ExeQuantum

WHITE PAPER

The STAC Doctrine

Sovereignty, Transparency, Agility and Compliance for the Quantum Era

Samuel Tseitkin, Chief Executive Officer
Dr. Raymond K. Zhao, Chief Technology Officer
Prem Kumar, Chief Information Security Officer

ExeQuantum Pty Ltd · exequantum.com · June 2026

Contents

1. Executive Summary

Quantum computing has moved from a theoretical concern to a scheduled disruption. In August 2024 the United States National Institute of Standards and Technology (NIST) finalised the first post-quantum cryptographic standards: FIPS 203 (ML-KEM) for key establishment, FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) for digital signatures. The question facing governments and regulated enterprises has shifted from whether to migrate to post-quantum cryptography (PQC), to how to migrate, on what timeline, and under whose control.

The cryptographic systems that secure global commerce, defence, healthcare and digital identity rest on mathematical assumptions that a cryptographically relevant quantum computer will invalidate. Adversaries do not need that computer today. Under the harvest-now, decrypt-later model, any data with a long confidentiality horizon is already exposed the moment it crosses a network: captured now, decrypted later.

ExeQuantum does not offer another proprietary product that entangles organisations in long-term vendor dependency. We deliver deeply integrated cryptographic frameworks that allow enterprises and sovereign entities to build self-sufficient, durable cryptographic ecosystems aligned to their national, regulatory and operational priorities. Our purpose is to embed cryptographic resilience into the fabric of an organisation's infrastructure, not to become that fabric.

The STAC doctrine, Sovereignty, Transparency, Agility and Compliance, provides the operating model for that transition. Rather than treating sovereignty and agility as opposing forces, or compliance and transparency as afterthoughts, STAC redefines cryptographic modernisation as a strategic discipline. It offers:

- **Sovereignty**, ensuring national and organisational control over keys, entropy sources, cryptographic inventory and data flows, independent of cloud or vendor dependencies.
- **Transparency**, removing black-box dependencies through full algorithmic disclosure, third-party auditability, formally verified implementation, and verifiable system behaviour.
- **Agility**, enabling rapid adoption of evolving NIST-approved post-quantum algorithms across both legacy and modern architectures.
- **Compliance**, providing pre-mapped alignment with leading global frameworks, simplifying audit cycles and regulatory reporting.

Across finance, defence, healthcare, critical infrastructure, blockchain and the Internet of Things, cryptographic inertia is no longer defensible. Governments are mandating action on dated timelines. Regulators are codifying requirements. Vendors are retrofitting solutions into fragile architectures. STAC is not a temporary fix. It is a doctrine for durable cryptographic sovereignty in the quantum era.

> The organisations that succeed in the quantum era will not be those that simply purchase new algorithms. They will be those that adopt new doctrines.

This white paper outlines the STAC framework, demonstrates its alignment with the regulatory regimes now in force across the major markets, and details how ExeQuantum operationalises STAC across cloud-native, on-premise, embedded and air-gapped environments, with real-world deployments already live.

2. The Geopolitical Urgency of Cryptographic Sovereignty

The global cybersecurity landscape is entering a phase of profound recalibration. For the first time in decades, the foundational assumptions that underpin digital trust are being actively invalidated, not by speculation, but by accelerating advances in quantum computing, state-sponsored cyber capability, and regulatory fragmentation. At the heart of this recalibration is a simple, existential question: who controls the cryptography that secures a nation's critical assets?

The collapse of traditional trust models

For years, organisations outsourced trust. Cloud providers controlled key infrastructure. Global public key infrastructure relied on transnational certificate authorities. Cryptographic algorithms assumed adversaries lacked the necessary computational breakthroughs. Sovereign states, regulators and CISOs now recognise that these assumptions are no longer sustainable. The arrival of quantum computing threatens the asymmetric cryptography that secures banking transactions, healthcare records, national identity systems, defence communications, industrial control systems and blockchain ecosystems. This is not only a technology problem. It is a sovereignty problem.

The rise of regulatory fragmentation

As the quantum threat moves from academic to operational reality, governments are establishing cryptographic transition regimes, with concrete and increasingly divergent timelines:

- **United States:** NIST standards finalised in 2024, with the NSA's CNSA 2.0 setting binding deadlines for national security systems.
- **European Union:** a coordinated implementation roadmap with milestones in 2026, 2030 and 2035, now being written into NIS2 and aligned to DORA and the Cyber Resilience Act.
- **Australia:** an ASD Information Security Manual that withdraws approval for traditional asymmetric cryptography beyond 2030, among the most aggressive national timelines.
- **Middle East:** national encryption policies and cryptographic standards in the UAE and Saudi Arabia mandating transition planning and cryptographic inventory.
- **Asia-Pacific:** national post-quantum migration roadmaps in Malaysia and India, and strengthened cryptographic obligations for critical infrastructure operators in Vietnam.

This fragmentation creates real difficulty for multinational enterprises, cross-border infrastructure and international data flows. Cryptographic compliance is no longer a matter of selecting an algorithm. It requires reconciling divergent jurisdictional requirements while maintaining operational agility.

Sovereignty is no longer optional

In this landscape, sovereignty is not isolationism. Sovereignty is control: over keys, over entropy sources, over cryptographic inventory, over algorithmic agility, and over auditability and vendor risk. Without sovereignty, compliance becomes fragile, agility becomes dangerous, and transparency becomes performative.

The doctrine gap

While regulators race to define mandates, what is missing for enterprises and governments is a doctrinal architecture: a unified operating model that allows them to adapt to evolving standards, maintain jurisdictional control, simplify compliance mappings, and future-proof their cryptographic infrastructure. The STAC framework exists to close this doctrine gap.

3. The STAC Framework Explained

The shift to post-quantum security is not only a change of algorithm. It is a change of architecture, ownership and operational mindset. At the heart of this transformation are four pillars: Sovereignty, Transparency, Agility and Compliance. Together they reframe cryptographic modernisation as a strategic discipline, helping organisations avoid vendor lock-in, retain jurisdictional control, and embed cryptographic resilience across cloud, on-premise, embedded and air-gapped environments.

1. Sovereignty

Control over your cryptographic destiny. Sovereignty begins with ownership of keys, entropy sources and algorithm selection. Where global platforms operate across opaque infrastructure and undefined jurisdictions, sovereignty means giving organisations the ability to choose, audit and control every cryptographic primitive embedded in their operations.

How ExeQuantum delivers it:

- On-premise and air-gapped deployment models, with code handover where required.
- Bring-Your-Own-Key (BYOK) and sovereign key management.
- A Bring-Your-Own-Database (BYOD) architecture under which all cryptographic discovery findings, inventory and credentials remain inside the customer's own database rather than ExeQuantum's, so sensitive data never leaves the customer's jurisdiction or control.
- Domestic entropy sources, including optional quantum random number generation.
- Formal partnerships with approved local technology vendors to ensure jurisdictional alignment.
- Full infrastructure visibility and zero default trust in third parties.

2. Transparency

If you cannot see it, you cannot trust it. Black-box cryptography and hidden implementations no longer meet the bar for trust. Transparency means every cryptographic operation, from key generation to signature validation, is observable, auditable and explainable.

How ExeQuantum delivers it:

- Cryptographic Bills of Materials (CBOMs) in CycloneDX format, giving a verifiable inventory of quantum-safe and legacy algorithms.
- Formally verified cryptographic implementation. In our CipherForge engine, every routine that handles secret values is written in Jasmin, a language that enforces constant-time execution and enables verification at the assembly level by construction. This closes the compiler gap that can silently introduce timing side-channels into otherwise sound implementations, and it does so without the performance cost usually associated with formal verification: in our benchmarking, the verified ML-DSA signing path runs faster than the standard C reference implementation.
- Open algorithmic standards and verifiable source behaviour.
- Independent audit support and third-party review readiness.
- API observability, operational logging and detailed policy-to-practice mappings for auditors.

3. Agility

Post-quantum cryptography does not mean rigidity. Agility means being able to adapt, not only to cryptographic threats but to changing standards, policies and operational constraints. STAC supports algorithmic flexibility and modular architecture that lets organisations pivot without breaking systems.

How ExeQuantum delivers it:

- Support for NIST-standardised and forthcoming algorithms, including ML-KEM (FIPS 203), ML-DSA (FIPS 204) and SLH-DSA (FIPS 205), with FN-DSA (FALCON) expected as FIPS 206. HQC, a code-based key encapsulation mechanism selected by NIST in 2025 with a final standard expected around 2027, is supported to provide algorithmic diversity against category-specific attacks.
- Crypto-agility without a trade-off in assurance: our formally verified implementation lets algorithms be added or replaced while preserving correctness and constant-time guarantees.
- Hybrid post-quantum and traditional layering as a transition aid. Hybrid suitability is jurisdiction-dependent: several regimes recommend hybrid schemes during migration, while others, including Australia's ASD, direct organisations toward standalone post-quantum algorithms. Our architecture supports both postures.
- Modular API infrastructure that integrates across TLS, VPNs, PKI, identity, storage, IoT and cloud, with upgrade pathways designed for controlled change windows.

4. Compliance

Security is only useful when it is provable. In regulated industries, cryptographic strength is not enough. It must be demonstrable. Compliance within STAC means building cryptographic systems that map directly to regulatory frameworks, reducing the burden on security teams and streamlining audits.

How ExeQuantum delivers it:

- Alignment with ISO 27001, NIST PQC standards, ASD ISM, EU NIS2 and DORA, APRA CPS230, GDPR, Saudi NCA standards, ENISA guidance, HIPAA and PCI DSS.
- Pre-packaged audit reports, checklists and control mappings.
- Collaboration with local regulators, regional partners and accredited auditors for jurisdiction-specific certification.
- Vertical-specific audit frameworks for banking, healthcare, defence, blockchain and critical infrastructure.
- Integration into governance and risk management platforms.

Together, these four pillars form a cryptographic doctrine that is globally interoperable and sovereign in execution.

4. Global Alignment: STAC Across National Initiatives

Post-quantum migration is a global imperative, but every jurisdiction approaches cryptographic sovereignty through its own policy lens. STAC is designed to be globally interoperable and locally adaptable, letting governments, enterprises and critical sectors meet both technical and jurisdictional requirements. The regimes below are those now in force or in active rollout.

North America

United States. NIST finalised FIPS 203, 204 and 205 in August 2024. The NSA's Commercial National Security Algorithm Suite (CNSA 2.0) requires new national security system acquisitions to be compliant from 1 January 2027, with full migration across national security systems by 2035. NIST's transition guidance (IR 8547) deprecates RSA-2048 and ECC P-256 by 2030 and removes quantum-vulnerable algorithms from federal standards by 2035, while FIPS 140-2 cryptographic modules move to historical status in September 2026. Civilian procurement has shifted toward agency discretion, making market-led PQC readiness a competitive requirement rather than only a mandate.

STAC alignment: sovereignty through zero-trust compatibility without long-term lock-in; transparency through FIPS-aligned, source-auditable implementations and verifiable CBOMs; compliance pre-mapped to FISMA, FedRAMP and CMMC.

Canada. The Canadian Centre for Cyber Security published its migration roadmap in June 2025. Government departments are to develop initial migration plans from April 2026 and report progress annually, complete migration of high-priority systems by the end of 2031, and migrate remaining non-classified systems by 2035.

STAC alignment: phased migration anchored to cryptographic inventory and dependency mapping, with sovereign control retained across federal and provincial systems.

Europe

European Union. Following the European Commission's April 2024 recommendation, the NIS Cooperation Group published a coordinated implementation roadmap in June 2025. Member states are to define national strategies and complete first steps by the end of 2026, migrate critical infrastructure by the end of 2030, and complete transition as far as feasible by 2035. A February 2026 proposal writes post-quantum migration explicitly into NIS2, reinforced by DORA for the financial sector and the Cyber Resilience Act for products entering the single market. European guidance favours standardised, tested hybrid schemes during the transition where suitable.

STAC alignment: cross-border interoperability with sovereign execution; cryptographic asset management and CBOM inventory map directly to the roadmap's first steps; compliance aligned to NIS2, DORA and the Cyber Resilience Act.

Spain. Spain follows the EU coordinated roadmap and has supplemented it with a national quantum technologies strategy driven by the Centro Criptológico Nacional and the Ministry for Digital Transformation, extending the migration agenda into the enterprise and telecommunications sectors.

STAC alignment: sovereign deployment for national and enterprise infrastructure, with audit-ready evidence for national certification authorities.

United Kingdom

United Kingdom. The National Cyber Security Centre frames PQC as a long-term national resilience programme delivered in three phases: cryptographic discovery, inventory and dependency mapping by 2028; pilots and highest-priority migration from 2028 to 2031; and wider migration from 2031 to 2035. The

emphasis is on a centrally managed transition that avoids a rushed, fragmented migration.

STAC alignment: discovery and inventory tooling for the 2028 milestone; agility for phased, low-disruption migration; transparency for centrally governed assurance.

Middle East

United Arab Emirates. In late 2025 the UAE approved a National Encryption Policy, announced by the Cyber Security Council and overseen by the National Cryptography Centre. Government entities are required to submit officially approved transition plans from traditional encryption (RSA, ECC) to post-quantum standards, and to use automated tools to maintain a real-time cryptographic inventory, as part of a coordinated national post-quantum migration programme.

STAC alignment: automated cryptographic discovery, real-time inventory and continuous monitoring map directly to the mandated controls; sovereign deployment within UAE jurisdiction; transparency through CBOM delivery for regulated sectors.

Saudi Arabia. The National Cybersecurity Authority (NCA) has issued National Cryptographic Standards specifying minimum cryptographic requirements for national data, systems and networks for civilian and commercial use, complementing the sovereign digital infrastructure goals of Vision 2030.

STAC alignment: on-premise and air-gapped deployment under national control; CBOM and audit frameworks aligned to NCA standards; cryptographic diversity for evolving national requirements.

Asia-Pacific

Australia. The ASD Information Security Manual withdraws approval for traditional asymmetric cryptography, including RSA, ECDH and ECDSA, beyond 2030, and requires new cryptographic equipment and software to support ML-DSA-87, ML-KEM-1024, SHA-384, SHA-512 and AES-256 by that date. Organisations are expected to hold a refined transition plan by the end of 2026, begin transition of critical systems by the end of 2028, and complete it by the end of 2030. This is one of the most aggressive national timelines in force, and ASD directs organisations toward standalone post-quantum algorithms rather than hybrid schemes.

STAC alignment: as an Australian provider, sovereign alignment with ASD requirements; our formally verified ML-DSA-87 and ML-KEM-1024 implementation supports ASD's standalone-algorithm posture directly; transparency reinforced by peer-reviewed research with Australian universities.

India. The Department of Science and Technology, under the National Quantum Mission, published its national roadmap, Implementation of Quantum Safe Ecosystem in India, in February 2026. It sets a tiered, time-bound approach: full post-quantum adoption for Critical Information Infrastructure by 2029 and for broader enterprise by 2033, with cryptographic inventory and Cryptographic Bill of Materials requirements embedded into procurement and supported by a national post-quantum testing and certification programme.

STAC alignment: domestic key management integrated with sovereign cloud and public-sector infrastructure; CBOM reporting aligned to CERT-In and national audit processes.

Malaysia. The Ministry of Digital and the National Cyber Security Agency (NACSA) launched the National Post-Quantum Cryptography Migration Plan 2025 to 2030, with a sandbox proof-of-concept programme, in November 2025. Eleven National Critical Information Infrastructure sectors fall under mandatory compliance through the Cyber Security Act 2024, with financial-sector alignment driven by Bank Negara Malaysia.

STAC alignment: phased NCII transition with hybrid deployment support; sovereign white-label delivery through approved local partners; compliance aligned to NACSA and Bank Negara requirements.

Vietnam. The new Law on Cybersecurity (No. 116/2025/QH15), effective 1 July 2026, consolidates the national cybersecurity framework and strengthens data-security and cryptographic obligations for

information systems critical to national security. State Bank of Vietnam circulars are tightening authentication and reporting across the banking sector, where harvest-now-decrypt-later exposure and correspondent-banking requirements are making post-quantum readiness a forward priority.

STAC alignment: cryptographic discovery and inventory for banking and critical infrastructure; sovereign deployment within national jurisdiction; agility for phased migration of digital signature and key-exchange infrastructure.

Singapore and ASEAN. Singapore's Cyber Security Agency and the Monetary Authority of Singapore increasingly treat quantum risk as a supervisory concern, with regional coordination through the ASEAN-Singapore Cybersecurity Centre of Excellence. Singapore functions as a regional hub for cryptographic governance across Southeast Asia.

STAC alignment: regional interoperability and cross-border consistency, with compliance evidence portable across ASEAN jurisdictions.

The financial sector

Across jurisdictions, financial services is the sector where discovery, agility and compliance converge most sharply. The G7 Cyber Expert Group's roadmap, co-chaired by the United States Treasury and the Bank of England, frames PQC as a systemic resilience issue and targets migration of key financial systems by 2032 and full transition by 2035. The Basel Committee, the European Central Bank, SWIFT and the Hong Kong Monetary Authority, through its Quantum Preparedness Index, are establishing parallel expectations, while PCI DSS 4.0 already requires a maintained inventory of cryptographic algorithms.

> Across jurisdictions, STAC operates not as a one-size-fits-all product, but as a doctrine that lets sovereign entities execute cryptographic independence without sacrificing interoperability.

5. The ExeQuantum Architecture

The STAC doctrine is not theory. It is operationalised through ExeQuantum's architecture, which functions as a cryptographic control plane: it sits above existing security tooling such as SIEM, GRC, CSPM and identity systems, and governs cryptography as a regulated risk system rather than competing at the feature level. ExeQuantum operates as an architecture partner, embedding cryptographic resilience into the customer's own control plane rather than becoming the customer's infrastructure.

The platform

Component	Function
CipherScout	Cryptographic discovery, inventory and CBOM generation across the cryptographic estate, producing CycloneDX output for verifiable, population-level visibility.
CipherForge	API-native post-quantum implementation engine for ML-KEM, ML-DSA and related algorithms, built on a formally verified Jasmin and C hybrid architecture, with stateless, BYOK-first deployment across hybrid, cloud, on-premise and air-gapped environments.
CipherWatch	Continuous monitoring, compliance reporting, audit trails and algorithm lifecycle management.
EQCore	Orchestration connecting discovery, remediation and governance into a single control plane.
SiFA	Quantum-safe authentication layer, developed jointly with Krown Technologies. Patent declared.

Core delivery models

- **PQCaaS platform:** API-driven infrastructure for organisations preferring scalable, SaaS-based cryptographic modernisation, with STAC-aligned insertion into existing stacks.
- **On-premise and air-gapped appliances:** full-stack deployments for government, defence and critical sectors requiring complete sovereignty and offline key control.
- **Embedded and hardware integration:** post-quantum cryptography embedded into IoT, industrial controllers and edge devices, with optional QRNG-integrated hardware for verifiable entropy.

Core architectural features

- Formally verified implementation. Every subroutine handling secret values is written in Jasmin, which enforces constant-time execution and formal verification at the assembly level by construction, while public-only operations remain in C where compiler optimisation is safe. This closes the last-mile compiler gap that can introduce timing side-channels into otherwise well-regarded implementations, and the verified ML-DSA signing path runs faster than the standard C reference rather than paying the performance cost usually associated with formal verification.
- Algorithm agility across ML-KEM, ML-DSA, SLH-DSA, the forthcoming FN-DSA, and code-based HQC for algorithmic diversity.
- Bring-Your-Own-Database architecture, keeping all discovery findings, inventory and credentials within the customer's own database.
- Sovereign Bring-Your-Own-Key architecture and domestic entropy integration.
- Transparent CBOM reporting and audit frameworks in CycloneDX format.
- An API-first model for TLS, VPN, storage, identity, blockchain and PKI integration.
- Partnerships with approved local vendors to meet jurisdictional sovereignty requirements.

ExeQuantum does not seek to replace or centralise a nation's digital infrastructure. We act as an integration partner and operational enabler, delivering post-quantum capability while preserving sovereign control, jurisdictional ownership and long-term transparency. Organisations retain key ownership, regulatory alignment and cryptographic oversight, while ExeQuantum operates, maintains and updates the cryptographic core as standards evolve. The result is both sovereign assurance and operational simplicity, without building in-house cryptographic teams or accepting vendor dependency.

> ExeQuantum is ISO 27001 certified and aligned with NIST PQC standards. Its post-quantum capability is recognised in the Austrade Australian Quantum Technology Industry Capability Report and the Wavestone 2026 Post-Quantum Migration Solution Radar, and its cryptographic engineering is grounded in peer-reviewed research with Australian universities including RMIT, Swinburne and Deakin.

6. The Cost of Inaction

The post-quantum transition is not a future compliance exercise. It is a geopolitical, economic and national security reality unfolding now. As quantum capability advances, organisations that delay cryptographic modernisation will find themselves exposed not only to technical risk, but to non-compliance with mandates that already carry dated deadlines across the United States, the European Union, the United Kingdom, Australia, the Gulf and Asia-Pacific.

The harvest-now, decrypt-later threat means the exposure window is not the distance to the day a quantum computer can break current encryption. It is the confidentiality lifetime of the data minus that distance. For records that must remain protected for a decade or more, the decision to protect them must be made now, because data captured today cannot be un-stolen.

Migration is also slow. Cryptography is embedded in protocols, certificates, key exchanges, signatures, firmware and hardware across every system. Identifying, assessing and upgrading each instance is a multi-year undertaking, which is precisely why every major roadmap places cryptographic inventory and crypto-agility at its first milestone. The organisations that begin discovery now will meet their deadlines. Those that wait will face rushed remediation at two to three times the cost.

STAC is not a product. It is a doctrine: a durable operating model that lets governments, enterprises and critical sectors embed cryptographic resilience directly into their infrastructure while preserving operational agility and jurisdictional control. ExeQuantum delivers that doctrine with real-world execution, integrating into partner systems, empowering sovereign control, maintaining full auditability, and providing operational expertise across cloud-native, on-premise, air-gapped and embedded environments.

> The organisations that thrive in the quantum era will not be those that simply acquire algorithms, but those that adopt doctrines built for sovereignty, transparency, agility and compliance.

7. Engaging with ExeQuantum

ExeQuantum is actively engaging with:

- governments defining national cryptographic standards and post-quantum migration programmes;
- enterprises navigating multi-jurisdictional regulatory landscapes;
- critical infrastructure operators preparing for quantum resilience.

We invite agencies, regulators, CISOs and technology leaders to engage directly with ExeQuantum to explore how the STAC framework can be tailored to your jurisdiction, sector and infrastructure priorities. A structured cryptographic discovery is the first step: it establishes the inventory on which every national roadmap, and every credible migration plan, depends.

Contact
info@exequantum.com · exequantum.com · linkedin.com/company/exequantum
ExeQuantum Pty Ltd · ABN 86 680 683 738