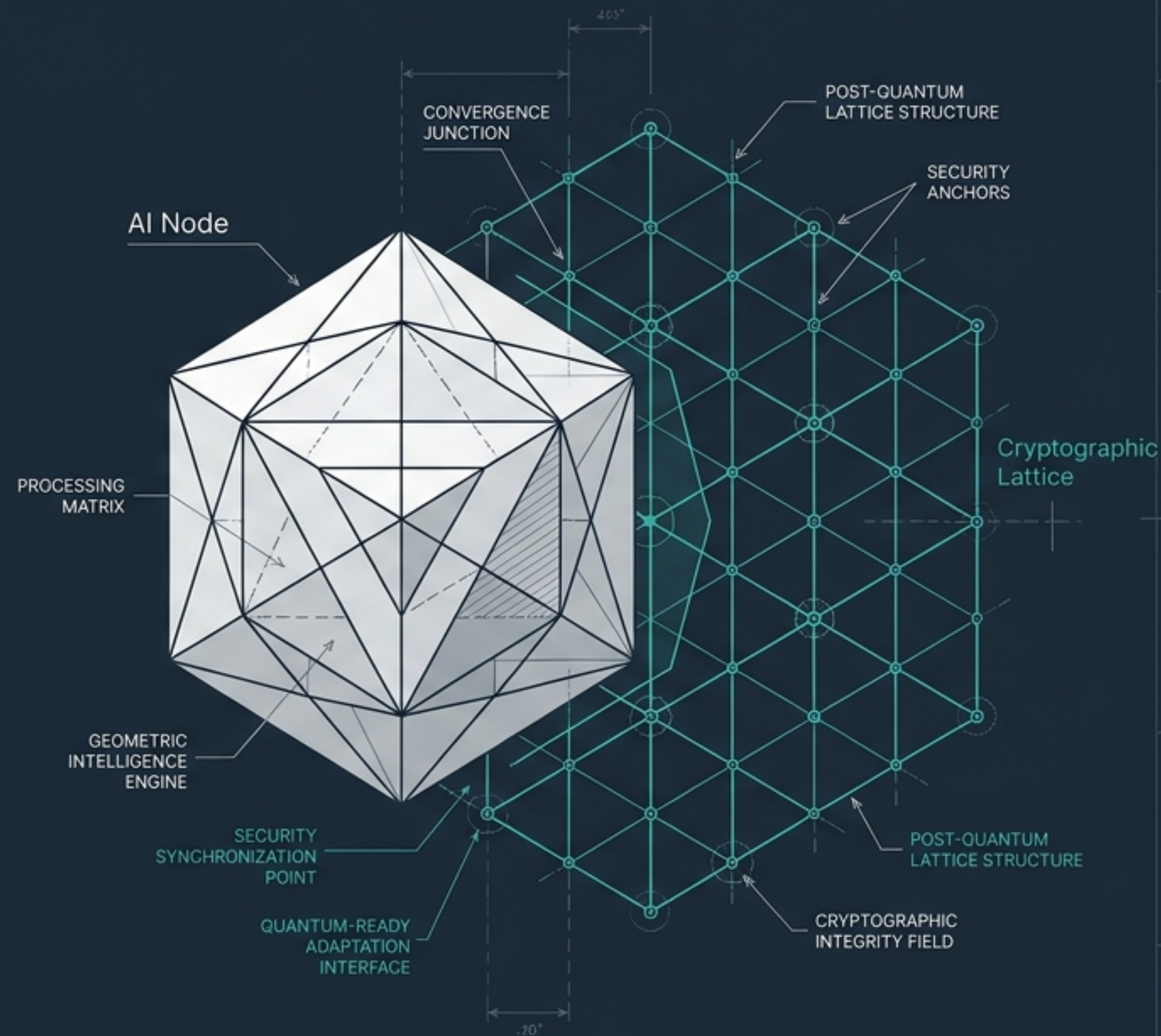


Navigating the AI-Quantum Security Crossover

Translating market signals, the HAWK research finding, and practical readiness for Singapore SMEs.



AI is accelerating cryptographic research, not breaking production encryption.

The biggest post-quantum security update isn't a quantum computer breaking today's encryption. It is AI assisting experts in exploring cryptographic structures—making the move to quantum-resistant standards a practical engineering programme, not a panic response.



Separating research candidates from finalized NIST standards.

On 28 July 2026, Anthropic's Claude Mythos Preview helped identify a weakness in HAWK. This finding proves open evaluation works—but it does not impact your production cryptographic stack.

HAWK (Withdrawn)

Status:

Candidate digital-signature scheme.



Event:

Failed in public review via AI-assisted research.

Impact:

Will not be standardized or deployed.

ML-KEM & ML-DSA (Active)

Status:

Finalized NIST post-quantum standards.



Event:

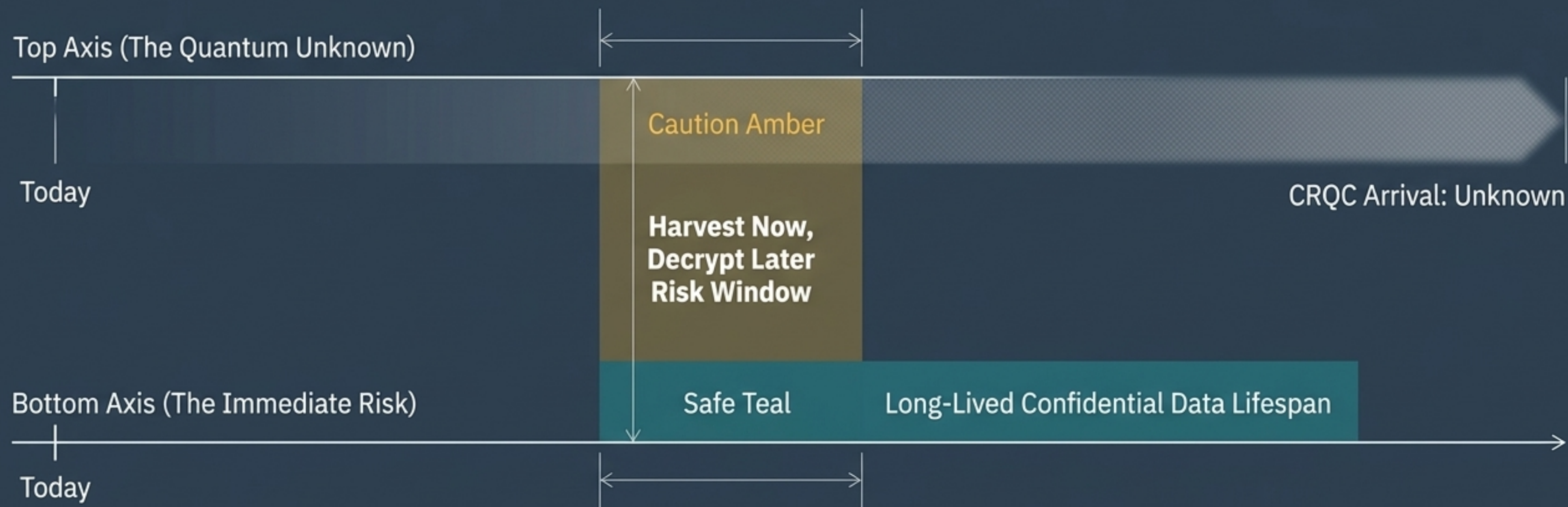
Unaffected by HAWK findings.

Impact:

Ready to implement.

The threat horizon is driven by data lifespan, not a specific Q-Day.

A Cryptographically Relevant Quantum Computer (CRQC) has no known arrival date. However, long-lived confidential information is at risk today due to **Harvest Now, Decrypt Later** tactics, where encrypted data is collected now and targeted for decryption in the unknown future.



Singapore quantum-safe RFI signals market interest.

CSA and GovTech invited market input on quantum-safe readiness. This is an information-gathering exercise, not a compliance deadline, certification, or regulatory mandate, though immediate attention is recommended.

Caution Amber

Market Readiness (CSA-GovTech RFI)

26 Aug – 27 Nov 2026



Seeking visibility into quantum-safe market readiness.

This is an industry information-gathering exercise, not a blanket compliance deadline or product certification. Ask suppliers what they support today.

The Singapore Signal



AI Security (CSA Agentic AI Addendum)

17 June 2026

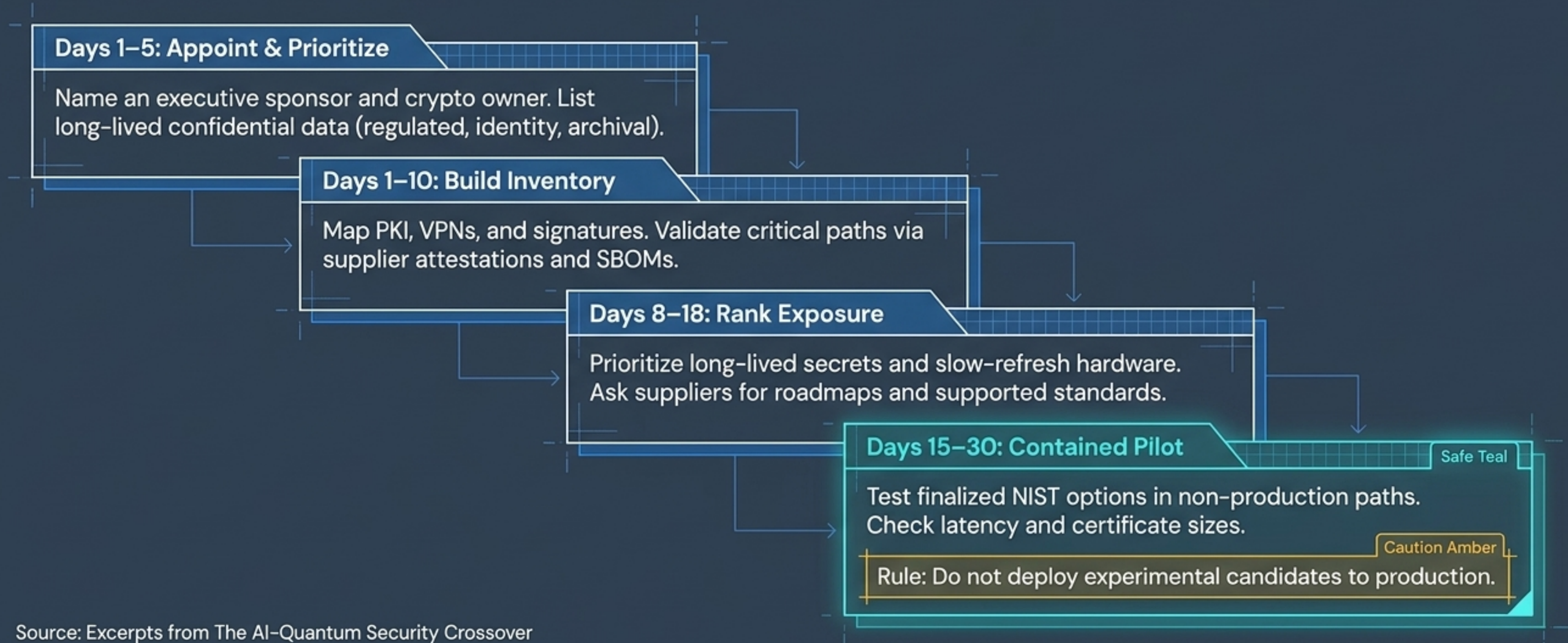
Provides guidance for system owners to map workflows, capabilities, tool access, and data access when assessing risk, without implying a new legal requirement.

Safe Teal

A practical 30-day blueprint for quantum readiness

Treat cryptographic resilience as a managed lifecycle.

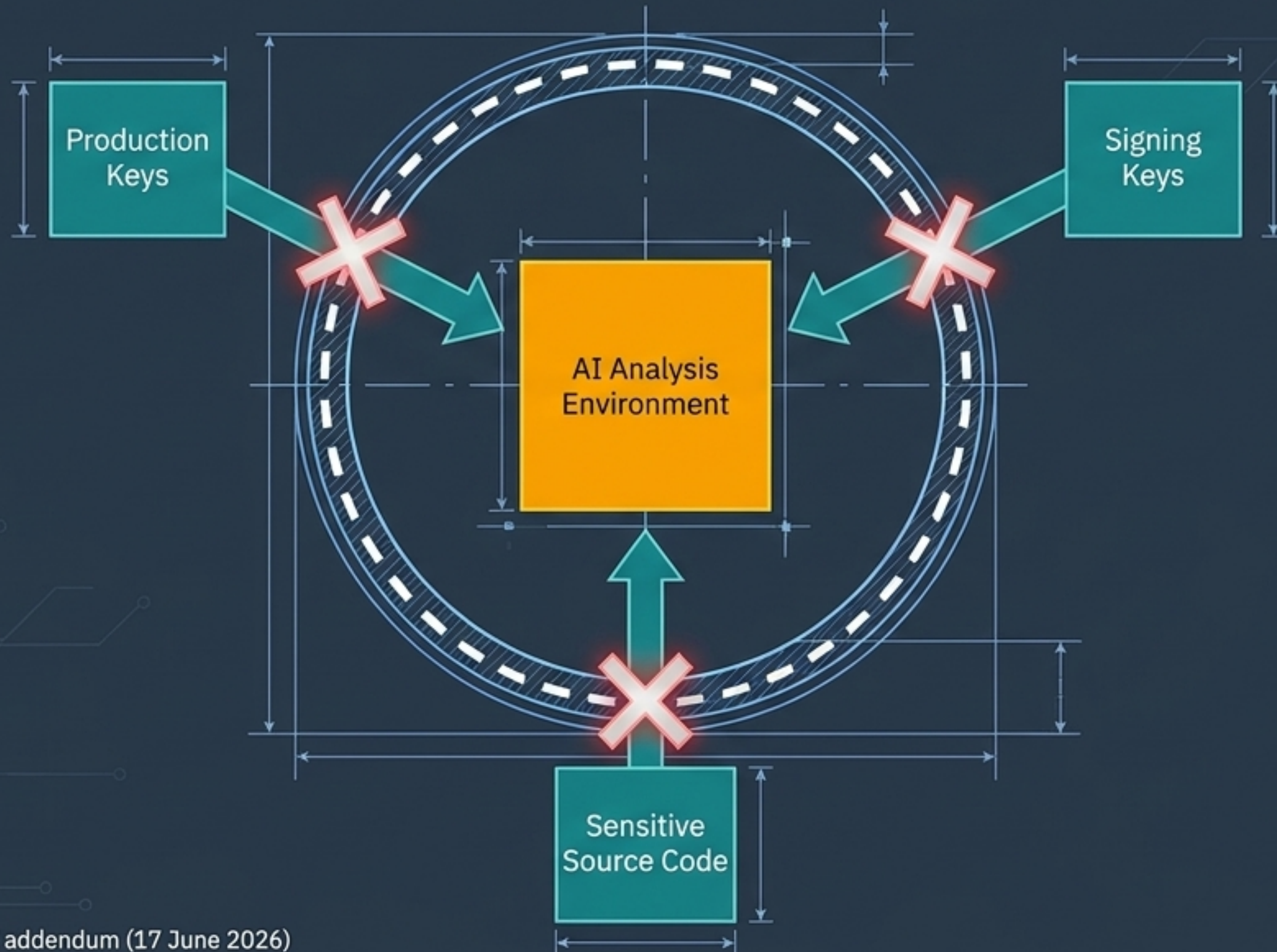
Focus on inventory and vendor roadmaps before attempting deployment.



Source: Excerpts from The AI-Quantum Security Crossover

Treat AI findings as hypotheses requiring bounded verification

When utilizing AI for code review or security research, provide it with a bounded environment. AI output is a hypothesis, not a cryptographic assurance claim, and requires a qualified reviewer to approve model-suggested changes.



Transitioning from assessment to managed lifecycle.

Suggested Monthly Management Metrics

- Percentage of critical services inventoried.
- High-priority systems lacking vendor migration paths.
- Expiring certificates or hardware constraints.
- Pilot results and unresolved supplier dependencies.
- Named risk acceptances.

Where KIS can help

Specialized Expertise

Security assurance, technology risk assessment, and specific AI Security offerings for engineering workflows.

Structured Approach

Assessments are aligned around your unique systems, standards, and supplier environment. There is no one-size-fits-all migration promise.