Board Briefing — Quantum Exposure & Cryptographic Assumption Risk

Board-level assessment of quantum-related cryptographic risk, aligned to executive policy and stress testing. Focus: exposure duration, assumption expiry, and required executive decisions.

Area	Board Question	Current Posture
Long-Term Confidentiality	Do any data classes require confidentiality beyond 10–20 years?	Yes / No
Tier-1 Crypto Exposure	Are Tier-1 systems dependent on RSA or ECC?	Yes / No
Harvest-Now Risk	Could encrypted traffic collected today be decrypted later?	Yes / No
Crypto Agility	Can cryptographic algorithms be replaced without redesign?	Yes / Partial / No
Migration Governance	Are time-bound migration decisions approved?	Yes / No

Tier-1 Cryptographic Exposure Register (Template)

Inventory of cryptographic dependencies for Tier-1 systems. All entries must be evidence-backed.

Tier-1 System	Crypto Use	Algorithm	Externally Exposed	Rotation Capability	Notes

Quantum Assumption Register

Explicit cryptographic assumptions with owners and expiration. Undocumented assumptions are unmanaged risk.

Assumption	Applies To	Expiration Date	Owner	Status
RSA/ECC acceptable for external TLS	Tier-1 Internet Services		CISO	Accept / Replace
Encrypted data confidentiality < X years	Data Class ___		Data Owner	Accept / Revise
Vendors will migrate before deadline	Critical Vendors		Procurement	Accept / Challenge

Required Executive Decisions & Attestation

Decisions below must be approved, rejected, or explicitly time-bound.

Decision Item	Approve / Reject	Notes
Define long-term confidentiality requirements by data class		
Set Tier-1 crypto migration deadlines		
Mandate crypto agility standards		
Deprecate non-migratable systems		

Risk Acceptance Effective Date: ____________________

Risk Acceptance Expiration Date: ____________________

Next Mandatory Review Date: ____________________

Role	Name	Signature	Date
CEO			
CISO			
CIO			
General Counsel			
Board Risk Chair			