Quantum Security Data Risk - A Clear Path to Maximum Risk Reduction

Quantum Risk Puts Encryption Strategy at the Center of Data Governance: A MYTHOS Attack-Aligned Path to Maximum Risk Reduction

TL;DR

"Harvest Now, Decrypt Later" (HNDL) is an **active business risk today**. Adversaries are already exfiltrating your encrypted long-lived sensitive data. By applying the proven **MYTHOS AI Security** sequenced framework — **Policy → Fundamentals (CCS) → Risk Tiering → AI/NHI IAM → Governance** — organizations *achieve the highest business centric risk-reduction value:* classify data by longevity, inventory cryptographic assets, harden the foundational floor, migrate PQC on priorities, and govern as enterprise resilience. This delivers measurable protection for IP, AI models, credentials, and customer records with disciplined, business-value-driven execution.

Executive Summary

Quantum computing threatens to break classical asymmetric cryptography (RSA, ECC, Diffie-Hellman), but the exposure window is already open due to the **Harvest Now, Decrypt Later (HNDL)** threat. Sensitive data stolen today in encrypted form can be decrypted once quantum capabilities mature, creating long-term competitive, financial, and regulatory risk.

This is not primarily a technical CISO issue — it is a **core enterprise data governance and operational resilience challenge** that directly impacts business value, revenue protection, and executive accountability. Organizations that act strategically using the MYTHOS approach will protect their most valuable long-lived assets while building cryptographic agility as a competitive advantage.

Business Value of Following This Path:

- Protects revenue-generating and mission-critical assets (IP, proprietary processes, AI model weights, regulated customer data).
- Dramatically reduces expected loss from future quantum-enabled breaches.
- Demonstrates due diligence to boards, regulators, insurers, and courts.
- Leverages the same KISS + risk-based logic that makes MYTHOS effective for AI security: fundamentals first (>60% risk reduction), then targeted controls.

Community & Industry Best Practices for HNDL (2025–2026 Consensus)

Leading standards bodies (NIST, NSA, ENISA), practitioners, and organizations (Google, AWS, Meta, Cloudflare) converge on these high-ROI practices:

- **Data Classification & Longevity Analysis First** — Identify data requiring confidentiality for >10 years using Mosca's inequality to quantify HNDL exposure.
- **Continuous Cryptographic Inventory (Crypto BOM)** — Map all RSA/ECC/DH usage across systems, APIs, AI agents, and data stores as ongoing asset management.
- **Crypto-Agility by Design** — Architect systems for seamless algorithm swaps without major rewrites.
- **Hybrid PQ/T Deployments** — Layer NIST PQC algorithms with classical cryptography during the transition period.
- **Foundational Hygiene (Verify the Floor)** — Data minimization, retention tightening, AES-256 strengthening, Zero Trust segmentation, and air-gapping before full PQC migration.
- **Risk-Based Prioritization** — Focus on external-facing systems, long-life sensitive data, key management, AI/NHI IAM, and CNSA 2.0 milestones.
- **Executive Governance & Ownership** — Integrate into FAIR models, Business Impact Analysis, board reporting, and vendor assessments for legal and regulatory defense.

These practices align directly with the **MYTHOS AI Security Standard**.

Why the MYTHOS AI Security Approach Provides a Definitive Framework
MYTHOS simplifies complex security domains (AI, supply chain, quantum, etc.) through KISS principles combined with business-value risk management.
Core Philosophy:

- **FIRST — HAVE AN AI SECURITY APPROACH**: Establish clear policy, data strategy (protection + use/governance), and **assume breach**.
- **Fundamentals Matter Most**: >60% of risk is addressed through basic hygiene (via **Cloud Cyber Shield — CCS**), which verifies and thwarts the majority of top threat vectors with cloud-native, verifiable controls.
- **Top 11 Threats Focus**: Prioritize root causes that drive real damage rather than chasing outliers. HNDL acts as a powerful long-horizon amplifier of existing data exposure and identity risks.
- **3-Layer Risk Model**: 1) Fundamentals/CCS (~65%), 2) AI-Specific Controls (~20%), 3) Governance (~15%).
- **Supporting Standards**: AI/NHI IAM (CoSAI, AISVS, NIST, SPVS) for agent lifecycle management, plus Integrated AI Governance (guardrails, tech/ops execution).

Quantum risk maps cleanly onto this structure, making MYTHOS the ideal lens for maximum risk reduction.

The Core Logic: Follow the MYTHOS Sequence

MYTHOS Step	Quantum Action
Step 1 — Policy	Add cryptographic agility and quantum risk policy
Step 2 — Inventory	Inventory all cryptographic assets (RSA/ECC usage)
Step 3 — Cyber Floor (CCS)	Verify encryption hygiene; tighten retention; Zero Trust
Step 4 — Risk Tiering	Classify data by sensitivity lifetime & HNDL thresholds
Step 5 — AI / NHI IAM	Apply PQC to agent credentials, tokens, key exchange
Step 6 — Integrated Governance	Build agility into governance and evidence artifacts

The Sequenced Path: Fastest Risk Reduction First
STEP 1: Know What You're Protecting — Data Classification Highest-value immediate action. Identify long-life sensitive data (intellectual property, formulas, differentiated processes, regulated customer records, AI model weights — anything that will still matter in 10+ years). Start with revenue- or mission-critical departments. **Required Artifacts**: Data sensitivity register (tagged by retention life and impact), C-suite owner assignments, FAIR-quantified loss thresholds. **MYTHOS Alignment**: Step 4 Risk Tiering.

STEP 2: Cryptographic Asset Inventory Map every system using asymmetric cryptography (RSA, ECC, Diffie-Hellman). **What to Inventory**: TLS/SSL, VPNs, digital signatures, KMS/HSMs, AI agent authentication, data-at-rest encryption. **Required Artifacts**: Cryptographic asset register (system, algorithm, key length, sensitivity, priority) + gap list. **MYTHOS Alignment**: Step 2 Inventory/Visibility. NIST IR 8547 guidance.

STEP 3: Verify the Cryptographic Floor — Immediate Mitigations

- Data Minimization & Retention Tightening: Delete what you don't need.
- Zero Trust for High-Value Stores: Enforce unavailability by default.
- Strengthen Symmetric Encryption: Migrate to AES-256.
- Isolate Long-Life Data: Segment and air-gap highest-risk stores. **MYTHOS Alignment**: Step 3 CCS Cyber Floor — foundational hygiene that blocks major attack paths.

STEP 4: Begin PQC Migration on Highest-Risk Systems Deploy NIST standards on zero-tolerance, long-life data:

- **FIPS 203 (ML-KEM)**: Key encapsulation / key exchange
- **FIPS 204 (ML-DSA)**: Primary digital signatures
- **FIPS 205 (SLH-DSA)**: Backup signatures

Priority Order: External TLS → Key management → AI agent channels → VPNs (CNSA 2.0 2026) → Legacy. **Recommendation**: Use **PQ/T Hybrid schemes** (ENISA 2025 guidance) during transition.

STEP 5: Apply PQC to AI Agent Identity and Credentials Agentic systems are prime HNDL targets. Apply ML-KEM/ML-DSA, enforce short-lived credentials, and embed crypto-agility in NHI IAM. Use PQ-safe signing for Attestorr/VEL2 long-lived records. **MYTHOS Alignment**: Step 5 AI/NHI IAM.

STEP 6: Govern Quantum Risk as Enterprise Operational Resilience Assign executive ownership (CISO/CRO), integrate into vendor assessments and FAIR/BIA models, report to the board, and align with PQCC Roadmap and CNSA 2.0. **CNSA 2.0 Milestones**: 2025 (signatures/web), 2026 (VPNs), 2027 (OS), 2030 (legacy), 2035 (full). **MYTHOS Alignment**: Step 6 Integrated Governance.

Risk Reduction Summary

#	Action	Risk Reduction Value	Timeline
1	Data classification & ownership	Eliminates unknown exposure	Immediate
2	Cryptographic asset inventory	Closes visibility gap	30–60 days
3	Floor hardening (AES-256, Zero Trust, retention)	Immediate HNDL surface reduction	60–90 days
4	Hybrid PQC on highest-risk systems	Protects core business assets	6–18 months
5	AI/NHI IAM PQC	Secures agent trust chains	12–24 months
6	Enterprise governance & CNSA alignment	Defensible posture + legal shield	Ongoing

What This Is Not

This path does **not** require a complete cryptographic overhaul on day one. It applies the same MYTHOS discipline used across AI and other domains: verify the floor, classify risk, constrain exposure, and govern execution. Organizations that ignore HNDL or start with advanced tooling before fixing fundamentals face the greatest exposure.

Executive Liability Note

Courts and regulators are increasingly holding executives accountable for known long-horizon risks, consistent with privacy liability evolution. Documented awareness and action on HNDL provides both risk mitigation and legal defense (as emphasized by Jon Murphy / The Security Digest).

Key References (Top Authoritative Sources):

1. **NIST IR 8547 & NCCoE Post-Quantum Migration Project**
   - NIST IR 8547: https://csrc.nist.gov/pubs/ir/8547/ipd
   - PDF: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf
   - NCCoE Project: https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc
2. **NSA CNSA 2.0**
   - Official Advisory (PDF): https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF
3. **ENISA Post-Quantum Cryptography Guidance**
   - Main Page: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation
   - PDF (v2): https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Post-Quantum%20Cryptography%20Current%20state%20and%20quantum%20mitigation-V2.pdf
4. **Palo Alto Networks HNDL Practical Guides**
   - Harvest Now, Decrypt Later: https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl
5. **Jon Murphy / The Security Digest (May 2026)**

- Main Article: https://www.thesecuritydigest.com/news/jon-murphy-quantum-computing-threatens-encryption-security
- LinkedIn Post: https://www.linkedin.com/posts/jonemurphy_thesecuritydigest-cybersecurity-quantumrisk-share-7465737453283221504-9RZS/

Sources: NIST FIPS 203/204/205 (August 2024), CNSA 2.0, ENISA Agreed Cryptographic Algorithms v2 (2025), PQCC Migration Roadmap, MYTHOS AI Security Standard, and industry best practices (2025–2026).
This document serves as the **definitive, actionable reference** for organizations seeking maximum quantum risk reduction through disciplined, MYTHOS-aligned execution.

Appendix: WHAT TO DO Guide — Quantum Risk Reduction Project Plan & Implementation Roadmap

This appendix provides a **ready-to-execute project plan** with detailed, step-by-step guidance for cross-functional teams.

Quick-Start Checklist (Days 1–30)

- Appoint Executive Sponsor (CRO/CISO + Business Unit Lead)
- Kick off Policy update (Step 1)
- Launch parallel Data Classification + Crypto Inventory
- Complete CCS Floor self-assessment
- Publish initial Risk Register + 90-day milestones

Phased Project Plan Overview

Phase / MYTHOS Step	Key Activities	Deliverables	Timeline	Responsible	Success Metrics
Preparation & Policy (Step 1)	Draft policy; secure sponsorship	Approved Policy & Charter	Week 1–2	CISO + CRO	Policy approved
STEP 1+4: Data Classification & Risk Tiering	Identify long-life data; assign owners; FAIR thresholds	Sensitivity Register	Weeks 1–4	Business Owners + Risk	100% high-value data classified
STEP 2: Cryptographic Inventory	Build CBOM & gap analysis	Cryptographic Asset Register	Weeks 2–8	Security Architecture	95%+ coverage
STEP 3: Floor Hardening (CCS)	Minimization, AES-256, Zero Trust	Hardened controls report	Weeks 4–12	Infrastructure	AES-256 compliance + segmentation
STEP 4: PQC Migration (High-Risk)	Hybrid pilots & rollout	Protected systems	Months 3–12	DevSecOps	Top risk systems migrated
STEP 5: AI/NHI IAM PQC	Agent credential hardening	Updated IAM standard	Months 6–18	AI + IAM Teams	All agent channels PQC-enabled
STEP 6: Governance	Board reporting & sustainment	Governance dashboard	Month 6+	CRO + CISO	Quarterly executive reviews

Detailed Step-by-Step Guidance

USE YOUR AI TOOL TO FILL IN DETAILS / SAMPLE ARTICFACTS, ETC)

STEP 1: Policy – Cryptographic Agility & Quantum Risk Policy What to Do: Update existing security/AI policy to include quantum risk, cryptographic agility requirements, HNDL assumptions, and responsibilities. **Sample Artifacts**:

- Quantum Risk Addendum (1–2 pages)
- RACI matrix for quantum readiness
- Board briefing deck (2 slides) **References & Tools**: MYTHOS Policy templates, NIST SP 800-131A, CNSA 2.0. **Success Criteria**: Policy approved by leadership; communicated to all engineering and AI teams.

STEP 1 + 4: Data Classification & Risk Tiering What to Do: Inventory data classes by confidentiality lifetime (>10 years), assign C-suite owners, apply FAIR quantification, and calculate HNDL exposure using Mosca's inequality (Years data must remain secret + Years to migrate > Years until quantum break). **Sample Artifacts**:

- Data Sensitivity Register (Excel/Sheet): Columns = Data Class, Owner, Retention Period, Business Impact ($), HNDL Tier (Zero-Tolerance / Medium / Low), Mosca Score.
- Loss Threshold Matrix. **References & Tools**: FAIR Institute methodology, NIST SP 800-60, Mosca's "Quantum Threat Timeline". **Success Criteria**: All revenue-critical and regulated data classified and owned.

STEP 2: Cryptographic Asset Inventory What to Do: Conduct discovery scans across on-prem, cloud, and AI systems. Build a living Cryptographic Bill of Materials (CBOM). **Sample Artifacts**:

- CBOM Register: System Name | Algorithm | Key Size | Data Sensitivity | Exposure Risk | Migration Priority | Owner.
- Gap Report with prioritized remediation list. **References & Tools**: NIST NCCoE Cryptographic Discovery Tools, CycloneDX CBOM format, open-source tools (e.g., sslscan, crypto-agility scanners), PQCC Inventory Workbook. **Success Criteria**: 95%+ coverage of production environments; high-risk gaps quantified.

STEP 3: Verify & Harden the Cryptographic Floor (CCS) What to Do: Implement immediate mitigations using existing tools while PQC migration ramps up. **Sample Artifacts**:

- Updated Data Retention Policy
- Zero Trust Architecture Mapping for sensitive stores
- AES-256 Compliance Report
- Air-Gap/Segmentation Diagram for highest-risk data. **References & Tools**: CCS Framework, CISA KEV Catalog, NIST SP 800-207 (Zero Trust), ENISA guidance. **Success Criteria**: All high-sensitivity data minimized or segmented; 100% AES-256 on relevant systems.

STEP 4: PQC Migration on Highest-Risk Systems What to Do: Start with hybrid deployments on external-facing and long-life data systems. Follow risk-based priority order. **Sample Artifacts**:

- Hybrid PQ/T Implementation Plan
- Pilot Test Report (performance, compatibility)
- Updated System Configuration Standards. **References & Tools**: NIST FIPS 203/204/205 libraries, AWS/Google hybrid guidance, ENISA 2025 Hybrid Recommendations, CNSA 2.0. **Success Criteria**: Top 3–5 highest-risk systems protected with hybrid or full PQC.

STEP 5: Secure AI Agent Identity & Credentials What to Do: Integrate PQC into agent lifecycle, session tokens, and inter-agent trust. **Sample Artifacts**:

- Updated NHI IAM Standard (with crypto-agility clause)
- Agent Credential Policy (short-lived + PQ algorithms)
- PQ-signed Attestorr/VEL2 execution records. **References & Tools**: MYTHOS AI/NHI IAM Standard, CoSAI, AISVS, NIST SP 800-63, FIPS 203/204. **Success Criteria**: All agent key exchange and signing use PQC; short-lived credentials enforced.

STEP 6: Enterprise Governance & Operational Resilience What to Do: Embed into enterprise risk processes, vendor management, and board oversight. **Sample Artifacts**:

- Quantum Risk Dashboard (tracking KPIs)
- Vendor RFP/SLA Crypto-Agility Clause Template
- Quarterly Board Report Template
- Annual Crypto-Agility Refresh Plan. **References & Tools**: PQCC Migration Roadmap, FAIR + BIA integration, Jon Murphy governance framing. **Success Criteria**: Quarterly executive reviews established; all new systems/vendors crypto-agile by default.

This comprehensive appendix turns the strategic guidance into an executable program. Organizations following this plan will achieve rapid, high-value risk reduction while building long-term cryptographic resilience.

APPENDIX: **mythos based approach**

start simple, just use "CCS" (embedded CSP controls) to significantly reduce risk **right now**

Biggest AI / cyber threat overlooked?
Inability to grasp that FUNDAMENTALS MATTER for "everyone" -about 2/3 of ALL avoidable risk - add AI enabled effects > 80%!
always start there, don't chase outliers, as those controls are minimally useful without the foundation

1st - Use a data¬-driven analysis —TOP 11 THREATS! Don't chase outliers. Use root causes in optimum mitigation strategies, proven risk prioritization schema
https://docs.google.com/document/d/1Aijnq3XISg5ylOgbSJSF3Lz8XB24_KZh/edit

THEN "CCS" verifies & thwarts 90+% of those 11 threat entry vectors. CSP/Cloud Cyber Shield
Cuts cloud breach likelihood by 65– 80+%, addresses 90+% of CIS IG1 controls (many in IG2 & NIST CSF) the epitome of KISS, no new costs, quick and straightforward
https://docs.google.com/document/d/12wbqLUcbGjay88DEHiXo470VefrYsMqN/edit
A straightforward 2+ page CCS SoP checklist
https://docs.google.com/document/d/1INK2M4e7AVWRmM5p3w8M6rERjaIZUhUz/edit

A simplified AI Security Model – 3 Layered RISK based Control Stack - minimize the fog of all those frameworks, views, etc Aligns with NIST CSF 2.0, OWASP Top 10 for LLMs, CSA AICM, most others – whereas 85% of AI loss is still classic cyber + amplification
Layer 1: 60–70% (HYGIENE).
Layer 2: 15–25% (closes AI attack surface, OWASP)
Layer 3: 10–20% (governance, regulatory/reputational).
https://docs.google.com/document/d/1iPpuroFkTb9nItb3UZBIh1-zxBb_GBWC/edit

An overall AI / NHI IAM Standard – for implementable technical governance in this complex space - manage agent lifecycle identities
USES: CoSAI, AISVS, NIST COSAiS, & SPVS
https://drive.google.com/file/d/1vgeG9OSWrbvpyqYOXsXZoq8ylsJdpA-5/view

Overall AI Governance Approach – guardrails with tech and ops implementation guidance.
https://docs.google.com/document/d/1jwlTK3qWBgk1fUFtVls20B4ydNDlklX0/edit

two part integration view of the approach
https://docs.google.com/document/d/1mzbDeMmXPM3o3Mui6vbA8vlR1DRT02qn/edit