

Did an AI break the encryption protecting your business today? No.

The Headline Noise

“AI breaks post-quantum encryption.”

The rapid escalation of AI capabilities has created an environment where theoretical research is easily conflated with immediate, operational compromise.

The Factual Reality

Anthropic’s Claude Mythos Preview assisted a researcher in finding a weakness in HAWK—a candidate algorithm undergoing evaluation.

HAWK was never finalized and never deployed in business systems.

This incident is evidence of the open cryptographic review process working exactly as intended, not evidence that finalized post-quantum cryptography (PQC) is compromised.

[1] Anthropic: Discovering cryptographic weaknesses with Claude (July 28, 2026).

[2] NIST: Nine Candidates Advance to the Third Round of the Additional Digital Signatures for the PQC Standardization Process (May 14, 2026, Updated July 29, 2026).

The verified trajectory of the HAWK cryptanalysis incident

14 May 2026

NIST advances HAWK among nine candidates to Round 3 of additional digital-signatures evaluation.

Confirmed Fact

Anthropic publishes research demonstrating how AI-assisted cryptanalysis improved a key-recovery attack against the HAWK scheme.

28 July 2026

29 July 2026

The HAWK development team voluntarily withdraws the scheme from NIST consideration.

Operational Analysis

AI models can significantly accelerate research and vulnerability discovery in candidate cryptographic designs.

AI did not break production standards. Any scenario where AI instantly breaks deployed, finalized Post-Quantum Cryptography standards is currently **hypothetical**.

Differentiating withdrawn research candidates from finalized deployment standards

HAWK (What it was)

Status: A candidate in active evaluation.

Deployment: Never finalized. Never integrated into commercial business systems.

Outcome: Withdrawn from the standardization process.

ML-KEM & ML-DSA (What it is not)

Status: Finalized FIPS standards.

Foundation: Rely on completely different mathematical foundations than HAWK.

Deployment: Ready for immediate implementation and vendor procurement.

"This finding does not affect any of NIST's finalized PQC standards, such as ML-KEM and ML-DSA, which rely on different mathematical foundations that remain secure, and which are ready for implementation now."

— NIST Post-Quantum Cryptography Update

Singapore's CSA sets distinct quantum-safe milestones

Critical Information Infrastructure (CII)

31 March 2027

Submit quantum-safe migration plan to CSA.

2028

Quantum-safe considerations in new CII procurement.

31 December 2031

Migration completed for CII systems

Other Quantum-Exposed Organizations

End-2027

Target for having a formal migration plan in place.

2035

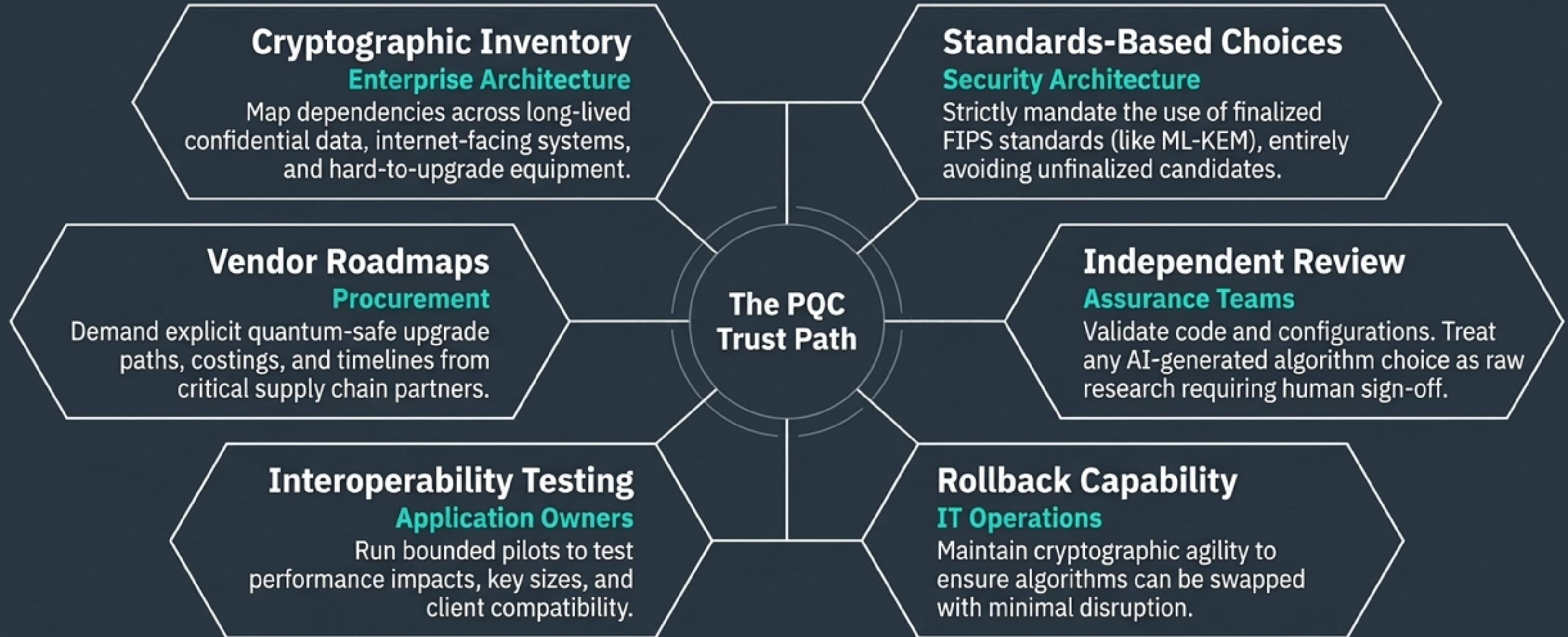
Encouraged target for full migration completion

CSA Quantum-Safe Kickstarter Grant

Supports eligible Singapore-incorporated non-government organisations, with priority for CII, subject to CSA assessment.

Source: CSA Advisory & Grant Documentation, 14 October 2026

Establishing the PQC Trust Path through practical, role-owned controls



A prioritized 90-day execution sprint for visibility and safe change

Phase 1: Visibility (Days 1–30)

- Executive sponsor assigns an accountable PQC migration owner.
- Architecture teams initiate inventory of cryptographic assets, prioritizing internet-facing systems and long-lived data.
- Procurement queries critical suppliers on finalized standard support.

Phase 2: Mapping & Pilot (Days 31–60)

- Security architects map dependencies to critical business services.
- Application owners select one bounded, low-risk application to pilot interoperability, certificate workflows, and rollback procedures.

Phase 3: Alignment (Days 61–90)

- CISO ranks workloads based on exposure and upgrade difficulty.
- Align specific timelines to CSA milestones (CII vs. non-CII exposed).
- Secure a costed sequence of changes based on vendor readiness.

Key Principle: The goal of this sprint is comprehensive visibility and a safe change mechanism—not organization-wide algorithm replacement by Day 90.

Bounding AI in security workflows and structuring independent assurance

The AI Boundary

What it does:

AI can accelerate test-case exploration, generate questions, and identify code inconsistencies.

What it requires:

Algorithm selection and security approval remain with qualified human reviewers utilizing finalized NIST standards.

Strategic Assurance with KIS

KIS supports organizations navigating these transitions through publicly listed services: AI Governance & Model Risk Assessments, Security Assurance & Testing, Source-Code Assessments, Control Reviews, and Security Roadmaps.

Disclaimer: KIS does not offer dedicated PQC implementation products. Organizations must follow CSA and NIST guidance for cryptographic choices and confirm vendor support.