

IMPLEMENTING PQC PROTECTION IN THE VITAL RECORDS MANAGEMENT FUNCTION



DATA CENTER ASSISTANCE GROUP, LLC

By:

Thomas Bronack, President

Data Center Assistance Group, Inc.

bronackt@dcag.com | bronackt@gmail.com

Phone: (917) 673-6992

Website: <https://www.dcag.com>

Implementing PQC Protection in the Vital Records Management Function

Prepared by Data Center Assistance Group, LLC

Table of Contents

Contents

Executive Summary	3
Understanding the HNDL Threat	3
New Functional Responsibilities.....	3
Cost and Risk Comparison	3
Cost-Benefit and ROI	4
Project Plan: 12–18 Months	4
Strategic and Client Benefits	4
Next Steps	5
Call to Action.....	5

Executive Summary

This document outlines how to integrate Post-Quantum Cryptography (PQC) into the Vital Records Management (VRM) function of enterprises. It addresses how to protect both past records stored in physical and digital vaults and new records as they are ingested, transported, or retrieved. The strategy mitigates Harvest Now, Decrypt Later (HNDL) threats posed by future quantum computers.

Understanding the HNDL Threat

HNDL is a tactic used by adversaries to intercept and store encrypted data today, with the intent of decrypting it when quantum computers become powerful enough. PQC ensures long-term confidentiality using quantum-resistant algorithms, such as CRYSTALS-Kyber and Dilithium.

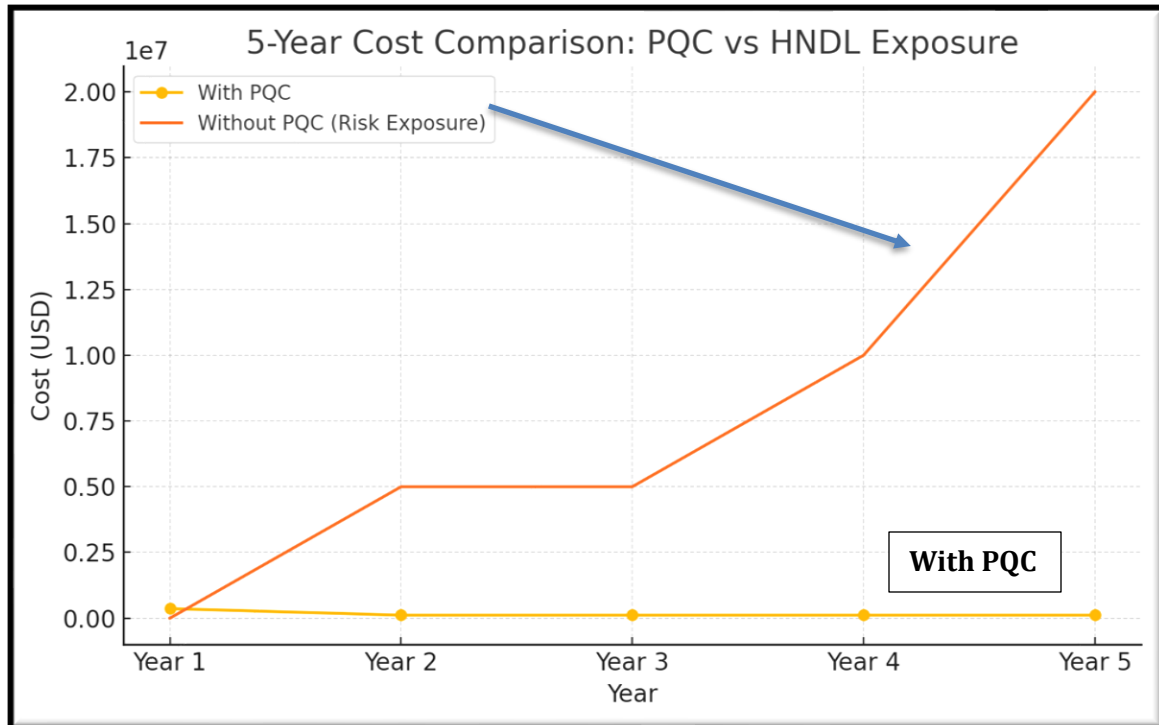
Analogy: Think of current encryption as a steel lock—strong today but vulnerable to future lock-picking tools (quantum decryption). PQC is like upgrading to a biometric vault door—unbreakable by future tools.

New Functional Responsibilities

- Integrate PQC-capable encryption during record ingestion and retrieval
- Maintain crypto-agility for vault rotation
- Train staff on hybrid encryption operations
- Conduct cryptographic audits for compliance and key lifecycle management

Cost and Risk Comparison

Estimated 5-year cost with PQC vs projected liabilities without PQC:



Cost-Benefit and ROI

PQC implementation cost: ~\$940,000 over 5 years.

Potential HNDL-related liability: \$30M–\$50M depending on regulatory, legal, and reputational fallout.

ROI exceeds 30x over the 5-year period, with measurable risk reduction and compliance gains.

Project Plan: 12–18 Months

1. Identify existing vault content at risk for HNDL.
2. Select vendors (e.g., Analysis of Alternatives - AoA) and upgrade vault infrastructure.
3. Begin re-encryption with hybrid PQC layers for existing records.
4. Transition future record ingestion to PQC-compliant processes.
5. Audit and validate cryptographic operations annually.

Strategic and Client Benefits

- Improves client trust and regulatory alignment
- Enhances disaster recovery and long-term data resiliency

- Positions the enterprise as a quantum-resilient vaulting provider

Next Steps

- Conduct vault audit for cryptographic exposure
- Issue RFPs for PQC vendor support and conduct AoA
- Launch proof-of-concept for PQC vault integration
- Train staff and implement crypto-lifecycle governance

Call to Action

Secure Your Data Supply Chain Today

- The **quantum threat** is real and approaching rapidly
- **Present data is exposed** to HNDL attacks by Hackers
- PQC implementation is a strategic necessity
- DCAG provides expert guidance through the entire process

Contact us to begin your quantum-safe journey

DCAG

PQC Advisory Group

Email: bronackt@dcag.com

Phone: (917) 673-6992

Schedule a Consultation

7/18/2025

Copyright 2025 © Data Center Assistance Group, LLC,

Page: 19