Post-Quantum

Cryptography Conference

The ABCs (Accelerated, Better and Cheaper) to Cryptographic Resilience

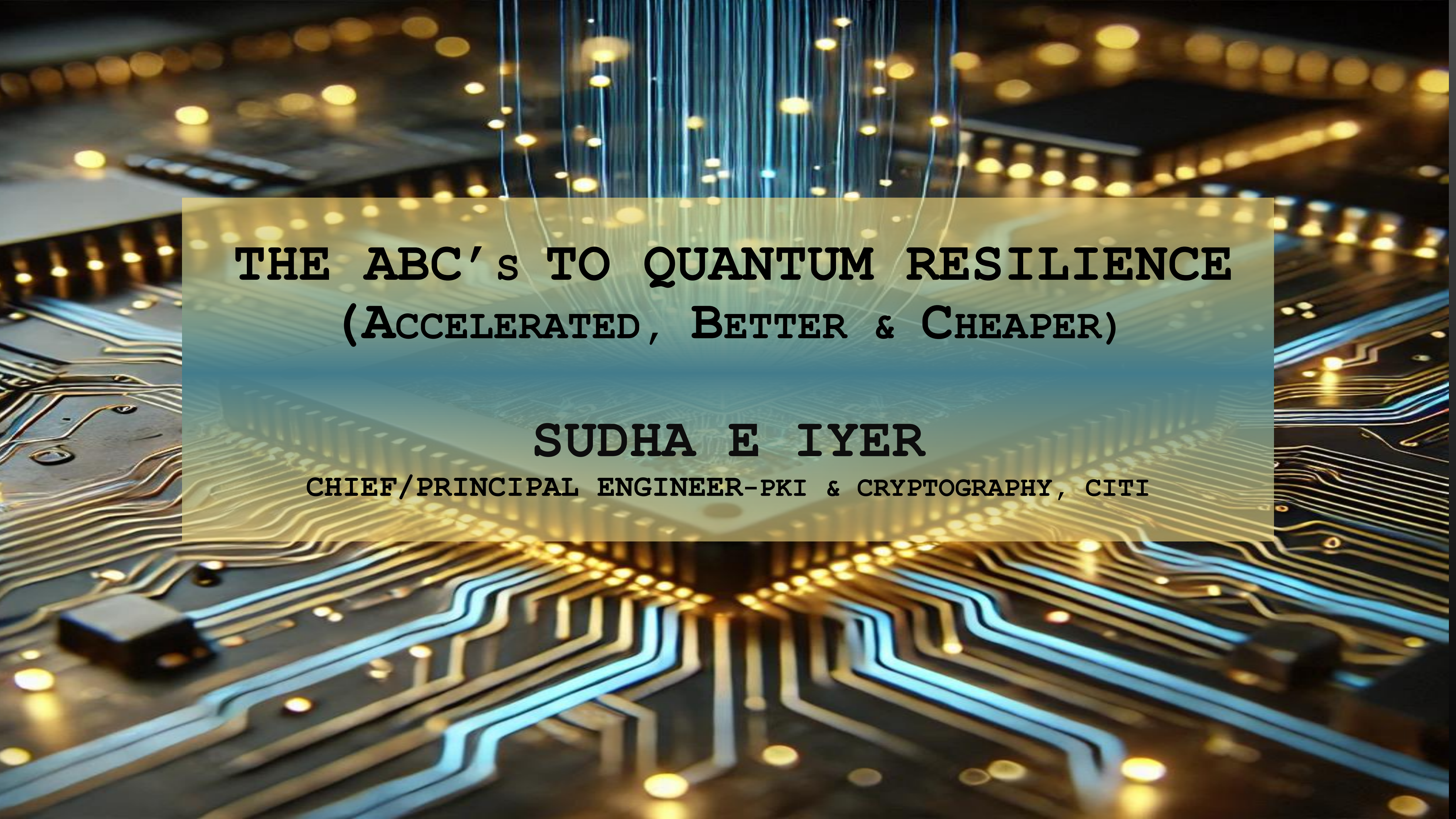
Sudha Iyer

Chief/Principal Engineer-PKI & Cryptography at Citi

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium



THE ABC's TO QUANTUM RESILIENCE (Accelerated, Better & Cheaper)

SUDHA E IYER

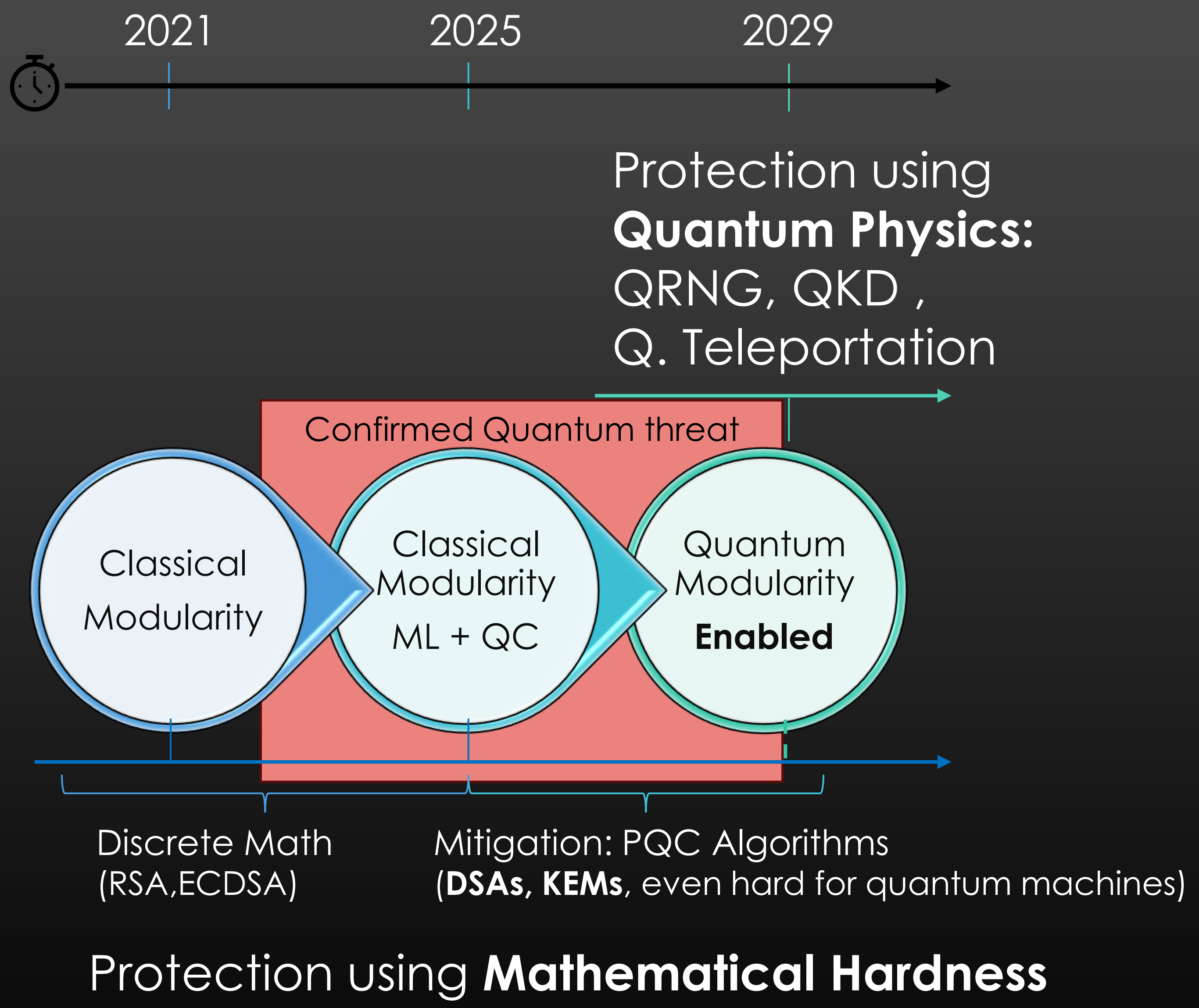
CHIEF/PRINCIPAL ENGINEER-PKI & CRYPTOGRAPHY, CITI

OVERVIEW

Agenda:

- Where we stand today
- Why this transition is complex
  - How some are are solved using NIST and IETF
  - Key adoption challenges leaders face
- ABC: A decision framework for quantum resilience
- Roadmap to help you execute Accelerated, Better and Cheaper modernization and resilience

WHERE ARE WE NOW?



2021

2025

2029

Protection using
Quantum Physics:
QRNG, QKD ,
Q. Teleportation

Confirmed Quantum threat

Classical Modularity

Classical Modularity
ML + QC

Quantum Modularity
Enabled

Discrete Math
(RSA,ECDSA)

Mitigation: PQC Algorithms
(**DSAs, KEMs**, even hard for quantum machines)

Protection using **Mathematical Hardness**

COMPLEXITIES AHEAD OF US

- Mathematical Complexity
- Implementation Complexity
- Decision Complexity

STANDARDS (NIST)

- Solved Mathematical Complexity via:
  - **PQC Algorithms***: Kyber, Dilithium, Sphincs+ and Falcon, also known as FIPS 203, 204, 205 and 206.
  - **Key Encapsulation Mechanisms** : NIST SP 800-227.

*NIST is working on widening the selection pool.

STANDARDS (OTHERS)

- IETF Standards
  - Configuration and syntax
  - Implementation protocol
  - Interoperability and
  - Reference architectures
    - TLS, IPSEC.
    - Message Encoding signatures (JOSE/ COSE)
- PCI DSS, BSI and also Health Industry cybersecurity standards to follow later

PQC TRANSITION OPTIONS

- Hybrid & Composite choice
- Pure PQC choice
- Decoupled cryptographic designs
- Hardware Support. example: FIPS certified modules

Tune in to the panel discussion at 2:30 on 30th Oct 2025 covering this in detail

KNOWN CHALLENGES

- Legacy system dependencies
- Regulatory uncertainty
- Supply chain readiness
- Efficiency of PQC algorithms

PRODUCT READINESS

Predicted readiness

Q2 2026: Product readiness for HSMs and libraries

Q4 2028: Certification using Regional CMVP for Compliance and regulatory clarity for HSMs, offline, TEE, TPM and PCI compliant devices

Q4 2029: Standard Implementation in new firmware and OS cryptography in most products

Assumptions: Businesses and their suppliers actively volunteer in the early FIPS/ other hardware level testing to uncover operational disruptions

CYNEFIN DECISION FRAMEWORK

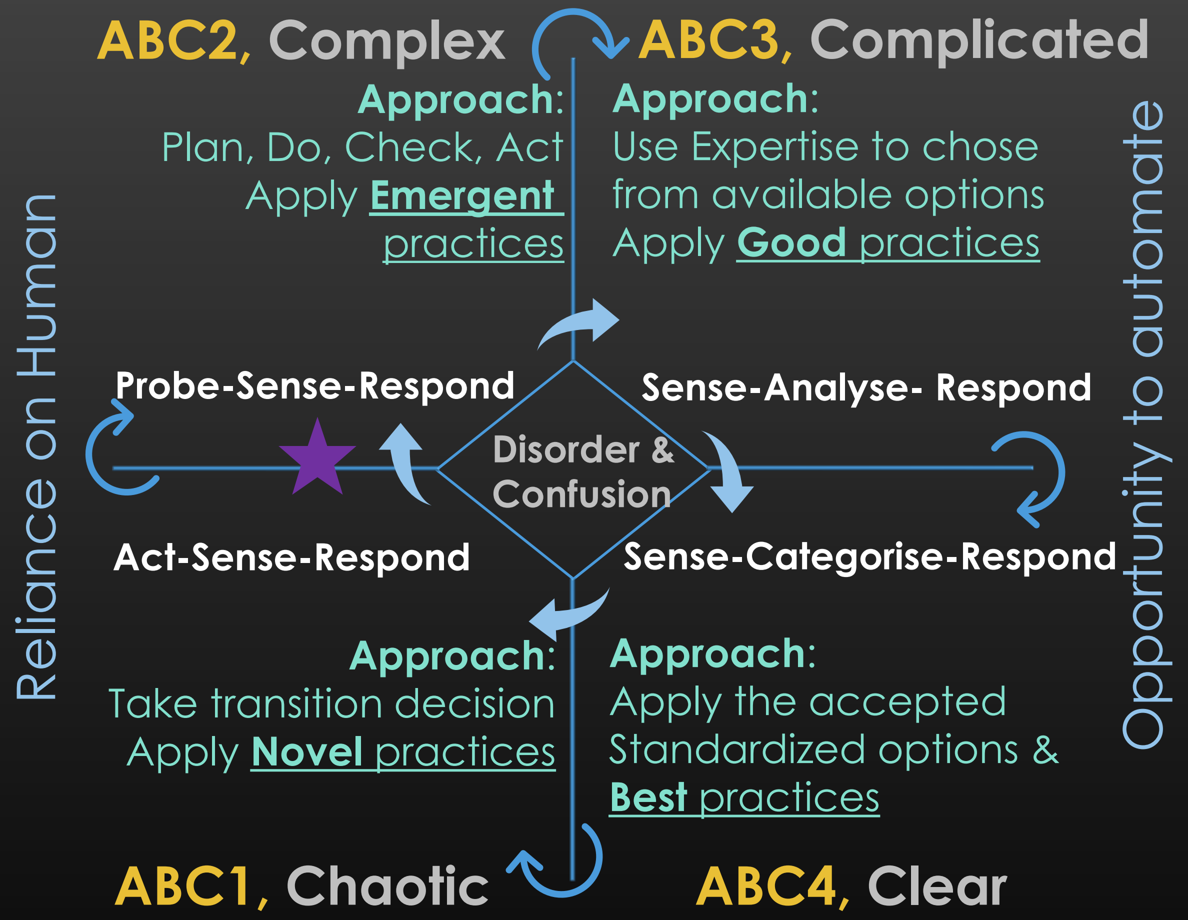
Change Definition:
Structural Challenges
Difficult to Change

Change driven by?:
Crisis

What can you do?:
Risk Management

What you invest in?:
Services

Process are established and repeatable



Reliance on Human

Opportunity to automate

ABC2, Complex

Approach:
Plan, Do, Check, Act
Apply **Emergent** practices

ABC3, Complicated

Approach:
Use Expertise to chose from available options
Apply **Good** practices

Probe-Sense-Respond

Sense-Analyse- Respond

Disorder & Confusion

Act-Sense-Respond

Sense-Categorise-Respond

Approach:
Take transition decision
Apply **Novel** practices

Approach:
Apply the accepted Standardized options &
Best practices

ABC1, Chaotic

ABC4, Clear

Unaccounted edge-cases may result in chaos

Change Definition:
Changeable Design
Enables Control

Change driven by?:
Problems

What can you do?:
Fix the problem

What you invest in?:
Technology

Accelerated, Better, Cheaper (ABC)
Pick from options ABC1,ABC2,ABC3 or ABC4

© www.linkedin.com/in/sudhaeiyer

ROADMAP FOR YOU

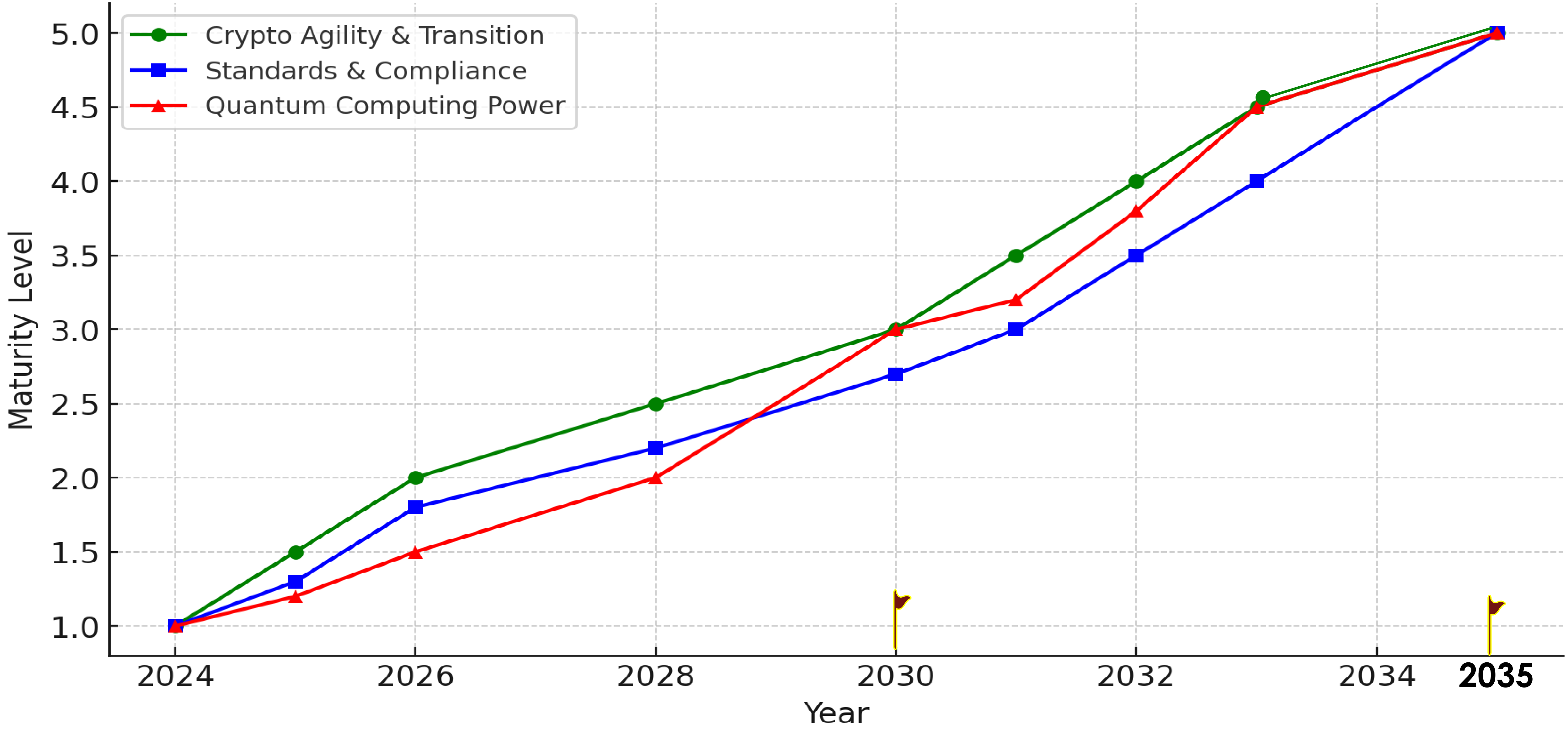
- **2025-2028** (Tactical plan):
  - Build Inventory of whatever you can
  - Partner with your current vendors
  - Test all PQC developer tools and libraries
  - Document your own lessons learnt
  - Kick start your strategic replacement
  - Kick off the budget & resourcing plan
- **2029-2035** (Implementation Plan):
  - Full PQC adoption execution
  - Compliance alignment execution
  - Can review/implement QKD solutions

You are here

Timeline	2024	2025	2026	2028	2030	2031	2032	2033	2035
Quantum Computing Power	**5k gates,** Classical Modularity + Quantum Circuits		**7.5k gates,** Quantum Modularity	**15k gates,** Quantum Modularity	**100 Million gates** Error Corrected and stable quantum modularity			**1Billion gates** unlocking Fully **Powerful Quantum-centric super computers**	
Standards & Compliance Timeline	Initial NIST Standards & US Gov Memo	NIST include more PQC options	**IETF standards Inter-op & Reference architectures**	HSM, Modules and libraries certifications	PCI DSS SWIFT etc	Increased **Regulatory Scrutiny**	ISO, OWASP, etc	Accessibility to **standardized and certified vendor options** for implementation	
Org & Sector Crypto Agility & Transition Timeline	**Incorporate PQC Standards** in their Cyber Standards	**Begin analysis** Of your **supplier** & Crypto-agility solutions	**Impact analysis** of algorithms of **strength less than 128 bits** SHA, AES, RSA, ECDH, ECDSA.	**Mandatory Replacement** algorithms of strength less than **128 bits SHA, AES, RSA, ECDH, ECDSA**		Tested all current supplier solutions with PQC designs	**Mandatory Retirement** of **all** RSA, ECDH & ECDSA In parallel, Evaluate new Quantum-enabled solutions		**Quantum enabled Networks**
Maturity	Initial					Managed		Defined	

Timetable for your Quantum Resilience

Quantum Resilience Timeline Depiction



Scaling this **cryptographic cliff** within the time is crucial.

© www.linkedin.com/in/sudhaeiyer

CALL TO ACTION

- **Start your tactical plan today**
- Engage with active industry groups directly working with NIST, IETF, **PKI Consortium and its PQC group**.
- **Evaluate PQC solutions** with or without vendors
- Monitor NIST, IETF standards and PQC group updates
- **Prepare** for regulatory adoption deadlines

CLOSING THOUGHTS

- PQC transition is a mandate
- Time is running out, but resilience is achievable
- Collaboration is key to success