HOW CAN BUSINESSES RESPOND TO THE QUANTUM THREAT TO CRYPTOGRAPHY?
ASSESSMENT
ASSESSMENT

RISK
Risk Questions

MAGNITUDE: What risks will information disclosure create? (Monetary loss, Compliance, Legal, Reputation)

DURATION: How long must confidentiality be maintained for each asset class?

SCOPE: Do you issue keys or certificates to third parties? Under what CPSs or SLAs?

DURATION: Can you quantify damage due to degradation or interruption of each service that uses crypto?

RESPONSE: Is there a plan to protect encrypted assets in case of a crypto failure?
ASSESSMENT

DATA
Data Questions

- **TYPE:** What classes of data do I encrypt? (PII, Trade Secret, Custodial Secret, Govt Classified...)?
- **PROTECT DURATN:** How long must confidentiality be maintained for each data class?
- **RETENTN:** Is encrypted data deleted according to a regular schedule?
- **DISCLOSURE IMPACT:** What are the consequences of disclosure of each data class?
- **EXPOSURE:** Is encrypted data normally exposed to potential attackers? (e.g., in transit or public cloud)?
ASSESSMENT

KEYS
Key Questions

- **TYPE**: What are the strength, algorithm binding, and usage (sign vs encrypt, application, etc...) of each key?
- **STRENGTH**: What is the effective strength of each key, vs. classical and quantum attack?
- **LIFETIME**: What are the issuance and expiration dates for each key?
- **MANAGEMENT**: Are all keys inventoried and locatable? Are keys easy to revoke and reissue?
Infrastructure Questions

- CRYPTO SOFTWARE INVENTORY: What crypto libraries are in use? What protocol libraries are in use?
- CRYPTO HARDWARE INVENTORY: What crypto hardware is in use?
- KEY INVENTORY: What keys are in use, by what applications?
- ADMIN INVENTORY: Who is authorized to manage which keys and which crypto modules and devices?
- CERTIFICATE INVENTORY: What certificates are issued to the organization? Who issued them? What attributes does each certificate have?
- APPLICATION INVENTORY: Which applications use which libraries, which keys, and which protocols?
Supplier Questions

CA: Do my CA agreements hold the CA to an SLA for timely reissuance? Do I have a backup CA under contract?

Are my CAs obligated and prepared to revoke certificates en masse in case of an algorithm breach?

MY CSRs: Have I installed my CSRs so I can request reissuance of certs with the correct attributes?

CODE SIGNATURES: Can and will my application vendors re-sign applications in a timely way?

SIAs CA): Do my revocation and reissuance requests get priority vs. others in emergencies?

SIAs Data Custodian): What obligations do custodians of my data have in case of an algorithm breach?

SIAs Software Vendor): Are my vendors obligated to timely upgrades to fix crypto breaches?
PREPARATION
PREPARATION

ORDERLY MIGRATION
Orderly Transition Planning

- **SUPPLIER READINESS PLANS:** Do your suppliers have quantum readiness plans? Do your contracts require them?
- **CRYPTO AGILITY:** Will your infrastructure support rapid replacement of crypto algorithms and protocols?
- **STANDARDS PARTICIPATION:** Are you participating in standards groups preparing for PQC?
- **PRODUCT TESTING:** Are you testing and certifying PQC algorithms and PQC-enabled products in advance?
- **HYBRID CRYPTO:** Are you investigating or implementing hybrid classical/PQC modes of operation?
- **REGULATORY ENGAGEMENT:** Are you engaging with regulators on use of PQC?
PREPARATION

EMERGENCY MIGRATION
Disorderly Transition Planning

EXERCISES: Are you planning and executing tabletop and simulation exercises for crypto algorithm failure response?

CA AGREEMENTS: Are you updating your CA agreements to cover algorithm failure?

SUPPLIER AGREEMENTS: Are you updating your supplier and partner agreements to cover algorithm failure?

SAVED CSRs: Are you retaining your Certificate Signing Requests to support emergency cert issuance?

EMERGENCY SOFTWARE DISTRIBUTION: Are you making arrangements to securely receive and deploy patches and updated software versions while network protocol and code signing cryptography is insecure?

E-RISK COVERAGE: Are you investigating Cyber Insurance for cryptographic algorithm failures?
MIGRATION
M igration

RESPONSIBILITY: What executive is responsible for Quantum Safety?

PROJECT MANAGEMENT: Is there a detailed plan for Quantum Safety? What is its priority?

BUDGET: Is there a budget for Quantum Safety projects?

METRICS AND TRACKING: Are there metrics for Quantum Safety? To whom are they reported?
MITIGATION
Mitigation

- **EXERCISES:** Are you planning and executing tabletop and simulation exercises for crypto algorithm failure response?
- **STAKEHOLDER ENGAGEMENT:** Are Legal, Compliance, and Corporate Communications involved in planning?
- **BUDGET:** Is there a budget for mitigation of crypto algorithm failures?
- **PLAYBOOKS:** Have exercises been used to create playbooks for mitigation?
QUESTIONS