CAPABILITIES · 2026–2027

SITG-Consulting

Independent advisory and validation for organisations where cryptographic, cyber and governance failure is systemic.

Strategy | Intelligence | Transformation | Governance

Independent Validation, held apart

Global · Headquartered in the United Kingdom · Established 1999



FOREWORD

A NOTE FROM THE CEO

SELECTED PUBLICATIONS

Flagship: A 2026 Global Doctrine for Post-Quantum Cryptography Migration, Board Accountability and Cryptographic Solvency
First published December 2025 as Quantum Risk; current edition May 2026

Cryptographic Transformation and Modernisation
A gated, evidence-driven, multi-year programme model, 2026

Quantum-Resilient Organizational Identity
With Carsten Stöcker and Ingrid Vasiliu-Feltes, 2026

National post-quantum readiness assessments
EU-27, ASEAN-10, BRICS-11, Africa and the United Kingdom, 2026

FIPS 140-3 Thematic Review
First half 2026

A General Theory of Recursive Governance
2026

Quantum Paradox: Why Mitigation is Not Elimination
2025

I began my career as a cost and management accountant. That training never left me. A number means nothing until you can trace it, and a control means nothing until you can test it. To me, process, control and governance are not paperwork. They are how an organisation knows it is telling the truth.

I later served as an intelligence analyst with the British government. The discipline was different but the rule was the same. You separate what is claimed from what is known, you grade every source, and you never brief a conclusion the evidence cannot carry.

Those two disciplines define SITG-Consulting. Since 1999 we have advised boards, regulated institutions, governments and operators of critical infrastructure. Our deepest roots are in financial services: Basel and risk-data governance for global banks, the Sarbanes-Oxley methodology adopted by Shell International, and the recovery of transformation programmes that had lost control. The question at the centre of that work has never changed. Can you prove it?

We take a no-nonsense approach. We do not sell maturity scores, vendor narratives or roadmaps that turn green on a dashboard and fail under scrutiny. We test what is claimed, we say what we find, and we put it in writing for the board, the regulator and the auditor.

That question now carries a deadline. Governments across Europe, the Americas, Asia-Pacific, the Gulf and India have now set national plans for retiring the cryptography that protects payments, identities and infrastructure. I first set out post-quantum migration as a question of board accountability in December 2025, when the market still treated it as a cryptography problem. That paper, now the Global Doctrine, remains the foundation of our work. Our papers have been downloaded thousands of times, and our national readiness assessments cover more than ninety countries. On 15 September 2026, Malaysia's National Security Council, an agency of the Prime Minister's Department, cited our ASEAN assessment in confirming Malaysia as the region's only Tier 1 state.

Our independence is structural. We hold no reseller, referral or commission arrangement with any product vendor, and no equity in the organisations we advise. We never mark our own work. For twenty-four months after a validation we do not sell the remedy, save in extremis with the client's board-level sign-off.

If you want comfort, there are other firms. If you want evidence, talk to us.



Brian Couzens
CEO, SITG-Consulting

HOW THE FIRM IS ORGANISED

Four pillars. One method. Validation held apart.

Each service has a principal home in one of the four pillars that give the firm its name, and contributes to others. Independent Validation is deliberately kept outside them.

SERVICE	S STRATEGY	I INTELLIGENCE	T TRANSFORMATION	G GOVERNANCE
Board Briefing and Readiness Review	●	○		○
Startup Advisory	●	○		
Executive Publications and Strategic Communications	●	○		
Quantum-Cryptographic Discovery Sprint	○	●		
Cyber Discovery Sprint		●		○
Thematic Reviews and National Readiness Reports		●		○
Transformation Leadership and Programme Recovery	○		●	○
Cryptographic Transformation and Modernisation			●	○
Cryptographic Agility		○	●	
Cyber Risk and Resilience		○		●
Cyber Framework Readiness				●
Quantum Governance and Operating Model	○			●

● Principal home ○ Contributes

HELD APART

Independent Validation

Our largest practice, set out on pages 5 and 6. Validation sits outside the four pillars by design. Remediation arising from our findings is not offered to that client for twenty-four months, and every engagement ends in a verdict.

Implementation Validation · Pre-Implementation Review · Product Validation for Vendors · Founder Validation · Supply-Chain Assurance · Continuous Assurance

2030

2035

THE LANDSCAPE

The deadlines are set. Readiness is not.

Cryptographic migration has moved from a research question to a governance obligation, and the evidence of readiness will be asked for by regulators, auditors and buyers.

The standards are published

The core post-quantum algorithm standards are final. The question has moved from what to use to how to migrate under control.

Guidance has become deadlines

National plans now span the United Kingdom, the European Union, India, Malaysia, the United Arab Emirates, Australia and the United States. Critical systems move first, and the leading timetables close by 2035.

Exposure is set by the life of the data

Information encrypted today can be harvested now and decrypted later. The risk to long-lived records has already begun.

> **Claims of quantum-safe readiness now carry regulatory and procurement consequence. They need independent evidence behind them.**



HELD APART FROM THE FOUR PILLARS

Independent Validation

We test what is claimed, and every engagement ends in a verdict.

Products ship with post-quantum labels and programmes declare readiness. Independent Validation establishes whether the claim holds. Verdicts are evidenced, traceable to the tests behind them, and written to enter board records, regulatory submissions and procurement files.

FOR ENTERPRISES

Assurance that a quantum-safe implementation is correct, that supplier claims are substantiated, and that governance can sustain what has been deployed.

FOR VENDORS

An independent verdict on a commercial product before a buyer, a regulator or an auditor tests it for you.

SERVICES

Implementation Validation

Pre-Implementation Review

Product Validation for Vendors

Founder Validation

Supply-Chain Assurance

Continuous Assurance

HOW WE WORK

1 **Scope** the claim and the boundary

2 **Test** against the claim and the standard

3 **Verdict** evidenced and traceable

The twenty-four-month bar. We do not sell the remedy. For twenty-four months after a validation engagement we will not bid for, deliver or sub-contract on any remediation arising from our findings for that client. A waiver exists only in extremis, requires named board-level sign-off from the client, and is disclosed annually in anonymised form. The validation fee buys the verdict and nothing else.

We never mark our own work. We do not validate anything we delivered. Where we designed a programme that others delivered, we may validate the implementation.

INDEPENDENT VALIDATION

What we validate, and what the verdict means

Any product, platform, protocol or implementation that claims to be quantum-safe, for the organisations deploying it and for the vendors selling it.

ENTERPRISE IMPLEMENTATIONS

- VPN, TLS and network encryption
- Key management, hardware security modules and entropy
- PKI, certificate authorities and digital signatures
- Cloud platforms, APIs and microservices
- Identity, messaging and database encryption
- Connected-device and industrial firmware, wallets and ledgers

COMMERCIAL PRODUCTS

- Cryptographic discovery and inventory tools
- Crypto-agility platforms and endpoint agents
- Quantum random number generators and quantum key distribution
- Post-quantum cryptography as a service, and network appliances
- Libraries and software development kits
- Founder products before market or investment

EVERY ENGAGEMENT ENDS IN ONE OF THREE VERDICTS

Validated

Genuine implementation. Algorithms correctly deployed. Governance sufficient. Fit for purpose.

Conditional

Partial implementation or governance gaps. Remediation path defined. Re-validation required.

Not Validated

Claims not substantiated. Mislabelled, wrapped or structurally non-compliant.

Verdicts are evidenced, traceable to the tests behind them, and written to enter board records, regulatory submissions, procurement files and vendor collateral.

> **Technical validation without governance validation is incomplete. If the governance cannot sustain the implementation, it is not validated.**

ONE METHOD

One method. Each engagement enters it where the client stands.

Whatever the domain, the regulation or the technology, control is established in the same disciplined order. Each phase produces auditable outputs before the next is released.

I	II	III	IV	V
DISCOVER	**GOVERN**	**TRANSFORM**	**ASSURE**	**SUSTAIN**
Forensic visibility of assets, dependencies, exposure and claims across the estate.	Decision rights, accountability and mandatory gates set before execution begins.	Risk-prioritised change, delivered in waves with validated outputs at every stage.	Independent testing of what is claimed against what is deployed.	Continuous monitoring, drift detection and evidence as a permanent capability.

No phase progresses without validated evidence.

Engagements enter where the client's condition requires: at discovery, in recovery mid-programme, or at the point of independent validation.

S

STRATEGY

PILLAR I S

STRATEGY

Board-level direction on cryptographic, cyber and regulatory risk, framed as liability, investment and accountability.

Boards are asked to approve programmes they cannot see inside. We give directors and executives an independent reading of exposure, options and consequence, and the decision structures to act on it. For founders building security, AI and technology products, the same discipline is applied to the product, its claims and its route to regulated markets.

SERVICES

Board Briefing and Readiness Review

Startup Advisory

Executive Publications and Strategic Communications

HOW WE WORK

1 **DIAGNOSE** exposure and current position

2 **FRAME** as liability, cost and obligation

3 **DECIDE** options with their consequences

4 **EVIDENCE** a decision the record can carry

> **EVERY RECOMMENDATION IS TRACEABLE TO EVIDENCE THE BOARD CAN SEE.**

I

INTELLIGENCE

PILLAR II I

INTELLIGENCE

Forensic visibility of estates, exposure and claims, established before any decision is taken.

An organisation cannot govern what it cannot see. Our discovery sprints and thematic reviews establish where cryptographic and cyber exposure sits, what depends on it, and how far reported readiness matches the evidence. Our published national readiness assessments apply the same discipline at country level, across more than ninety countries in Europe, ASEAN, Africa and the BRICS group.

SERVICES

Quantum-Cryptographic Discovery Sprint

Cyber Discovery Sprint

Thematic Reviews and National Readiness Reports

HOW WE WORK

1 **SCOPE** the question and the boundary

2 **COLLECT** evidence from systems and people

3 **ANALYSE** against the claim

4 **REPORT** findings and consequence

5 **PLAYBACK** to the decision-makers

EVIDENCE BEFORE OPINION.

T

TRANSFORMATION

PILLAR III T

TRANSFORMATION

Cryptographic and enterprise change delivered under control: gated, wave-based and phased.

Cryptographic modernisation is a multi-year programme across systems, suppliers and governance, not a product purchase. We design and oversee it in waves prioritised by business criticality and the life of the data, with mandatory gates between phases. The same discipline recovers stalled enterprise programmes.



SERVICES

Cryptographic Transformation and Modernisation

Cryptographic Agility

Transformation Leadership and Programme Recovery

HOW WE WORK

1 **MANDATE** business case, funding and ownership

2 **DISCOVER** inventory, risk and target architecture

3 **TRANSITION** in waves, each one gated

4 **OPERATE** and prove control continuously

Published as the SITG-Consulting Cryptographic Transformation Implementation Model.

NO WAVE ADVANCES WITHOUT EVIDENCE THAT THE LAST ONE HOLDS.



GOVERNANCE

PILLAR IV G

GOVERNANCE

Accountability, oversight and resilience that withstand examination by boards, regulators and auditors.

Cyber and cryptographic risk is a governance responsibility, not a technology line item. We embed it in enterprise risk frameworks, assign clear ownership, and prepare organisations for the control frameworks their regulators and buyers apply. We start from the client's own jurisdiction: national schemes and regulators lead, with international frameworks applied where markets require them. Resilience is modelled against realistic scenarios, including third-party concentration and long-lived assets.

SERVICES

Cyber Risk and Resilience

Cyber Framework Readiness: national and international frameworks

Quantum Governance and Operating Model

HOW WE WORK

1 **ASSESS** posture against the obligation

2 **ALIGN** risk to the enterprise framework

3 **ASSIGN** ownership and decision rights

4 **ASSURE** with evidence, not assertion

> **COMPLIANCE BECOMES AN OUTCOME OF CONTROL, NOT A TARGET.**

WHERE WE OPERATE

Sectors where failure is systemic

Cryptographic, cyber and governance failure in these sectors carries fiduciary, systemic or national-security consequence.

Financial Services

Payments, trading, custody and regulatory reporting, where resilience rules meet long-lived financial records.

Healthcare and Life Sciences

Patient data, connected medical devices and clinical systems, where confidentiality must outlast the record.

Energy and Critical Infrastructure

Control systems and grid assets with lifespans beyond twenty years, deployed today and expected to stay trusted.

Telecoms

Core networks, subscriber data and the infrastructure of national communications.

Government and Public Sector

Sovereign cryptographic policy, national-scale delivery assurance and cross-departmental governance.

Defence and Aerospace

Supply-chain integrity, embedded systems and mission-critical communications.

A common thread. Long-lived data, long-lived assets and regulators who now expect evidence. These are environments where proof of control is the operating licence.

NEXT STEPS

Where engagements begin

1

Scoping conversation

Current posture, regulatory exposure and governance maturity. No commitment beyond the conversation.

2

Entry engagement

A defined, time-bounded engagement that establishes visibility and evidence quickly.

3

Gated delivery

Each module produces validated, auditable outputs before the next is released.

4

Continuous assurance

Monitoring, drift detection and compliance evidence as an ongoing capability.

THE PRIMARY ENTRY POINT

Quantum-Cryptographic Discovery Sprint

A structured, time-bounded diagnostic that establishes cryptographic visibility, quantum exposure and a defensible, risk-prioritised migration pathway.

The client receives an initial cryptographic inventory and asset view, a risk and exposure heatmap, a migration roadmap and a board-level business case.

It leads into the gated transformation programme, or into independent validation of what is already deployed. Scope, team and duration are calibrated to the client, not packaged.

ENTRY ENGAGEMENTS

Quantum-Cryptographic Discovery Sprint · Cyber Discovery Sprint · Pre-Implementation Review · Thematic Reviews and National Readiness Reports · Board Briefing and Readiness Review

BUILT TO BE EXAMINED BY

Boards · Regulators · Auditors · Procurement teams · Chief information security officers · Government agencies · Critical infrastructure operators · Financial institutions

Begin with the question you cannot yet answer with evidence.



COMPLIANCE YOU CAN EVIDENCE.
ASSURANCE YOU CAN TRUST.

info@sitg-consulting.com · +66 97 217 6658 · www.sitg-consulting.com

SITG-Consulting · Global · Headquartered in the United Kingdom

STRATEGY | INTELLIGENCE | TRANSFORMATION | GOVERNANCE

© 2026 SITG-Consulting and Brian Couzens. All rights reserved. Registered in England and Wales. Co Number: 16881730.