

Q-ARM: Quantum-Adjusted Risk Mitigation

From Theoretical Assessment to Adaptive, Private Action.

Operationalizing PQC Risk: How to do More with Less, Faster, Better, and Cheaper.

Presenter: [Your Name/Team]

- ❏ **Core Message:** We provide the first unified platform that dynamically scores PQC risk and automatically prioritizes migration tasks, secured by **Differential Privacy**.

The Quantum Threat: A Single Vulnerability, Global Risk

What is the Threat?

A large-scale, fault-tolerant Quantum Computer (**CRQC**) will break the two most common public-key encryption standards globally:

- **RSA** (via Shor's Algorithm)
- **ECC** (Elliptic Curve Cryptography)

What is PQC? Post-Quantum Cryptography (PQC) refers to new, mathematically complex algorithms (like Lattice-based schemes) designed to resist attacks from quantum computers.



Why Now? (The Immediate Danger)

Harvest Now, Decrypt Later

Adversaries are currently stealing and storing encrypted data today.



Future Decryption

When a CRQC is available (\$Z\$), they will retroactively decrypt all captured data.



Immediate Mandate

Today's data is vulnerable for its entire confidentiality lifetime (\$X\$). Action cannot wait.

The Hard Problem: The Quantum Deadline is a Moving Target



Unpredictable Timeline

The \$Z\$ (CRQC Horizon) is constantly changing. Static, multi-year planning is already obsolete and costly.



Inventory Complexity

Organizations manage millions of crypto assets. Current tools lack the necessary **context** to prioritize which assets matter most.



Data Blindness

Prioritization fails without knowing the exact value and vulnerability (Exposure/Harvestability) of each asset.

Current Status Quo

Most organizations are stuck in Phase 1: **Inventory & Auditing**.

Few have an accurate, adaptive financial model for Phase 2: **Risk Assessment**.

Q-ARM moves you immediately into an operational, adaptive Risk phase, bypassing the "stuck" state.



Our Foundation: Built on Recognized Frameworks

Our methodology integrates established academic principles with continuous, dynamic modeling.



Mosca's Inequality

The foundational logic for migration urgency:
 $\$X+Y > Z\$$. ($\$X\$$ = Confidentiality lifetime, $\$Y\$$ = Migration time, $\$Z\$$ = CRQC Availability).



The PAREK Framework

We align with the five recognized PQC readiness phases: Planning, Assessment, Risk, Execution, Key Governance.



The QARS Model

We maintain the Quantum Asset Risk Score structure, making our output immediately comparable to existing academic work.

The core QARS calculation remains:

$$QARS = \omega_T \cdot T + \omega_S \cdot S + \omega_E \cdot E$$

The Innovation: We make the ω weights dynamic and the process continuous based on real-time threat intelligence.

Architecture: The Three Stages of Q-ARM

Data Synthesis

CTGAN generates safe synthetic data to preserve asset privacy for model training.

HITL Loop

Differential Privacy (DP/SGD) secures human expert feedback fed back into the QARS engine.



QARS Engine

Dynamic weights + threat intelligence produce prioritized risk scores for actioning.

Key Takeaways



Stage 1: Data Synthesis

CTGAN creates safe, synthetic training data that avoids exposing sensitive asset details, ensuring privacy from the start.



Stage 2: QARS Engine

Dynamic Weights react to real-time threat intelligence feeds, continuously tuning the prioritization score.



Stage 3: HITL Loop

Human expert feedback refines the model's accuracy, with the learning process entirely secured by **Differential Privacy (DP/SGD)**.

Limitations and Future Research

Current Limitations (For Researchers)

- E-Factor Granularity

The ω_E (Exposure) boost is currently heuristic; we need formalized models for supply chain risk and post-quantum cryptography scoring.

- Model Generalization

DP classifier performance is limited by the diversity of the initial training data (the scored CSV used for synthesis).

- Deployment Costs

Assumes a continuous, real-time Threat Feed exists; integrating and maintaining this feed will incur operational overhead for clients.

Future Research Trajectories (Novelty)

→ Advanced DP Classification

Explore DP kernel methods or deep learning classifiers for improved non-linear prediction accuracy in risk scoring.

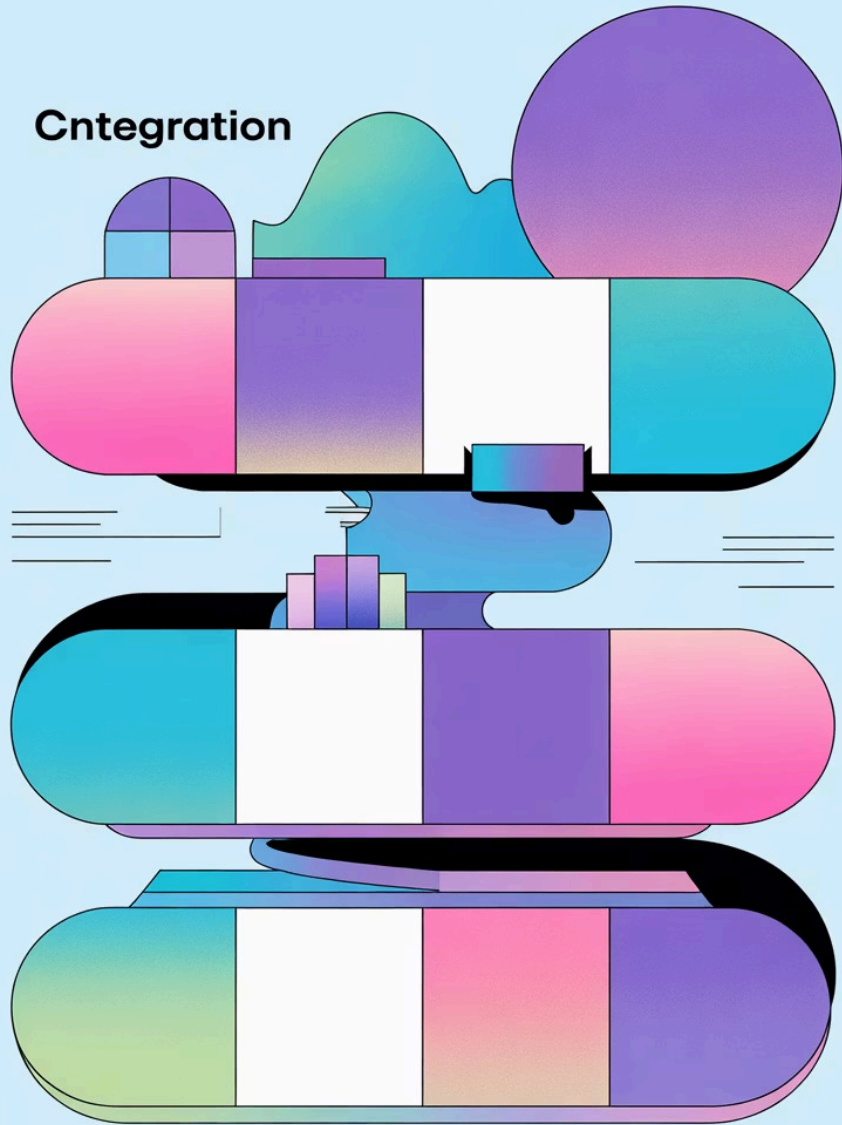
→ Dynamic Z Estimation

Integrate economic, geopolitical, and computing power metrics for a sophisticated, variable Z horizon estimate.

→ Federated Learning

Extend DP to a multi-organization framework for collaborative, private risk intelligence sharing across the industry.

Cntegration



Our Plan: From Proof-of-Concept to Production

A focused, phased approach to operationalize Q-ARM within your enterprise environment.

1

Phase I: Validation (Current Status)

Status: Q-ARM model logic is validated against the original paper's metrics. PoC Streamlit app operational.

Goal: Secure internal validation on [Specific Department/Data Set] to confirm real-world ROI metrics and efficacy.

2

Phase II: Integration (6 Months)

Goal: Integrate Threat Feed API/Service. Productionize the DP/SGD model as a continuous microservice. Formal integration with [Asset Inventory System, e.g., CMDB].

Output: Quantified, dynamic PQC migration pipeline.

3

Phase III: Expansion (12+ Months)

Goal: Extend QARS to cover other cryptographic risks (e.g., side-channel attack potential). Extend applicability to other risk domains (e.g., AI Governance).

Q-ARM: The Adaptive Standard for PQC Risk

The Adaptive Advantage



Dynamic Control

Risk is scored based on real-time threat intelligence, not static spreadsheets, guaranteeing up-to-the-minute prioritization.



ROI-Driven Accuracy

Prioritization is guaranteed to be accurate and cost-effective, ensuring you only spend migration resources where they matter most.



Future-Proof

Continuous DP-secured learning ensures the model stays current with evolving assets and expert knowledge, future-proofing your investment.

Call to Action: Executives

Fund the 6-month integration phase to quantify migration cost reduction and prove the ROI in your environment.

Contact: [Your Contact Information]

Call to Action: Researchers

Partner with us to extend the E-Factor model for post-quantum side-channel resistance research.