National Cryptologic Foundation: Convening to Act

Insights:
Accelerating Adoption of QRC at the C-Level

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

March 11, 2025

Agenda

01 Starting your quantum-safe journey

02 Identifying dependencies

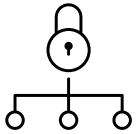
03 Understanding your exposure

04 Navigating the quantum-safe transformation

Cryptography impacts everything

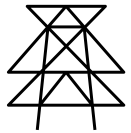
Cryptography touches every corner of the digital world

Internet protocols



Domain Name Service(DNS), Hyper-text Transfer Protocol (HTTP), Telnet, SFTP

Critical infrastructure



Code updates; Control systems- Oil pipelines, Electric grids; Car systems,...

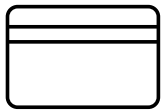
Blockchain applications

Coin wallets, Transactions, Authentication

Digital signature laws

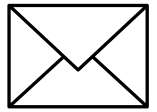
EiDAS - PDF Advanced Electronic Signature – (PAdES), Advanced Electronic Signatures (AES), ...

Financial systems



Payment Systems: (EMV, SWIFT, Settlement Systems, FinTech, ...)

Enterprise applications



EMAIL – PGP, Identity Management PKI/LDAP/.., Virus scanning patterns, PKI Services

Our digital world depends on cryptography, which is used in trillions of transactions on billions of devices

Internet
Domain name system (DNS), Hypertext Transfer Protocol (HTTPS), Telnet, file transfer protocol (FTPS)

Digital signatures
Electronic identification and trust services (eIDAS), PDF advanced electronic signature (PAdES), advanced electronic signatures

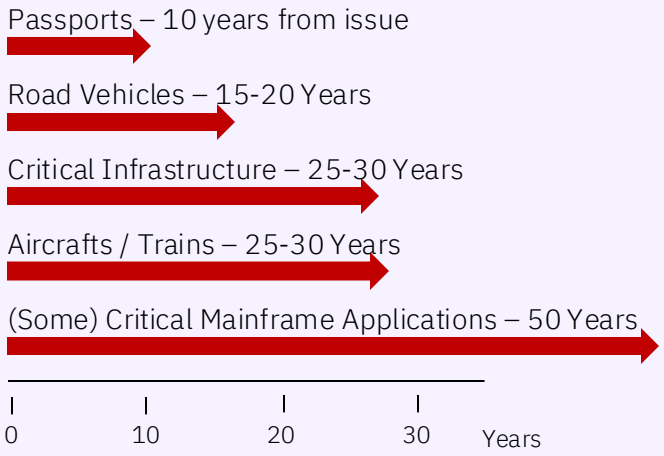
Critical infrastructure
Code updates, control systems, car systems

Financial systems
Payment systems: EMV, CHAPS, Fedwire, TARGET2, EURO1 SWIFT, settlement systems

Blockchain
Wallets, transactions, authentication

Enterprise
Email: PGP, identity management, PKI, LDAP; virus scanning patterns; PKI services; bespoke applications

Systems have long update cycles



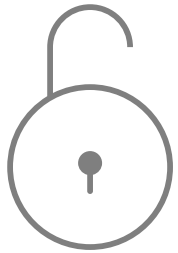
Data needs to stay secure for a long time

What will a cyber criminal be able to do?

Availability of “cryptographically relevant” quantum computer

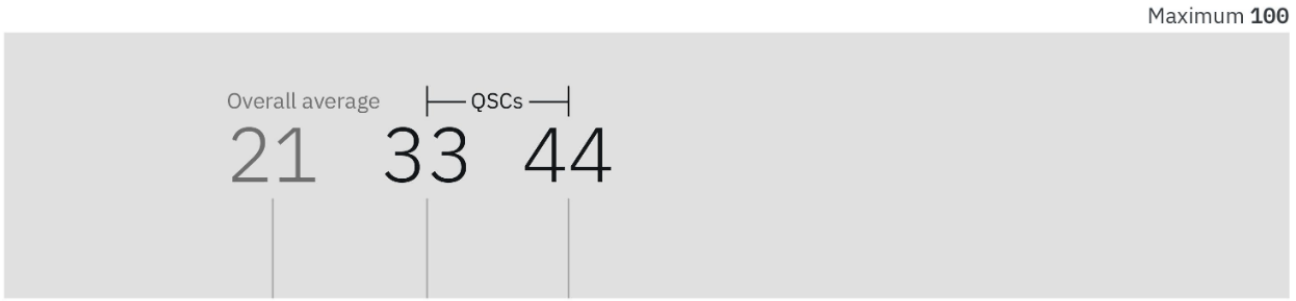
…before

…after

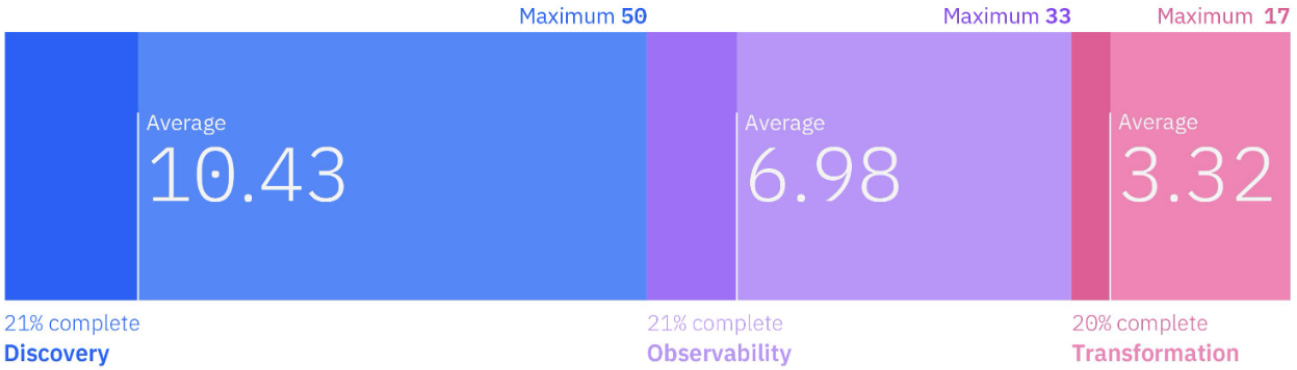
Harvest confidential data	Decrypt lost or harvested confidential data	Disrupt business with manipulation	Manipulate digitally signed contracts and legal history
			
in order to decrypt them later	by breaking encryption	through fraudulent authentication	by forging digital signatures
Urgency	Confidentiality	Integrity	Authenticity

IBM Quantum-Safe Readiness Index

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

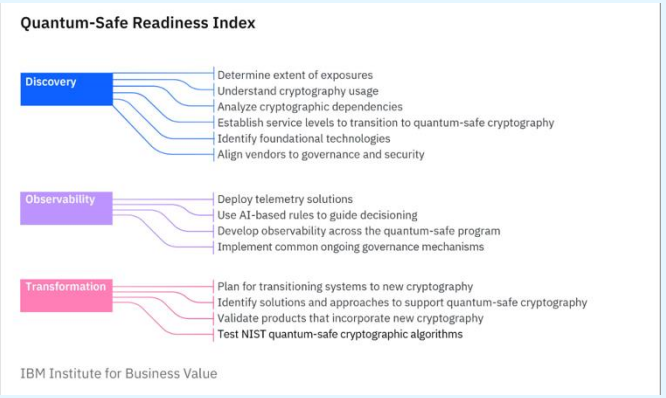


Measuring progress toward quantum-safe readiness



IBM Institute of Business Value

- 14 indicators
- Grouped into the three categories

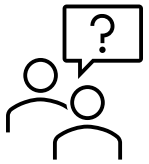


- Surveyed 565 CxOs across 15 countries and 13 industries: organizations with a minimum $250 million in annual revenue

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

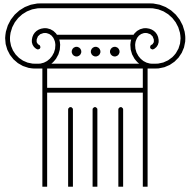
Key Discussions with C-Suite

Lack of awareness

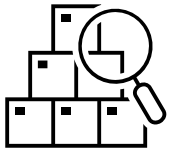


Weak or no data inventory

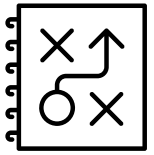
Legacy systems/processes



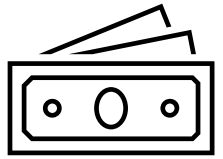
No cryptography inventory



No cryptography strategy



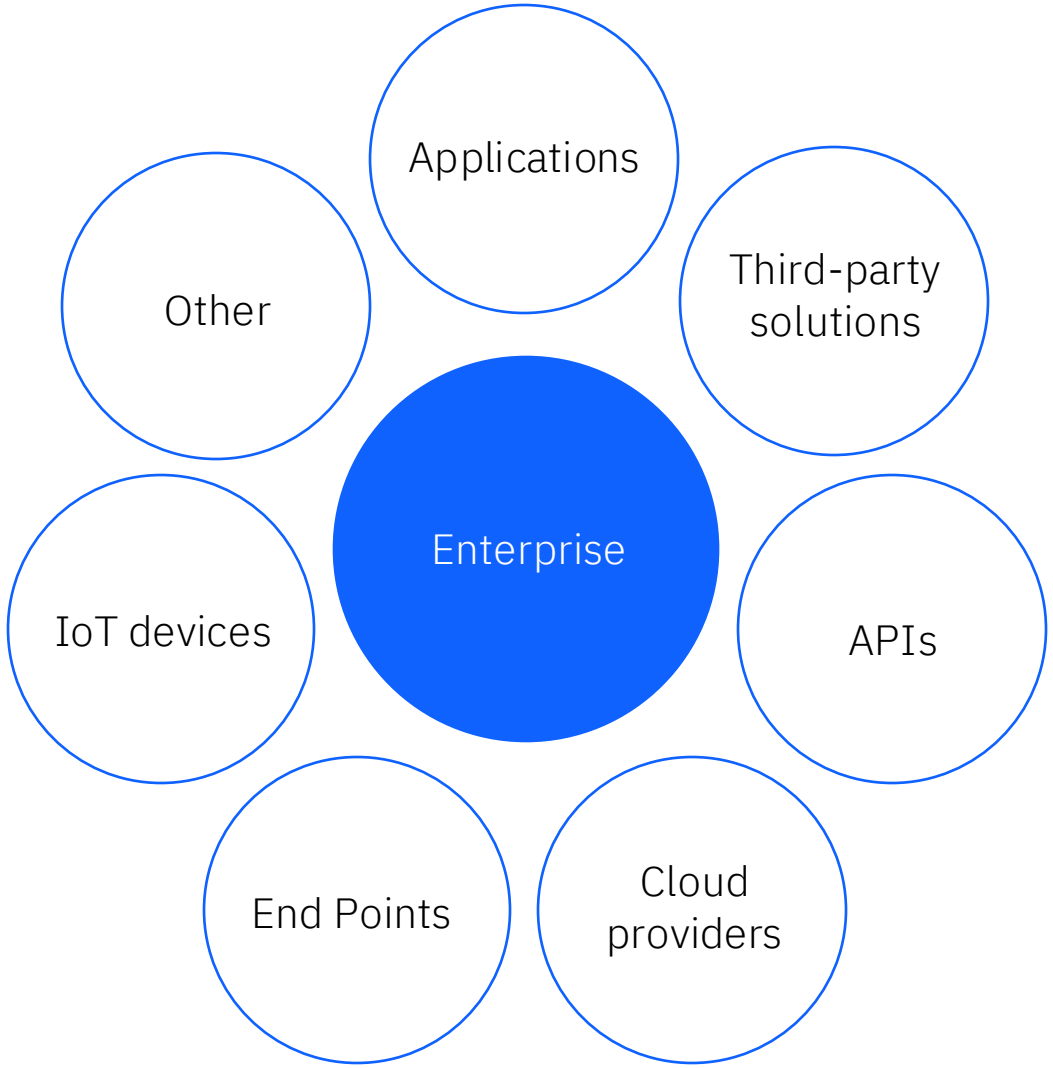
No budget for migration



Enterprises operate with many dependencies

Cryptographic transformation begins with a clear understanding of business objectives, assets, and dependencies, coupled with a strong governance model.

Once we can understand the dependencies, we can assess the risk, prioritize vulnerabilities, and plan remediation actions accordingly.



How to manage cryptography transition? It’s all about context!

Enterprise
Cryptographic
Posture

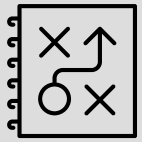
App & Product
Cryptographic
Posture

PREPARE	ASSESS	TRANSFORM
Understand the situation	Define the target	Execute the transformation
Raise awareness Map affected assets Identify urgent actions	Define governance Prioritize actions Initiate urgent measures	Implement actions Align with internal initiatives Use predefined patterns

Methodology and Technologies for Migration

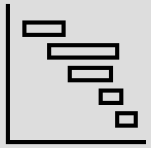
PREPARE → ASSESS → TRANSFORM

Enterprise
Cryptographic Posture



Awareness and strategy →

Business dependencies →



Prioritization of actions →

Mitigation and remediation

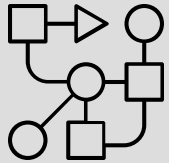
"Things that I use"

– 3rd party software, devices, SaaS
– applications developed inhouse

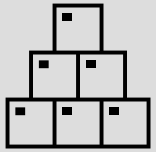
Cryptography Bill of Materials (CBOM)

App & Product
Cryptographic Posture

Code and dependency analysis →



Rearchitect for agility →



Code remediation

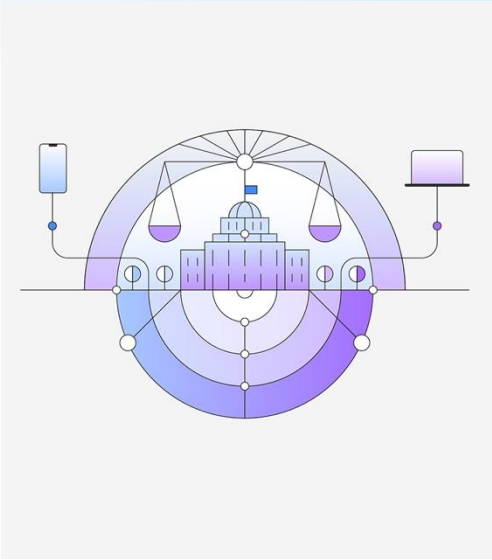
"Things that I control"

How can you get started

Three Case Examples and Lessons Learned

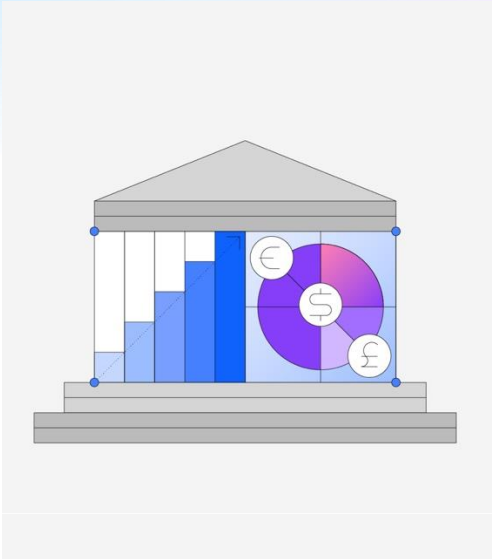
First 6 months → First year → Outer years

Zone 1
Understand the Threat



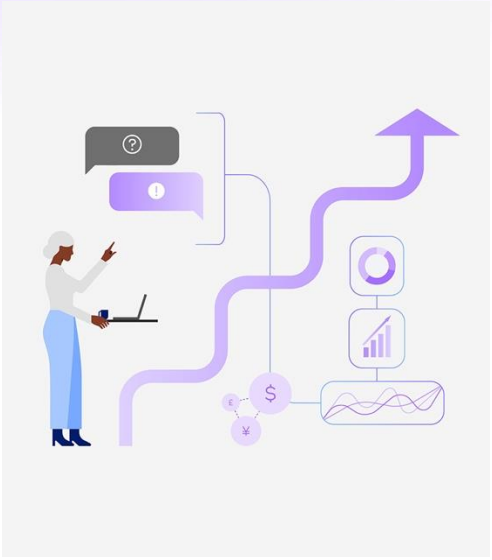
European Government
Central IT Agency

Zone 2
Prepare for Migration



One of the Largest
European Banks

Zone 3
Execute the Migration



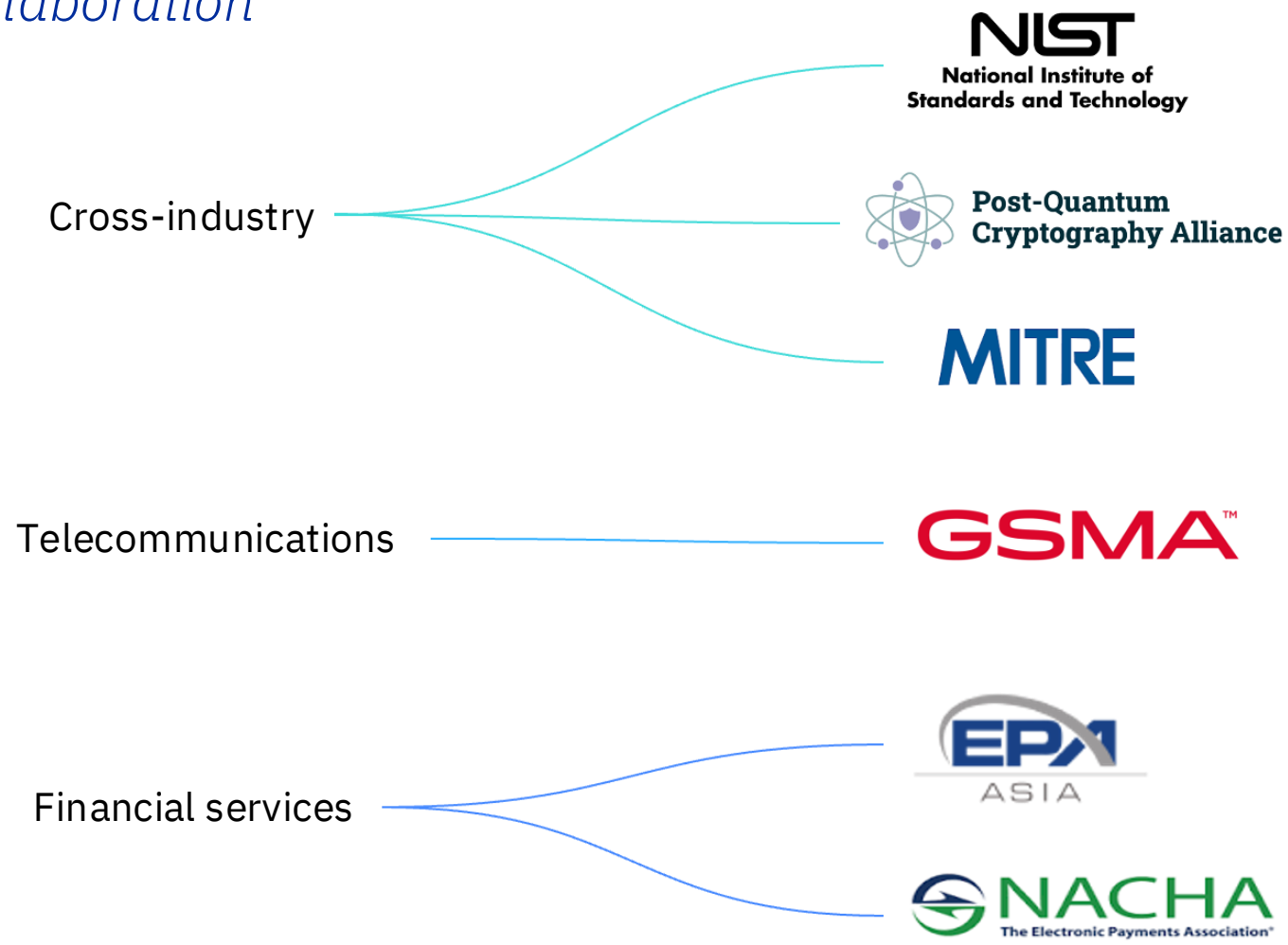
One of the Largest
Private Banks

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

Quantum threatens our digital security

Quantum computers **threaten current 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 **central team** approach is required to manage the complexity.

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

13


IBM