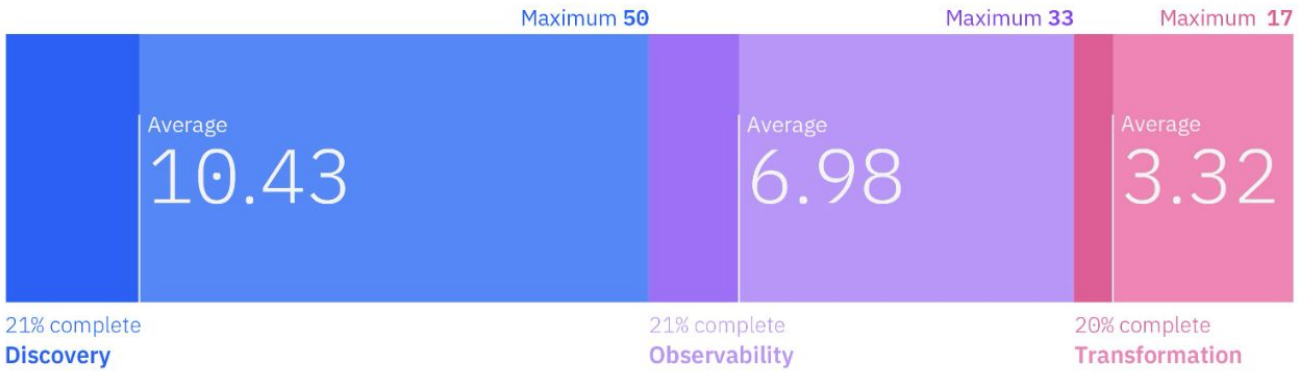
1. National Security Memorandum 10, Young, 2022
2. 2. Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography, BSI, 2024
3. Quantum-Readiness: Migration to Post-Quantum Cryptography, CISA, 2023
4. Advisory on Addressing the Cybersecurity Risks Associated with Quantum, Monetary Authority of Singapore, 2024
5. Migration to POST QUANTUM CRYPTOGRAPHY, Telecommunication Engineering Centre, 2025
6. Indonesia Defense University Launches Center for Quantum Security, Strengthening National Cyber Sovereignty, Intimedia, 2025

IBM **Quantum-Safe** Readiness Index

The average quantum-safe readiness score: 21 out of 100



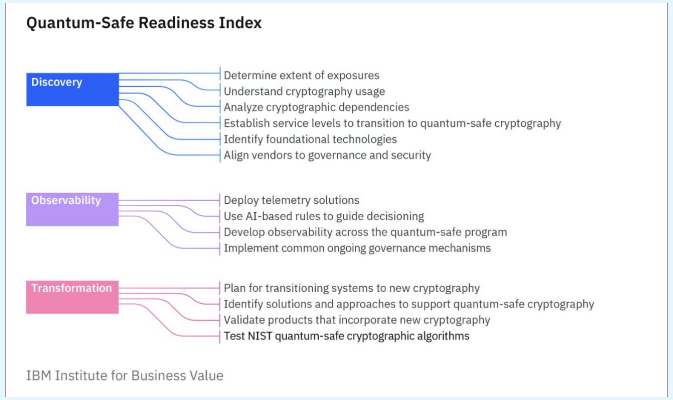
Measuring progress toward quantum-safe readiness



https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-safe

IBM Institute of Business Value

- 14 indicators
- Grouped into the three categories



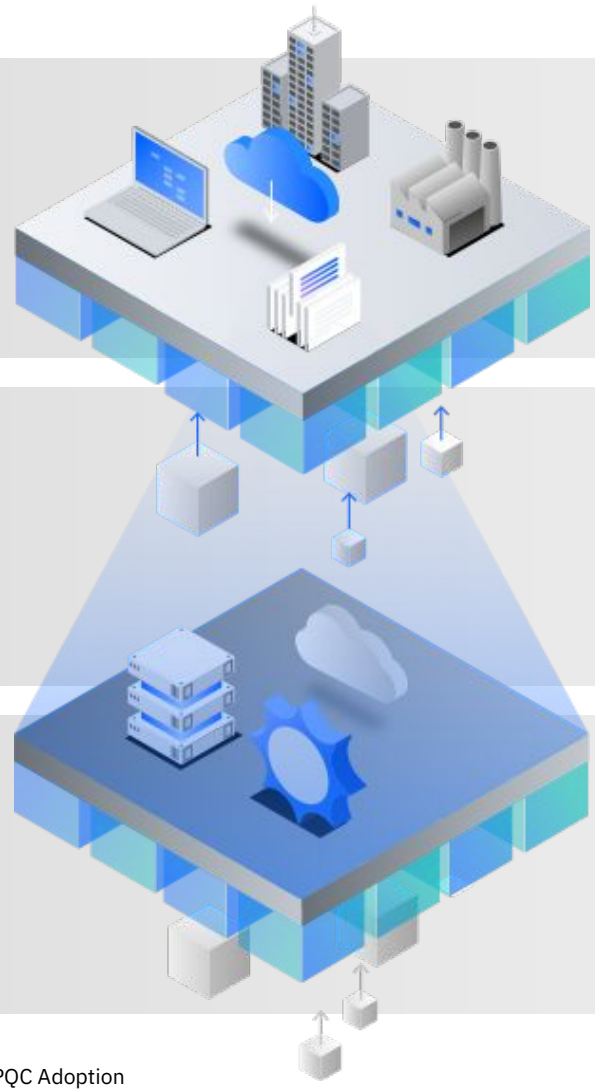
- Surveyed 565 CxOs across 15 countries and 13 industries: organizations with a minimum $250 million in annual revenue

Our Point of View

Driving Enterprise-Wide Quantum Resilience Across Domains

Our structured approach to align enterprise, applications, and third parties on modern, secure, and scalable cryptography practices

IBM Quantum Safe
EXECUTION FRAMEWORK



Enterprise and Strategy

Set the vision, enforce governance, and drive enterprise-wide consistency for cryptography modernization

CIO / CTO / CISO

Compliance, Risk and Cybersecurity

- Drive top-down policies and ownership
- Get full visibility of crypto use
- Modernize PKI, KMS, CLM for hybrid/cloud
- Align standards across teams

Business Units, Apps and Platforms

Transform systems, applications, and DevOps pipelines to adopt agile, future-proof cryptographic practices

Business Asset / Project Owners

Developers / Platform Teams

- Crypto often hidden and outdated
- Support for secure app migration
- Externalize crypto from code
- Embed into DevSecOps

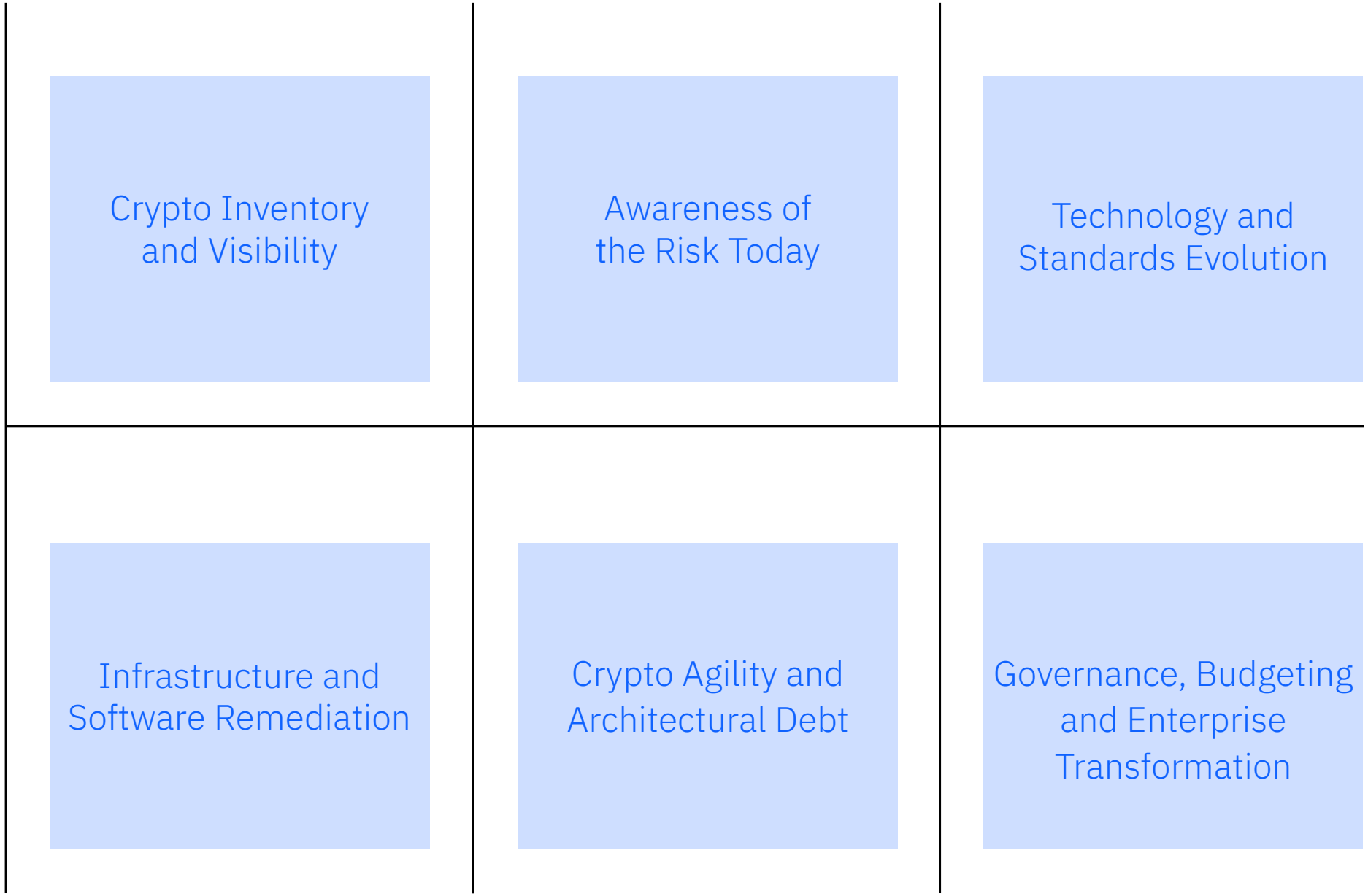
Third Parties and Suppliers

Align external partners and platforms with enterprise crypto standards to ensure secure and compliant ecosystems

3rd party Developers / Technology Providers

- Enforce crypto standards in contracts
- Validate external certs and keys
- Secure APIs and integrations
- Monitor third-party crypto use

Challenges confronting enterprises



Towards a Crypto Center of Excellence

Board of Directors
- Who owns the program?
- What is the migration timeline?
- What are the key milestones?
- Where is the talent?

CEO

Strategic framing and accountability
- Strategic prioritization
- Executive ownership
- Cross-enterprise alignment
- Stakeholder communication

CRO

Enterprise Risk Posture
- Enterprise risk heatmap
- Legal & regulatory exposure
- Industry risk benchmarking
- Long-term data protection

CFO

Budget and Capital Planning
- Program budget envelope
- CapEx vs OpEx planning
- Cost phasing (5–10 year horizon)
- ROI / risk reduction justification

CIO

Enterprise Migration Complexity
- Enterprise system inventory
- Application & certificate scale
- Vendor ecosystem readiness
- Operational migration complexity

CISO

Security Risk
- Harvest-now-decrypt-later risk
- Crypto inventory & agility
- Post-quantum algorithm adoption
- Security governance

CTO

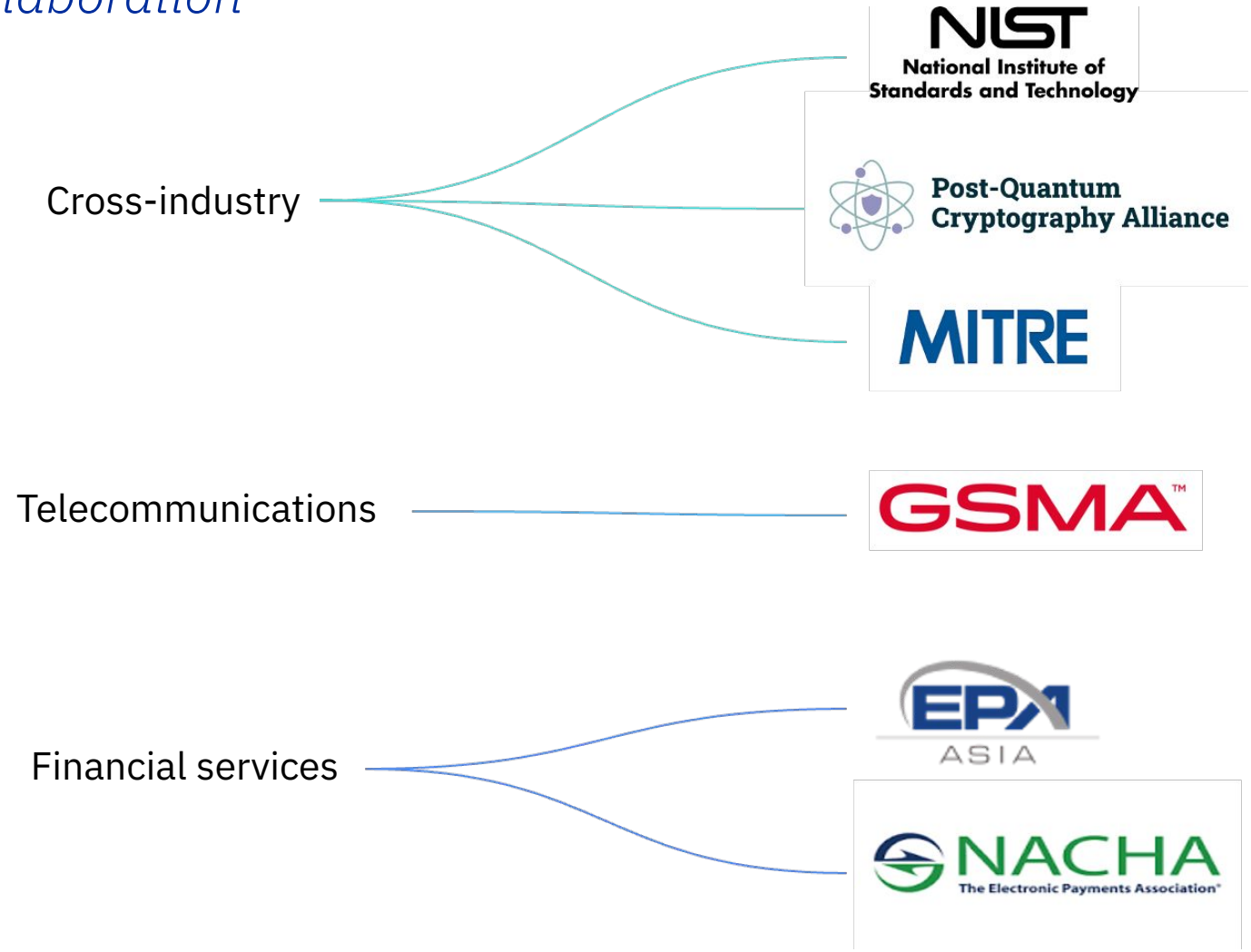
Technology Architecture
- Crypto-agile architecture
- Hybrid TLS deployment
- Platform modernization
- Cloud & infrastructure readiness

Consortia

Quantum Safe leadership and collaboration

Consortia are critical for raising awareness, uniting ecosystems, and enabling the adoption of post-quantum cryptography at scale.

We are working across industry, open-source, and government-based groups to serve our strategic market segments and to establish broad market credibility.



Key take aways

Fill out the form and get IBM’s recommended approach to PQC transformation.

Quantum threatens our digital security

Quantum computers **threaten classical cryptography**

The Quantum Threat is already **relevant today**

Cryptography is **difficult to replace**

Industry sectors and Governments recommend to act

New cryptographic algorithms have been developed and standardized

Nations have **incorporated quantum-safe** preparation into their national quantum strategies

The European Commission encourages member states to develop a **comprehensive strategy** for the adoption of Post-Quantum Cryptography

Organizations should take a re-usable approach

Organizations must **prioritize** their efforts to address the quantum threat.

A **risk framework** should be used to identify and prioritize areas of high risk.

A **center of excellence** approach is required to manage the complexity.

Authorities should **re-use own experience** and **interaction with industry associations** to ultimately drive regulation and certifications.


IBM