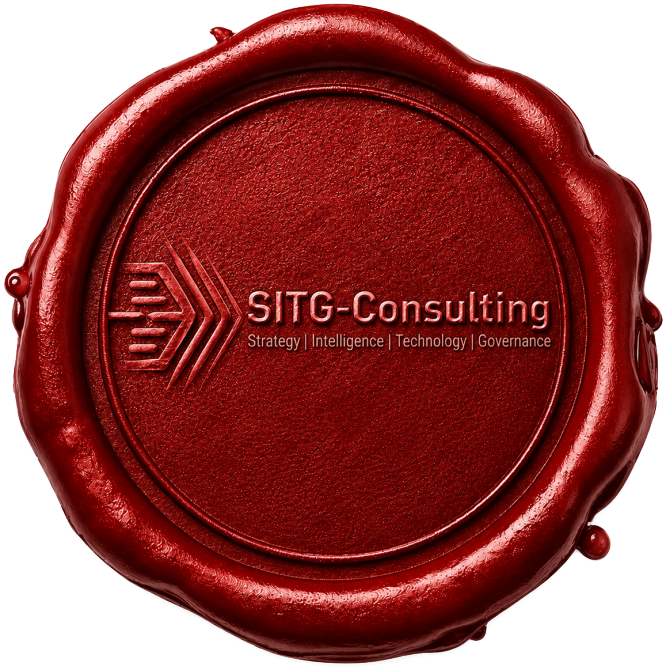
INDEPENDENT TRANSFORMATION · GOVERNANCE · ASSURANCE

SITG-CONSULTING

CORPORATE CAPABILITIES · 2026



Authority without evidence is narrative. Evidence without authority is ignored.
We provide both.

THE PREMISE

Organisations rarely fail for lack of strategy.
They fail for lack of control.

SITG-Consulting is an independent transformation, governance and assurance firm operating in complex cyber, regulatory and cryptographic environments. We help organisations establish five conditions that complexity erodes: visibility, governance, transformation under control, assurance and evidence.

This publication sets out how those conditions are built, the practices that deliver them, and the standard of proof to which we hold our own work.

CONTENTS

An independent firm for environments where control is non-negotiable

SITG-Consulting is an independent transformation, governance and assurance firm operating in complex cyber, regulatory and cryptographic environments. Founded in 1999 and headquartered in the United Kingdom, the firm advises boards, regulated institutions, governments and critical infrastructure operators worldwide.

We are retained where failure is systemic rather than local: where governance gaps, cryptographic drift, stalled programmes or data failures can cascade across an enterprise or across national infrastructure. Our approach is forensic. We expose blind spots, challenge assumptions and engineer outcomes that stand up to scrutiny.

INDEPENDENCE, BY STRUCTURE

No vendor partnerships. No equity stakes in clients. No delivery incentives that compromise objectivity. Independence is not a positioning statement. It is the structural condition that makes our judgement commercially valuable.

STRATEGY

Governance structures, transformation roadmaps and executive accountability frameworks aligned with organisational objectives.

INTELLIGENCE

Forensic analysis, quantitative diagnostics and evidence-based assessment that identify risk and validate assumptions.

TECHNOLOGY

Cyber resilience, quantum risk, cryptographic dependencies and emerging technologies assessed to strengthen readiness and control.

GOVERNANCE

Clear accountability, evidence-based oversight and decision structures that strengthen organisational control, resilience and trust.

EST. 1999 · UK HEADQUARTERED · OPERATIONAL IN THE UNITED KINGDOM, UNITED STATES, OMAN, THAILAND AND AUSTRALIA

Leadership is rarely short of information. It is short of coherence.

Information sits fragmented across teams, suppliers, tools, reports and governance structures. As environments grow more complex, boards receive multiple and sometimes conflicting narratives about risk, readiness and progress.

The consequence is predictable. Transformation programmes appear to advance but do not establish control. Readiness is declared but cannot be demonstrated. Vendor claims are accepted but never tested. When a regulator, an auditor or an incident finally asks the question, the evidence is not there.

If control cannot be demonstrated,
it cannot be considered established.

FRAGMENTED VISIBILITY

Cryptographic inventories, cyber exposure and programme status held in disconnected silos. No single, defensible view of the estate.

UNGOVERNED EXECUTION

Programmes that progress by timeline rather than by validated evidence. Direction without control.

UNVERIFIED CLAIMS

Vendor outputs, readiness declarations and maturity scores accepted without independent testing.

ABSENT EVIDENCE

An inability to demonstrate readiness to boards, regulators and auditors at the moment it matters.

OUR CENTRAL PREMISE

Five conditions separate organisations that govern complexity from organisations governed by it

I

Visibility

You cannot govern what you cannot see. We establish a single, evidenced view of estates, exposures, dependencies and claims.

II

Governance

Decisions made, documented and challenged through structures that withstand examination by boards, regulators and auditors.

III

Transformation

Change delivered through gated, risk-prioritised execution. Progression is earned through evidence, never assumed through timelines.

IV

Assurance

Independent validation that controls operate as intended in practice, and that what is claimed is what is deployed.

V

Evidence

Proof engineered to survive board examination, regulatory inquiry, procurement diligence and external audit.

Every SITG engagement is designed to establish at least one of these conditions, and to strengthen all five.

Discover · Govern · Transform · Assure · Sustain

One operating philosophy organises everything the firm does. Whatever the domain, whatever the regulation, whatever the technology, control is established in the same disciplined sequence.

Discover

Establish visibility. Forensic discovery of assets, dependencies, exposures and claims across the estate.

Govern

Establish authority. Decision rights, accountability, risk appetite and mandatory gates set before execution begins.

Transform

Execute change under control. Risk-prioritised, gated delivery with validated outputs at every stage.

Assure

Validate independently. Test what is claimed, examine what is deployed, issue a defensible verdict.

Sustain

Operate and prove. Continuous monitoring, drift detection and evidence production as a permanent capability.

No phase progresses without validated evidence.

Engagements enter the model wherever the client's condition requires: at discovery, in recovery mid-transformation, or at the point of independent assurance.

One model, every discipline

Each practice expresses the same philosophy at a different point of the control lifecycle. Filled marks denote a practice's centre of gravity; open marks denote its supporting reach.

		DISCOVER	GOVERN	TRANSFORM	ASSURE	SUSTAIN
I	Enterprise Transformation Leadership	○	●	●	○	○
II	Cyber Risk & Resilience	●	●	○	●	○
III	Quantum Trust & PQC Assurance	●	○	●	●	●
IV	Independent Reviews & Thematic Assessments	●	○	○	●	○
V	Executive Publications & Strategic Communications	○	●	○	○	●

● Centre of gravity ○ Supporting reach

Transformation, resilience, quantum trust, reviews and publications: one operating philosophy, expressed five ways.

One philosophy, five practices

SITG-Consulting is broader than any single practice. The firm is organised around five disciplines that reinforce one another: visibility feeds governance, governance directs transformation, transformation is tested by assurance, and evidence carries the result to the people who must act on it.

I

Enterprise Transformation Leadership

Leading, recovering and governing complex change in regulated environments.

PAGE 09

II

Cyber Risk & Resilience

Evidence-led cyber governance, operational resilience and regulatory readiness.

PAGE 10

III

Quantum Trust & PQC Assurance

Independent validation and governance for the quantum era. The firm's deepest specialism.

PAGES 11–13

IV

Independent Reviews & Thematic Assessments

Independent visibility into the risks, controls and decisions that matter.

PAGE 14

V

Executive Publications & Strategic Communications

Board-grade publications and evidence-driven communication, as a formal service.

PAGE 15

Not a service catalogue. A control system.

Enterprise Transformation Leadership

Direction is abundant. Control is rare.

We lead, oversee and recover complex change in regulated environments, on the principle that transformation is a governance discipline before it is a delivery exercise. Engagements span banking, payments, insurance, healthcare, energy, telecoms and government.

SELECTED OUTCOMES

SOX methodology authored for Shell International; Basel and BCBS239 governance frameworks for global banks.

BCBS239 and GDPR remediation with data-lineage solutions improving reporting accuracy and traceability.

Financial-crime remediation coordinating technical tracing, legal handoffs and operational fixes.

Recovered delivery on failing initiatives through governance redesign, PMO establishment and disciplined execution.

— REGULATORY TRANSFORMATION

Basel, BCBS239, Solvency II, DORA and GDPR programmes that expose systemic gaps and align governance with mandate.

— PROGRAMME RECOVERY

Stalled and failing initiatives restored through governance redesign, PMO establishment and disciplined execution.

— TRANSFORMATION OVERSIGHT

Independent oversight of in-flight programmes on behalf of boards, sponsors and regulators.

— EXECUTIVE GOVERNANCE

Accountability frameworks, board reporting and decision structures that withstand examination.

— DATA & CLOUD STABILITY

Audit-ready frameworks across AWS, Azure and GCP, with data lineage and reporting integrity engineered in.

— OPERATING MODELS

Target operating models that carry programmes into sustainable operational ownership.

— DIGITISATION INITIATIVES

Controlled execution of digitisation mandates, open banking and resilience regulation, with auditability designed in from the start.

Cyber Risk & Resilience

Cyber security is now a governance responsibility, not a technology line item.

We provide independent, evidence-led assessment of cyber risk posture, resilience gaps and governance weaknesses for complex, regulated organisations. Critical assets are mapped to realistic threat scenarios, exposing the resilience gaps that compliance audits overlook, and every finding is tied to a clear consequence for continuity, resilience or regulatory standing.

Operational resilience goes beyond continuity planning: the ability to absorb, adapt and respond to shock without losing critical services, with third-party concentration risk and cyber-physical dependencies modelled rather than assumed.

Compliance becomes a natural outcome, not a target.

THE TRIPLE-A GOVERNANCE STANDARD

ALIGNMENT

Cyber risk embedded in enterprise risk frameworks and communicated in the language of the board.

ACCOUNTABILITY

Clear lines of responsibility that withstand examination by boards, regulators and external auditors.

ASSURANCE

Evidence-led assurance that demonstrates resilience rather than asserting it.

NIST CSF 2.0 & NIS2

Implementation and maturity of NIST CSF 2.0 across its six functions, for governments, critical infrastructure and regulated enterprises. NIS2 readiness assessed against documented evidence of systemic resilience.

GOVERN	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER

FRAMEWORK ALIGNMENT

NIST CSF 2.0 · NIS2 · ISO/IEC 27001 & 27002 · DORA · NCSC CAF · CIS Controls · COBIT · SOC 2 · Essential Eight · APRA CPS 234 · MAS · GCC and national cyber frameworks

Quantum Trust & PQC Assurance

The market is saturated with post-quantum claims. The question is whether any of it is real.

Products ship with post-quantum labels. Programmes declare readiness. Discovery tools assert comprehensive coverage. PQC programmes fail for a simple reason: they focus on cryptography, not control. We provide independent, evidence-led validation for enterprises deploying quantum-safe cryptography and for vendors building quantum-safe products. We test what is claimed. We issue a verdict. We produce the artefacts that boards, regulators, auditors and procurement teams require.

TWO AUDIENCES, ONE STANDARD

Enterprises deploying PQC. Independent assurance that implementations are correct, vendor claims substantiated, and governance able to sustain what has been deployed.

Vendors selling PQC products. A defensible, independently validated market position before a buyer, a regulator or an auditor tests the product for you.

SEVEN ASSURANCE MODULES

1 PQC DISCOVERY & EXPOSURE ASSESSMENT
Where cryptography exists, hidden dependencies, harvest-now-decrypt-later exposure.

2 CRYPTO-AGILITY & ARCHITECTURE READINESS
Capacity to rotate algorithms, sustain hybrid cryptography and adapt without disruption.

3 PROTOCOL & IMPLEMENTATION VALIDATION
Real PQC usage in live traffic, implementation correctness, entropy quality, vendor claims.

4 PRODUCT VALIDATION, VENDOR PROGRAMME
Commercial PQC products tested against their claims, published standards and operational reality.

5 QUANTUM GOVERNANCE & OPERATING MODEL
Crypto ownership, lifecycle control and board-level oversight. Deployment without governance is exposure with a different label.

6 PQC SUPPLY-CHAIN ASSURANCE
Third parties rated for genuine readiness, dependency exposure and cryptographic transparency.

7 CONTINUOUS QUANTUM ASSURANCE
Ongoing validation, drift detection, vendor posture tracking and compliance evidence.

QCAS, the Quantum Cryptographic Assurance Standard

QCAS v1.1 is the formal methodology, authored by SITG-Consulting, for validating cryptographic resilience against quantum threats. It aligns with NIST FIPS 203, 204 and 205, FIPS 140-3, CNSA 2.0, ISO/IEC 19790 and the ETSI QKD frameworks, and maps to the US SEC cyber rules, EU DORA, MAS guidelines and APRA CPS 234. Asset owners maintain a machine-readable Cryptographic Bill of Materials and demonstrate active crypto-agility.

32	8	22	3	2
TECHNICAL CONTROLS	CONTROL DOMAINS	REFERENCED STANDARDS	VALIDATION VERDICTS	OPERATIONAL SCOPES

Governance is examined alongside the technology: documentation completeness, change management, SDLC maturity, configuration management, incident preparedness and audit trail integrity. If the governance structure cannot sustain the implementation, the implementation is not validated.

EVERY ENGAGEMENT ENDS IN A 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 collateral.

The Cryptographic Transformation Implementation Model

A gated, evidence-driven programme architecture spanning six levels, from board mandate to continuous proof. This is not a migration project. It is the establishment of a sustainable cryptographic operating capability, governed through mandatory gates.

L0 EXECUTIVE BOARD VIEW

Business mandate, funding, governance and accountability.

L1 PROGRAMME VIEW

Discover, control, transform and sustain as the tactical sequence.

L2 GOVERNANCE GATES

Formal decision points that prevent uncontrolled progression.

L3 ENGINEERING EXECUTION

Discovery, inventory, migration, interoperability and monitoring.

L4 OPERATING MODEL

Transition from programme delivery to operational ownership.

L5 CONTINUOUS EVIDENCE

Ongoing assurance, reporting and proof of control.

SIX MANDATORY GATES

- **G1** Business case and executive mandate
- **G2** CBOM and risk approval
- **G3** Architecture approval
- **G4** Vendor and supply chain readiness
- **G5** Go-live and interoperability validation
- **G6** Operational handover and assurance

Transformation is delivered in prioritised waves, ordered by business criticality, data sensitivity, regulatory obligation, operational exposure and long-term confidentiality requirements.

If you cannot operate it and prove it, you do not control it.

Independent Reviews & Thematic Assessments

When leadership receives conflicting narratives, an independent review establishes what is actually happening.

A thematic review is an evidence-based assessment of how a specific issue operates across systems, functions, suppliers and decision-making processes. The objective is simple: establish what is happening, where material risk exists, and what should follow. Reviews span governance, board effectiveness, readiness, vendors, risk, operations and assurance.

HOW A REVIEW WORKS

1	2	3	4	5
SCOPE	COLLECT	ANALYSE	REPORT	PLAYBACK

Outputs are written for decision-makers, auditors, regulators and programme leaders, and validate or challenge internal opinion on control effectiveness.

SIX LENSES OF EXAMINATION

GOVERNANCE

How decisions are made, documented and challenged.

VENDOR CAPABILITY

Supplier claims, outputs and dependencies tested.

OPERATIONAL BEHAVIOUR

How teams actually work against documented process.

RISK VISIBILITY

Whether leadership holds an accurate picture of exposure.

CONTROL EFFECTIVENESS

Whether controls operate as intended in practice.

EVIDENCE INTEGRITY

Whether conclusions rest on verifiable evidence.

Evidence before opinion. Independence by design.

TYPICAL DELIVERABLES

Executive summary · Evidence-based findings · Root cause analysis · Risk prioritisation · Dependency assessment · Governance observations · Remediation roadmap · Executive presentation and playback

PRACTICE V

Executive Publications & Strategic Communications

Documentation is not treated as a communication exercise. It is treated as evidence.

Organisations can write. Very few can write with authority, empirical grounding and regulatory defensibility. We produce high-authority written assets engineered for boards, regulators and investors: publications that withstand scrutiny, influence regulators and equip executives with narratives built on validated data. Nothing is published without a traceable verification chain.

We work on the assumption that every word will be read by a competitor, a regulator or an adverse analyst. Every claim is evidence-indexed accordingly. This is a formal service offering, delivered to the same gated standard as every other practice.

AUTHORING METHODOLOGY

1	2	3	4
FORENSIC INTERROGATION	EVIDENCE-DRIVEN AUTHORING	ITERATIVE VERIFICATION	GOVERNANCE REVIEW

WHAT WE PRODUCE

— **WHITE PAPERS & TECHNICAL PUBLICATIONS**

Deep research and reproducible analysis, 40 to 80 pages, built to define categories and act as industry reference points.

— **BOARD BRIEFINGS & EXECUTIVE MEMOS**

Clipped, high-density intelligence for high-stakes decisions, board votes and fiduciary-risk framing.

— **REGULATORY SUBMISSIONS & POSITION PAPERS**

Technically precise, defensible documents that move seamlessly from a conference stage to a regulatory inquiry.

— **INDUSTRY REBUTTALS & STRATEGIC NARRATIVES**

Independent, empirical responses to market claims. Narrative built on data, not opinion.

— **GHOSTWRITING, KEYNOTES & CONFERENCE ASSETS**

Speeches, op-eds, speaker packs and evidence-grade event content where accuracy carries the brand.

Your presence at a global summit should be defined by the quality of your evidence, not just the quality of your slides.

WHERE ENGAGEMENTS BEGIN

Entry engagements

Defined, time-bounded engagements that establish visibility and evidence quickly, and create the baseline from which governance, transformation and assurance proceed. Calibrated, not packaged: scope, team and duration reflect regulatory exposure, architectural complexity and governance maturity.

20–30 DAYS

Quantum Discovery Sprint

Cryptographic visibility, quantum exposure analysis and a defensible, risk-prioritised migration pathway for board-level stakeholders.

TIME-BOUNDED

Cyber Discovery Sprint

A defensible view of cyber governance, exposure and operational resilience. Structural weaknesses and blind spots surfaced as a clear baseline.

SCOPED TO THEME

Thematic Review

Independent, evidence-based assessment of a defined technical, governance or operational theme, with executive playback.

FRAMEWORK-LED

NIST CSF 2.0 Assessment

Current state, framework mapping, gap analysis and target operating model across the six CSF functions.

VERDICT-LED

PQC Readiness Review

Implementation, architecture and governance readiness examined under QCAS, concluding in a defensible validation verdict.

BOARD-LEVEL

Board Readiness Review

Oversight structures, accountability and fiduciary exposure framed in board-ready language, with liability and solvency in view.

Each engagement produces validated, auditable outputs before any further phase is initiated.

Sectors where failure is systemic

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

FINANCIAL SERVICES

Payments, trading, custody and regulatory reporting. AML and sanctions remediation, Basel IV alignment, BCBS239 lineage, DORA resilience and solvency-aligned quantum governance.

HEALTHCARE & LIFE SCIENCES

Clinical systems safety, patient data, connected devices, and the privacy liability attached to biometric and genetic assets.

ENERGY & CRITICAL INFRASTRUCTURE

SCADA and OT security governance, grid control and cryptographic estate mapping for assets with lifespans beyond twenty years.

TELECOMS

5G core and network infrastructure, subscriber data, platform modernisation and PQC readiness for national communications.

GOVERNMENT & PUBLIC SECTOR

Policy-aligned transformation, national-scale delivery assurance, sovereign PQC alignment and cross-departmental governance.

DEFENCE & AEROSPACE

Supply-chain integrity, embedded systems and mission-critical communications under sustained adversary interest.

PQC PRODUCT VENDORS

Independent validation for commercial products entering regulated markets: the evidence buyers and regulators will ask for.

A COMMON THREAD

Long-lived data, long-lived assets and short regulatory patience. Environments where evidence of control is the operating licence.

Independence & evidence

Validation is only commercially valuable when the validator has nothing to gain from the answer.

SITG-Consulting holds no vendor partnerships, no equity stakes in clients and no delivery incentives that compromise objectivity. Where a validation engagement produces findings, the firm will not bid for, deliver or sub-contract on any remediation programme arising from those findings for the same client within twenty-four months.

The engagement fee is the only fee.
There is no downstream revenue line. By design.

01 **No vendor partnerships.** Every technology is assessed on evidence, never on alliance.

02 **No equity stakes.** No financial interest in any client outcome beyond the quality of the work.

03 **The 24-month bar.** Findings can never become a sales pipeline. Verdicts stay clean.

04 **Evidence as the standard.** Conclusions grounded in demonstrable evidence rather than maturity scores, assumptions or marketing claims.

EVIDENCE OVER ASSUMPTION · CONTROL OVER NARRATIVE

Forensic by training, independent by conviction

BRIAN COUZENS · FOUNDER & CEO

Forensic strategist, transformation leader and global PQC thought leader. Brian leads SITG-Consulting's work across quantum risk, cryptographic governance, regulatory transformation and board advisory. His career spans the critical sectors: financial services, healthcare, energy and critical infrastructure, telecoms and central government, in environments where failure is systemic rather than local.

He is the author of the Quantum Cryptographic Assurance Standard (QCAS) and of the SITG-Consulting Cryptographic Transformation Implementation Model, and has authored the SOX methodology adopted by Shell International alongside Basel and BCBS239 frameworks for global institutions.

PUBLISHED AUTHORITY

- **Eight white papers** on quantum risk, PQC governance, CBOM frameworks and cryptographic transformation, with further titles scheduled for 2026.
- **Joint authorship by invitation** with established professors and practitioners in quantum and cryptographic governance, a rarity that reflects the credibility of the firm's research position.
- **QCAS v1.1**, the formal assurance standard referenced throughout this brochure, issued 2024.
- **The SITG bench** deploys board-level strategists, regulatory architects, cryptography engineers, quantum computing specialists, risk analysts, auditors and programme leadership, aligned to phase, risk state and governance requirement.

How we engage

SITG-Consulting operates a modular, gated engagement model. Clients select the modules relevant to their current state. Progression is earned through validated evidence, never assumed through timeline.

1

SCOPING

A scoping call establishes current posture, regulatory exposure and governance maturity. No commitment beyond the conversation.

2

MODULE SELECTION

Discovery, review, governance alignment, transformation, validation or board advisory, chosen to fit the condition, not the catalogue.

3

GATED DELIVERY

Each module produces validated, auditable outputs before the next is initiated. Evidence accumulates as the engagement proceeds.

4

CONTINUOUS ASSURANCE

Post-engagement monitoring, drift detection and compliance evidence, available as an ongoing capability.

BUILT TO BE EXAMINED BY

Boards · Regulators · Procurement teams · CISOs, CIOs and CTOs · Government agencies · Critical infrastructure operators · Financial institutions · External auditors · PQC vendors

Begin with the question you cannot yet answer with evidence.

Compliance you can evidence.
Assurance you can trust.

ENGAGEMENT ENQUIRIES

For discovery sprints, thematic reviews, validation engagements, board briefings and publication commissions. An initial scoping conversation establishes posture, exposure and fit, and carries no commitment beyond the conversation itself.

EMAIL	info@sitg-consulting.com
TELEPHONE	+66 97 217 6658
WEBSITE	www.sitg-consulting.com

OPERATIONAL PRESENCE

United Kingdom	United States	Oman	Thailand	Australia
HEADQUARTERS	OPERATIONS	OPERATIONS	OPERATIONS	OPERATIONS