ExeQuantum

Post-Quantum Cryptography

Industry Use Cases

How organisations across manufacturing, insurance, banking, and government are preparing for the quantum transition

Powered by EQCore

ExeQuantum Pty Ltd

ISO 27001 Certified | NIST-Aligned | Formally Verified PQC

The Quantum Cryptography Challenge

Governments and standards bodies worldwide have set clear timelines for the transition to post-quantum cryptography. NIST finalised three PQC algorithm standards in August 2024 (FIPS 203, 204, 205). The NSA's CNSA 2.0 requires national security systems to begin migrating immediately, with full compliance by 2035. National cybersecurity agencies across Australia, Canada, the EU, and the UK have published parallel mandates, most targeting completion between 2030 and 2035.

The urgency is driven by a real and present threat. Nation-state adversaries are already conducting harvest-now-decrypt-later (HNDL) operations, intercepting encrypted data today with the intention of decrypting it once quantum computing reaches sufficient capability. For any organisation holding data with a confidentiality horizon beyond 2035, the risk window is already open.

The first step in any credible migration is knowing what you have. Most organisations have never conducted a comprehensive cryptographic inventory. Without visibility into which algorithms are in use, where they are deployed, and what data they protect, building a transition plan is guesswork.

EQCore is a Cryptographic Control Plane that takes organisations from discovery through to full post-quantum migration. It combines CipherScout (cryptographic discovery and compliance reporting), CipherWatch (continuous monitoring), and CipherForge (formally verified PQC implementation) in a single integrated platform.

The following use cases illustrate the specific pain points and migration challenges facing four key industries, and how EQCore addresses each.

Global PQC Transition Timeline

> **2024:** NIST PQC standards finalised (FIPS 203/204/205)
> **2025-2027:** Cryptographic inventories and transition planning
> **2028-2030:** Critical system migration underway across regulated industries
> **2030-2035:** Full transition mandated (CNSA 2.0, national mandates)

MANUFACTURING AND CRITICAL INFRASTRUCTURE

A Regional Manufacturer Discovers 1,200+ Quantum-Vulnerable Assets Across Its OT Estate

The Challenge

A mid-market manufacturer operating multiple production facilities engaged EQCore after a board-level risk review flagged post-quantum cryptography as an unaddressed exposure. The company's SCADA controllers, programmable logic controllers (PLCs), and remote terminal units (RTUs) were running firmware with hardcoded RSA keys that had not been rotated since installation. Several systems used 1024-bit RSA, already considered weak by classical standards.

The OT estate had a projected remaining service life of 15 to 25 years, meaning equipment installed today would still be operating well past the deadlines set by NIST and national cybersecurity agencies for phasing out traditional asymmetric cryptography. IT/OT convergence had connected previously isolated production networks to the corporate environment, creating exposure to harvest-now-decrypt-later (HNDL) collection that the security team had not previously considered.

The company had no centralised view of which cryptographic algorithms were in use across its operational environment. Certificate management on industrial gateways was manual, firmware signing keys used legacy algorithms, and device-level authentication relied on classical PKI with no quantum migration path.

How EQCore Helps

CipherScout was deployed across both IT and OT surfaces, scanning TLS certificates, SSH keys, APIs, and network protocols. The scan identified over 1,200 discrete cryptographic assets, including legacy SCADA protocol configurations, firmware signing chains, and device certificates that had never appeared in any previous security audit. The output was delivered as a standards-compliant Cryptographic Bill of Materials (CBOM) with risk-scored findings mapped to NIST PQC guidance and the company's applicable regulatory frameworks. The report flagged long-lived controller certificates, weak key lengths on industrial gateways, and unencrypted OT protocol segments as the highest-priority migration targets.

CipherWatch was configured for continuous monitoring of the cryptographic estate. Within the first 60 days, it caught two instances where vendor firmware updates introduced new quantum-vulnerable algorithm configurations that would have otherwise gone undetected.

For the company's air-gapped production environment, CipherForge was deployed on-premises with offline licensing, delivering formally verified post-quantum cryptographic algorithms (ML-KEM, ML-DSA, SLH-DSA) without requiring any external connectivity.

Outcome

✓ Cryptographic assets inventoried across IT and OT surfaces for the first time

✓ Risk-prioritised migration roadmap aligned to NIST standards and the company's compliance obligations
✓ Two previously invisible cryptographic regressions caught by continuous monitoring within 60 days
✓ On-premises, air-gapped deployment ensuring zero data leaves the production environment

INSURANCE

A National Insurer Quantifies HNDL Exposure Across 30 Years of Policyholder Data

The Challenge

A national insurance carrier approached EQCore after its CISO raised concerns about the quantum vulnerability of long-lived policyholder data. The company's life insurance policies, annuity contracts, and workers' compensation claims had confidentiality horizons of 30 to 50 years. Actuarial models containing proprietary pricing assumptions represented core competitive IP. Claims files held sensitive personal, medical, and financial information subject to privacy legislation and data breach notification requirements.

The CISO's concern was specific: any data encrypted today with RSA or ECC and intercepted by a sophisticated adversary could be stored cheaply and decrypted retroactively once quantum computing matures. For an insurer, the consequence would not be a single breach but the exposure of decades of policyholder records, medical histories, and financial information in a single event.

The company's financial regulator was already signalling expectations around cryptographic risk management, and the board risk committee wanted to understand the scope of the exposure before the next audit cycle. The insurer had no inventory of which cryptographic algorithms were in use across its policy administration systems, claims platforms, data warehouses, or third-party integrations.

How EQCore Helps

CipherScout discovered cryptographic usage across the insurer's full digital estate: TLS certificates on customer portals and API integrations, database encryption configurations protecting policyholder records, JWT authentication tokens in the claims management platform, and SSH keys across internal infrastructure. The scan produced a complete CBOM with findings mapped against the insurer's regulatory obligations and international standards (NIST, ISO 27001, ASD), producing board-ready documentation that quantified cryptographic risk in business terms. Critically, the report identified which policyholder data stores were protected by quantum-vulnerable encryption and cross-referenced each against its required confidentiality horizon, giving the risk committee a clear view of HNDL exposure by data class.

CipherWatch was deployed for ongoing monitoring, catching cryptographic regressions introduced through system updates, vendor integrations, and legacy platform migrations. This was particularly important because the insurer's policy administration platform was extended through multiple management transitions, each bringing its own cryptographic configurations.

The BYOD (Bring Your Own Database) architecture ensured that all scan data remained in the insurer's own provisioned database. ExeQuantum never held, retained, or had persistent access to any client data, eliminating third-party data residency concerns for the regulated entity.

Outcome

✓ First complete cryptographic inventory covering policy administration, claims, and data warehouse systems

✓ Board-ready risk reporting quantifying HNDL exposure by policyholder data class and confidentiality horizon

✓ Continuous monitoring catching cryptographic regressions introduced through acquisitions and vendor updates

✓ Zero third-party data residency exposure through BYOD architecture

FINANCIAL SERVICES AND BANKING

A Bank Maps Its Entire Cryptographic Estate and Discovers Systemic JWT Weaknesses

The Challenge

A bank with retail, commercial, and wealth management divisions engaged EQCore after failing to produce a credible cryptographic inventory for its regulator. Every card transaction, interbank transfer, API call, and customer authentication event depended on cryptographic protocols vulnerable to quantum attack. Payment HSMs, TLS termination points, SWIFT messaging, and mobile banking APIs all relied on RSA or ECC key exchange that would eventually need to be replaced.

The bank retained financial data with confidentiality requirements spanning 7 to 25 years: credit files, mortgage documentation, wealth management records, and anti-money laundering (AML) transaction histories. The CISO identified this long-lived data as the primary HNDL exposure, but had no way to quantify which systems were most at risk.

Regulatory pressure was converging from multiple directions. NACSA and regional equivalents were all imposing parallel requirements on cryptographic risk management. The bank operated across multiple jurisdictions and needed a single assessment that could serve multiple compliance obligations simultaneously.

The scale of the cryptographic estate was substantial: thousands of TLS certificates, hundreds of SSH keys, dozens of API gateway endpoints, internal JWT fleets for microservices authentication, and cloud KMS configurations across multiple providers. No previous audit had attempted to map it comprehensively.

How EQCore Helps

CipherScout performed discovery across all ten supported surfaces: TLS/certificates, APIs, HTTP, SSH, JWT fleets, cloud KMS (AWS and Azure), source code, email, databases, and identity systems. The JWT fleet analysis proved particularly revealing: rather than inspecting a single token at a point in time, CipherScout examined the full population of authentication tokens in use across the bank's microservices architecture, uncovering systemic algorithm weaknesses that no previous assessment had detected. The output was a Cryptographic Bill of Materials (CBOM) in CycloneDX 1.7 format, providing a machine-readable inventory that integrated directly with the bank's existing GRC and SIEM platforms. Risk scoring was mapped to NIST, ISO 27001, and NACSA, enabling the bank to satisfy multiple regulatory reporting requirements from a single assessment.

CipherWatch delivered continuous monitoring across the entire cryptographic estate, with alerting for certificate expiry, algorithm downgrades, and configuration drift. During the bank's multi-year migration programme, this ensured that new deployments and vendor updates did not reintroduce quantum-vulnerable algorithms after remediation.

CipherForge provided formally verified post-quantum cryptographic implementation using ML-KEM and ML-DSA. The formal verification, performed at the assembly level using Jasmin, closes the

compiler-introduced side-channel gap that affects most other implementations. For the bank's payment and settlement systems, this level of assurance was a requirement, not a preference.

Outcome

- ✓ Enterprise-wide cryptographic inventory across all ten discovery surfaces completed for the first time
- ✓ Multi-framework compliance reporting (NIST, ISO 27001, NACSA) from a single platform
- ✓ Formally verified PQC implementation with provable side-channel resistance for payment-grade systems

GOVERNMENT

A Government Agency Builds a Compliant PQC Transition Plan Across Classified and Unclassified Networks

The Challenge

A national government agency engaged EQCore to build the cryptographic transition plan required by its country's cybersecurity mandate. The agency faced a hard regulatory deadline to cease using traditional asymmetric cryptography, with interim milestones for planning and critical system migration. New procurement rules already required PQC considerations in all technology acquisitions, making this a live compliance obligation.

The agency's IT environment was characterised by layered complexity: legacy systems running decades-old cryptographic configurations, classified networks with strict air-gap requirements, multi-vendor supply chains where each link introduced its own cryptographic dependencies, and cross-agency data sharing arrangements that assumed the integrity of current digital signatures.

Critical infrastructure legislation extended cryptographic risk obligations across energy, telecommunications, water, and transport sectors. Defence industry participants in the agency's supply chain faced elevated exposure that many had not yet quantified.

For the classified environment, the migration challenge was compounded by the requirement for sovereign solutions. Cryptographic tools that route data through offshore infrastructure, or that depend on foreign-controlled key management, were ruled out during the procurement evaluation.

How EQCore Helps

CipherScout mapped the cryptographic posture across the agency's full digital estate, producing a CBOM that formed the foundation of the mandated transition plan. The scan covered external-facing TLS endpoints as well as internal infrastructure: SSH keys, API integrations between systems, database encryption configurations, and identity federation chains across multiple agencies. Findings were aligned to the relevant national cybersecurity framework and transition methodology, with the output structured to support both the near-term planning milestone and subsequent implementation milestones. The report was accepted as a compliance-ready artefact by the agency's audit body.

For the firewalled network segments, EQCore was deployed fully on-premises. All scan data remained within the secure environment at all times. The on-premises deployment used the same formally verified CipherForge engine as the cloud-hosted version, ensuring identical cryptographic assurance regardless of deployment model.

ExeQuantum's ISO 27001 certification, NIST alignment, and BYOD architecture were key factors in the procurement decision. The agency's data never left its own infrastructure, and ExeQuantum's independently verified security posture satisfied the supply chain assurance requirements that disqualified several international alternatives.

Outcome

- ✓ Regulatory-compliant PQC transition plan delivered within the mandated planning deadline
- ✓ On-premises deployment for firewalled assets
- ✓ CBOM and risk reporting structured to the national transition framework phases
- ✓ ISO 27001 certified platform with zero third-party data residency

Getting Started

Every organisation's cryptographic estate is different, but the starting point is the same: visibility. Without a comprehensive inventory of where quantum-vulnerable cryptography exists in the environment, no transition plan is credible and no compliance obligation can be met with confidence.

A Quantum Readiness Assessment (QRA) is a self-contained engagement that produces a Cryptographic Bill of Materials (CBOM), a risk heat map scored against relevant regulatory frameworks, a prioritised migration roadmap, and a board briefing pack. It is the fastest path from uncertainty to an actionable plan.

What you get from a Quantum Readiness Assessment:

- ✓ Cryptographic Bill of Materials (CBOM) in CycloneDX 1.7 format
- ✓ Risk heat map scored against NIST, ISO 27001, and applicable regulatory frameworks
- ✓ Prioritised migration roadmap aligned to 2026/2028/2030 milestones
- ✓ Board briefing pack translating technical findings into risk language

---

To discuss a Quantum Readiness Assessment for your organisation:

Audrey Nicoll, Chief Growth Officer
info@exequantum.com