Quantum Trust & PQC Assurance Services

A governance, validation, and operational assurance capability for organisations deploying quantum-safe cryptography and vendors building quantum-safe products.

The Core Problem

The market is saturated with PQC claims. Products ship with post-quantum labels. Programmes declare readiness. Discovery tools assert comprehensive coverage. Endpoint solutions promise quantum-safe protection. The question is whether any of it is real.

For enterprises deploying PQC: how do you prove your cryptography is genuinely quantum-safe, operationally governable, and enforceable across real environments? For vendors selling PQC products: how do you prove your product does what it claims before a buyer, a regulator, or an auditor tests it for you?

SITG-Consulting provides independent, evidence-led validation for both. We test what is claimed. We issue a verdict. We produce the artefacts that boards, regulators, auditors, and procurement teams require.

Who This Service Is For

Enterprises Deploying PQC

Organisations migrating to quantum-safe cryptography need independent assurance that implementations are correct, that vendor claims are substantiated, and that governance structures can sustain what has been deployed. SITG-Consulting validates the implementation, the architecture, and the control environment.

Vendors Selling PQC Products

Vendors building and commercialising PQC products: discovery platforms, endpoint agents, key management systems, crypto-agility middleware, QRNG modules, quantum-safe SDKs, or any product making post-quantum claims. Independent validation from SITG-Consulting provides market-ready evidence that the product is genuine, compliant, and operationally effective. A vendor whose product carries an independent validation verdict has a defensible market position. A vendor whose product has never been independently tested is making unsubstantiated claims.

What We Validate

SITG-Consulting validates any product, platform, protocol, or implementation that claims to be quantum-safe. The scope covers enterprise implementations and commercial PQC products alike.

Enterprise Implementations

VPN Solutions Protocol negotiation, tunnel integrity, hybrid handshake, fallback behaviour, real PQC in live traffic.	**TLS/SSL Implementations** Certificate chains, PQC cipher suites, negotiation correctness, downgrade resistance.
Key Management Systems PQC key generation, storage, rotation, lifecycle governance, entropy sourcing.	**HSM & QRNG Integrations** Hardware module compliance, entropy quality, side-channel protections, firmware provenance.
Digital Signature Platforms ML-DSA/SLH-DSA correctness, certificate issuance, signing ceremony integrity.	**PKI & Certificate Authorities** PQC certificate issuance, chain validation, hybrid certificate support, revocation.
Messaging & Email Encryption End-to-end PQC, key exchange protocols, backward compatibility, metadata exposure.	**Identity & Access Platforms** Authentication protocols, token signing, federation, PQC credential lifecycle.
Cloud Platform Services PQC integration across AWS, Azure, GCP: storage encryption, transit, key vaults.	**IoT & OT Firmware** Constrained-device PQC, firmware signing, update mechanisms, embedded crypto.
API Gateways & Microservices Service-to-service encryption, mTLS with PQC, certificate management at scale.	**Database Encryption** Transparent data encryption, column-level PQC, key rotation, performance impact.

brian.couzens@sitg-consulting.com

Crypto Wallets & DLT
Algorithm implementation, key derivation, transaction signing, wallet architecture.

Vendor Libraries & SDKs
Algorithm correctness, API design, dependency chains, version governance.

Commercial PQC Products

Cryptographic Discovery Tools
Scan accuracy, protocol coverage, false-positive rates, estate completeness, reporting integrity.

Crypto-Agility Platforms
Algorithm rotation capability, certificate management, interoperability, migration orchestration.

PQC Endpoint Agents
Algorithm implementation, key handling, system integration, performance under load.

Quantum Key Distribution (QKD)
Protocol correctness, key rate claims, integration architecture, operational viability.

QRNG Modules & Entropy Sources
Entropy quality, NIST SP 800-90B compliance, output rate claims, integration pathways.

PQC-as-a-Service Platforms
API correctness, algorithm implementation, tenant isolation, key lifecycle governance.

Quantum-Safe Network Appliances
Protocol handling, throughput claims, hybrid support, failover behaviour.

CBOM & Inventory Tools
Asset detection accuracy, dependency mapping, reporting completeness, audit-readiness.

brian.couzens@sitg-consulting.com

Service Modules

Each module is self-contained and can be engaged independently or as a sequenced programme. Progression is gated: each module produces validated, auditable outputs before the next is initiated.

1. PQC Discovery and Cryptographic Exposure Assessment

Forensic identification of where cryptography exists, what algorithms are in use, hidden dependencies, vulnerable protocols, harvest-now-decrypt-later exposure, and third-party cryptographic risk.

Deliverables: Cryptographic Exposure Map, Quantum Risk Register, Priority Migration Matrix.

2. Crypto-Agility and Architecture Readiness Assessment

Assessment of the organisation's capacity to rotate algorithms, update certificates, support hybrid cryptography, maintain interoperability, and adapt protocols without operational disruption. This is where architectural fragility is exposed.

Deliverables: Crypto-Agility Maturity Score, Architecture Weakness Assessment, Future-State Quantum-Safe Blueprint.

3. PQC Protocol and Implementation Validation

The high-value technical assurance layer. Validation of real PQC usage in live traffic, protocol negotiation, certificate chains, implementation correctness, side-channel protections, entropy quality, fallback behaviour, and vendor claims.

Core verdict: independent verification that the implementation is real, secure, and operationally effective. Genuine PQC, hybrid, wrapper, or not what the vendor claims.

Deliverables: PQC Assurance Report, Protocol Validation Evidence, Executive and Regulator Attestation Pack.

4. PQC Product Validation (Vendor Programme)

Independent validation of commercial PQC products prior to market release or procurement. SITG-Consulting tests the product against its own claims, against published standards, and against operational reality. The output is a defensible validation verdict that vendors can reference in sales collateral, procurement responses, and regulatory submissions.

Deliverables: Product Validation Report, Standards Compliance Evidence, Market-Ready Attestation Pack.

5. Quantum Governance and Operating Model Design

Organisations that have deployed PQC without establishing crypto ownership, governance structures, lifecycle control, or resilience telemetry have not established control. Deployment without governance is exposure with a different label.

Deliverables: Quantum Trust Operating Model, Cryptographic Governance Framework, Board-Level Risk and Oversight Model.

6. PQC Supply-Chain Assurance

Assessment of vendors and third parties for genuine PQC readiness, crypto-agility, dependency exposure, update mechanisms, and cryptographic transparency.

Deliverables: Third-Party Quantum Assurance Ratings, Supplier Risk Heatmaps, Contractual PQC Requirements.

7. Continuous Quantum Assurance

Ongoing protocol validation, telemetry, inventory drift detection, crypto exposure monitoring, vendor posture tracking, and compliance evidence production. Managed Quantum Trust Assurance: operational trust validation for the quantum era.

Deliverables: Quarterly Assurance Reports, Drift Alerts, Compliance Evidence Packs, Board Reporting Artefacts.

brian.couzens@sitg-consulting.com

Anchored in Governance

Technical validation without governance validation is incomplete. For any product or implementation, SITG-Consulting also examines:

- Documentation completeness: design specifications, architecture decision records, threat models.
- Version control and change management: provenance of cryptographic code, dependency tracking, release governance.
- SDLC maturity: security review gates, cryptographic code review processes, CI/CD pipeline controls.
- Configuration management: deployment procedures, environment controls, key material handling.
- Incident response preparedness: quantum-risk scenarios in IR playbooks, escalation paths, communication protocols.
- Compliance alignment: mapping to NIST, CNSA 2.0, ENISA, ETSI, and sector-specific mandates.
- Audit trail integrity: evidence chains that survive regulatory inquiry and external audit.

If the governance structure cannot sustain the implementation, the implementation is not validated. Control is the standard, not correctness alone.

Validation Verdicts

Every engagement concludes with a clear, defensible verdict:

Validated	Genuine PQC implementation. Algorithms correctly deployed. Governance sufficient. Fit for purpose.
Conditional	Partial PQC, hybrid implementation, or governance gaps identified. Remediation path defined. Re-validation required.
Not Validated	Claims not substantiated. Wrapper, mislabelled, or structurally non-compliant. Not quantum-safe as stated.

Verdicts are evidenced, traceable to test results, and designed to enter board records, regulatory submissions, procurement documentation, and vendor sales collateral.

Independence

SITG-Consulting holds no vendor partnerships, no equity stakes in clients, and no delivery incentives that compromise objectivity. Independence is not a positioning statement. It is the structural condition that makes validation commercially valuable.

SITG-Consulting will not bid for, deliver, or sub-contract on any remediation programme arising from a validation finding for the same client within twenty-four months of the engagement. The engagement fee is the only fee. There is no downstream revenue line. By design.

brian.couzens@sitg-consulting.com

How We Engage

SITG-Consulting operates on a modular, gated engagement model. Clients select the modules relevant to their current state. Progression is earned through validated evidence.

- Scoping call to establish cryptographic posture, product landscape, and governance maturity.
- Module selection: clients choose from discovery, architecture review, implementation validation, product validation, governance design, supply-chain assurance, or continuous monitoring.
- Gated delivery: each module produces validated, auditable outputs before the next is initiated.
- Validation verdict issued with full evidence pack for board, regulator, procurement, and audit consumption.
- Continuous assurance available post-validation for ongoing drift detection and compliance evidence.

Sector Coverage

SITG-Consulting operates across sectors where cryptographic failure carries systemic, fiduciary, or national-security consequences:

- Financial services: payments, trading, custody, regulatory reporting.
- Healthcare: patient data, connected devices, clinical systems.
- Energy and critical infrastructure: SCADA/OT, long-lifecycle assets, grid control.
- Telecoms: 5G core, network infrastructure, subscriber data.
- Government: sovereign PQC alignment, cross-departmental governance, classified systems.
- Defence and aerospace: supply-chain integrity, embedded systems, mission-critical communications.
- PQC product vendors: independent validation for commercial products entering regulated markets.

Evidence over assumption. Control over narrative.

brian.couzens@sitg-consulting.com
+66 972 176 658

Strategy | Intelligence | Technology | Growth