ETSI/IQC Quantum Safe Cryptography Conference 2026

The Post Quantum Cryptography Transition at Bank of Canada

Presented by:

BANK OF CANADA
BANQUE DU CANADA

17/06/2026

PQC Migration Journey

The Risk

Quantum computing threatens current public-key cryptography, and harvest-now, decrypt-later attacks make the exposure immediate, not future

The Mandate

CCCS, CFDIR, and G7 CEG guidance converge on a clear timeline: migration of high-priority systems by 2030, and all systems by 2035

The Plan

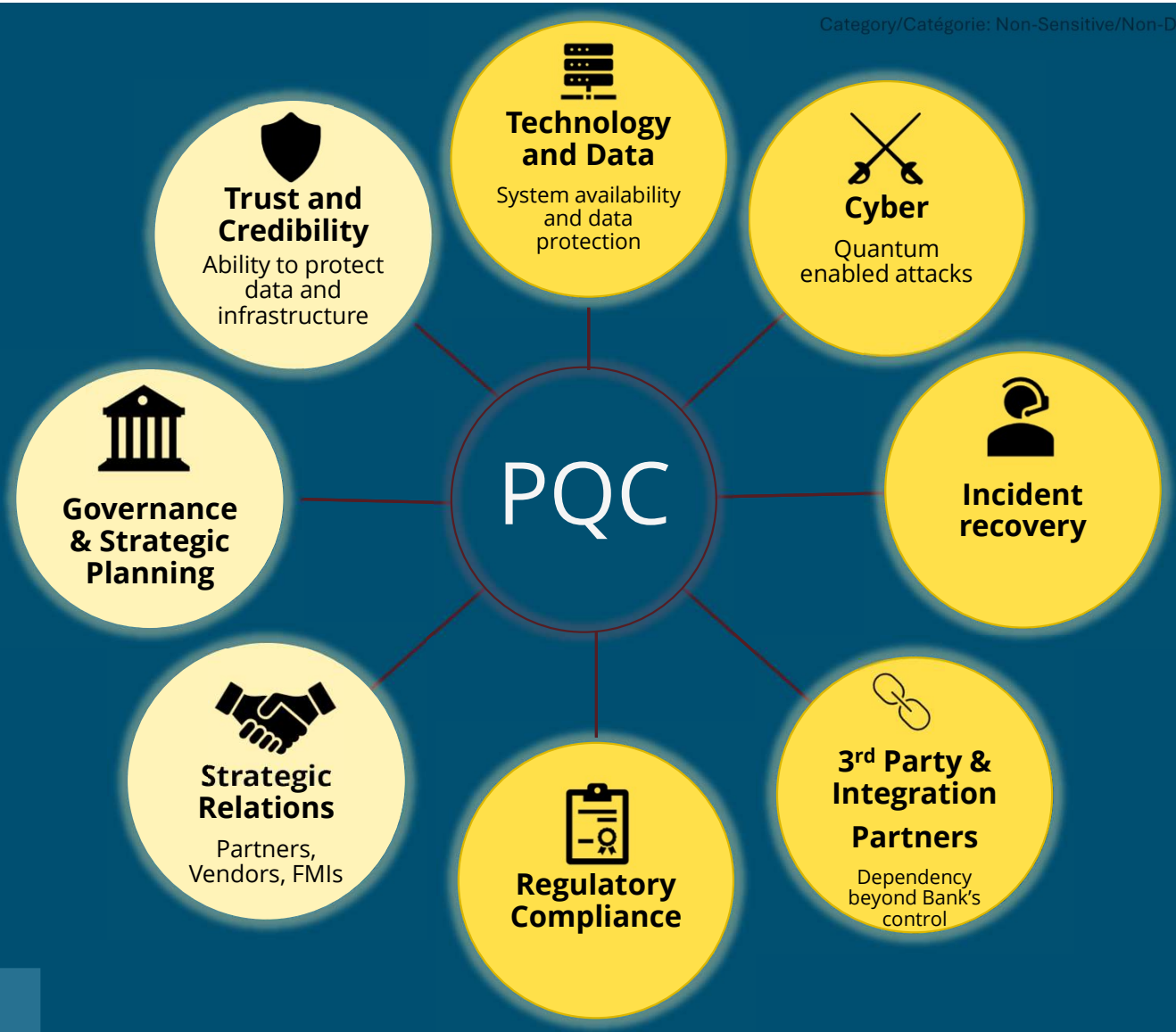
A phased migration: prepare governance and resourcing, inventory cryptography and assess risk, then transition with crypto-agility and hybrid approaches

The Imperative

Success depends on agreement, alignment, and coordination across the bank, third party vendors, system integration partners— starting now

Organization Risks

- Strategic Risks
- Operational Risks



Act Now:

Cryptographically relevant quantum computers are widely expected within 5–10 years, and adversaries can already harvest encrypted data today to decrypt later. The migration window is now.

The wide impact to confidentiality and integrity of the data encrypted using current algorithms

The amount of effort and time required for remediation will be substantial

(For example, the shift from SHA-1 to SHA-2 took over 12 years across industries.)

Significant amount of coordination with our partners and vendors will be required

Post Quantum Readiness Guidelines

Government of Canada

CCCS
Canadian Center of Cyber Security

April 2026: Departmental PQC migration plan
2031: Migration of high priority systems
2035: Migration of the rest of systems

Phase 1: Preparation

Define roles and responsibility, plan for financial impact, and create education strategy

Phase 2: Identification

Discover where and how cryptography is used . Conduct risk assessment to prioritize PQC migration, and engage 3rd party vendors for their PQC roadmap

Phase 3: Transition

Plan resources and maintain backwards compatibility. And explore other options to mitigate risk

Innovation, Science and Economic Development Canada

CFDIR
The Canadian Forum for Digital Infrastructure Resilience

Stage I: Initial Planning & Scoping (by 2024)

- Phase 0 - Preparation
- Phase 1 - Discovery
- Phase 2 - Quantum Risk Assessment

Stage II: Implementation (2025 – 2030)

- Phase 3 - Quantum Risk Mitigation
- Phase 4 - Migration to quantum safe cryptography
- Phase 5 - Validation

G7 2025 KANANASKIS

G7 CEG
G7 Cyber Expert Group

2030-2032: Migration of most critical systems to quantum resilience
2035: Overall migration to quantum resilience

Migration phases:

- Awareness and Preparation
- Discovery and Inventory
- Risk Assessment and Planning
- Migration Execution
- Migration testing
- Validation and monitoring

Migrate High Priority Systems by 2030

Discover & Assess

- Inventory cryptographic assets
- Classify data based on longevity
- Identify vulnerable or outdated cryptographic components
- Prioritize risk scenarios applicable to BoC. Know your critical path.
- Create a group of champions to initiate

Plan & Prepare

- Train security/IT teams and leaders on quantum risks
- Collaborate with financial sector partners for the alignment of roadmap and timelines
- Begin stakeholder engagement and vendor assessment
- Update encryption standard for PQC and assess IT solutions

Implement Resilience

- Adopt crypto-agility in application development
- Evaluate hybrid cryptographic protocols to support quantum safe crypto while preserving compatibility
- Run quantum-resilient pilot projects (test PQC algorithm)
- Strengthen incident response plan with quantum threat related scenarios

Stabilize & Monitor

- Roll out quantum safe crypto in production systems
- Monitor vendor and industry PQC adoption
- Collaborate with external partners to develop and support the compatibility with each other
- Continuously evaluate security risks and performance

Mitigate All Systems by 2035

Migrate Fully to PQC

- Replace all classical crypto with NIST-approved PQC
- Rebuild PKI: Root/intermediate CAs, certificates with PQC
- Deploy PQC-only for communication protocols (TLS, VPN, IPSEC)

Update Infrastructure

- Upgrade or replace incompatible systems and legacy apps
- Ensure infrastructure components are fully protected from quantum threat.
- Secure archived long-lived data with PQC encryption

Operation Readiness

- Establish crypto governance lifecycle process
- Maintain crypto agility as part of system and application design
- Maintain team knowledge on PQC and quantum threat models

Preparation for PQC Migration

Assess Risks and Priority

- Identify vulnerable or outdated cryptographic components
- Classify data based on longevity
- Prioritize risk scenarios applicable to BoC. Know your critical path.
- Raise awareness and educate PQC risks
- Create a group of champions to initiate

Locate vulnerable Crypto

- Inventory cryptographic assets
- Inventory embedded cryptography used by third party vendors
- Contact integration partners for their PQC readiness roadmap and timeline
- Feedback into risk assessment for prioritization

Build Crypto-agility

- Adopt crypto-agility in application development
- Evaluate hybrid cryptographic protocols (e.g. hybrid TLS) to support quantum safe crypto while preserving compatibility
- Run pilot to test PQC algorithm
- Strengthen incident response plan with quantum threat related scenarios

Manage Dependency

- Monitor vendor and industry PQC adoption
- Track timeline of PQC readiness of third-party vendors and service providers
- Collaborate with external partners to align the migration timeline and the compatibility with each other
- Continuously evaluate security risks and adjust PQC migration timeline and work plan

What if Q-Day arrives earlier?

Business Continuity

Integrate quantum cyber risk scenarios into business contingency planning.

Threat Monitoring

Track developments and adjust priorities as risk evolves

Dynamic Prioritization

Focus on the systems and data with the greatest exposure

Response Acceleration

Be ready to fast-track migration where risk increases

Create Technical Plan B

Consider technical options to secure the critical systems that cannot be remediated in time.

Key Considerations for Success

Agreement

Acknowledge PQC as a strategic risk and commit to the immediate start of the migration plan

Alignment

Champion a phased migration plan that is prioritized and resourced within the strategic roadmap

Coordination

Align with third-party vendors and external partners on joint PQC migration timelines and dependencies

Collaboration

Participate in industry forums and regulatory working groups to share best practices and stay current on PQC risk mitigation strategy