Cryptographic Transformation and Modernisation

A Gated, Evidence-Driven, Multi-Year Programme

The SITG-Consulting Cryptographic Transformation Implementation Model

Levels 0–5 | Multi-Year Transformation Programme

Abstract:
The SITG-Consulting Cryptographic Transformation Implementation Model is a gated, evidence-driven programme model for enterprise-scale cryptographic migration, built from operational delivery experience across regulated, multi-jurisdictional environments. If an organisation cannot operate its cryptographic estate and prove control continuously, it does not control it at all.

"Authority without evidence is narrative. Evidence without authority is ignored. We provide both." Brian Couzens, 2024.

PRACTITIONER HANDBOOK | COMMERCIAL IN CONFIDENCE

Version: 8.1 | April 2026

Author: Brian Couzens

Foreword

This is Version 8.1 of the SITG-Consulting Cryptographic Transformation Implementation Model. It reflects substantive revision through independent peer review and quality audit conducted in April 2026, covering structural integrity, regulatory precision, voice, and editorial discipline. The reviewers identified specific points at which earlier versions would be challenged under multi-jurisdictional regulatory scrutiny, post-incident audit, or conditions the model had previously assumed would not arise. Where the reviewers were right, the handbook has been revised. Where they drifted from model into implementation detail, the recommendations have been noted and respectfully declined. The reviewers are thanked for their rigour and remain anonymous at their request.

This handbook is written for transformation leads, programme directors, and governance practitioners with prior experience of enterprise-scale programme delivery in regulated environments. It assumes the reader will engage cryptographic specialists, security architects, and PKI engineers as subject matter experts during execution. It does not teach cryptography. It does not substitute for the specialist advice a real programme requires at the engineering layer. It is the governance model the transformation lead operates within, and the evidence standard against which the specialists' work is tested. Readers without transformation delivery experience in regulated environments, and organisations without access to cryptographic subject matter expertise, should engage specialist support before attempting to apply the model.

The model reflects patterns observed across cryptographic transformation delivery engagements in regulated, multi-jurisdictional environments. It is not derived from a single named client and carries no warranty of outcomes for any specific organisation. What it offers is the structural discipline that has held up under the conditions described, presented as a practitioner handbook that organisations can apply, adapt, and govern against their own risk appetite.

This handbook is a living document. The regulatory landscape, the standards ecosystem, and the vendor capability frontier all continue to move. Revisions will follow as material change demands. Readers should confirm the currency of regulatory citations before relying on them operationally.

Brian Couzens

April 2026

Table of Contents

1. Executive Summary

Cryptographic infrastructure is failing. Not because of algorithm weakness. Because of governance failure, operational opacity, and the systematic absence of structured programme delivery.

Across every regulated sector: financial services, telecommunications, government, critical national infrastructure, healthcare, the same pattern repeats. Organisations know quantum-era cryptographic migration is mandatory. They have read the NIST standards. They have attended the briefings. And then they commission a discovery exercise, produce a report, and stall. The gap between knowing and doing is where the risk lives.

The SITG-Consulting Cryptographic Transformation Implementation Model closes that gap. It is a practitioner handbook: a structured, gated, evidence-driven programme model built from operational delivery experience across complex, regulated, multi-jurisdictional environments. Its design reflects what actually stalls, fails, and succeeds when cryptographic transformation is executed at enterprise scale: the governance breakdowns that derail programmes, the vendor assurance gaps that create false confidence, and the evidence requirements that regulators and auditors enforce in practice. It is designed to be applied, not theorised, at the scale and consequence level where cryptographic failure has systemic impact rather than theoretical impact.

PREMISE | 01

Cryptographic transformation is not a migration. It is a multi-year, risk-driven, wave-based programme that must be operated, governed, and evidenced at every stage. If you cannot operate it and prove it, you do not control it.

The model operates across six levels, from Executive Board mandate through engineering execution to operational assurance, each with defined inputs, outputs, governance gates, and evidence artefacts. The transformation roadmap aligns these levels to a time-sequenced delivery arc that is risk-prioritised, not linear. Programme duration is not fixed at 36 months. It is determined by estate scale, jurisdictional complexity, regulatory entry tier, vendor readiness, and organisational change capacity. Real programmes run from eighteen months to ten years depending on these factors.

DURATION | 02

Thirty-six months is illustrative, not prescriptive. Programme duration is a function of estate scale, jurisdictional complexity, entry tier, vendor readiness, and organisational change capacity. A mid-size insurer with a clean single-jurisdiction estate may complete in eighteen months. A global financial institution with multi-jurisdictional operations and legacy embedded device populations will run for five to ten years. The gates and evidence requirements are invariant. The timeline is not.

This handbook presents the model in full. It is addressed to the executives, architects, regulators, and programme leaders who must make the decisions, allocate the resources, and bear the accountability for what happens to cryptographic infrastructure over the next decade.

The decisions taken in the next twelve months will determine the organisation’s position in the transition.

2. Why Cryptographic Transformation Is Now a Board-Level Mandate

The quantum threat to classical cryptography is no longer speculative. NIST published its first post-quantum cryptographic standards in August 2024: FIPS 203 (ML-KEM – Module-Lattice-Based Key-Encapsulation Mechanism), FIPS 204 (ML-DSA – Module-Lattice-Based Digital Signature Algorithm), and FIPS 205 (SLH-DSA – Stateless Hash-Based Digital Signature Algorithm), establishing the algorithmic baseline for a global transition that is now in motion (source: NIST Post-Quantum Cryptography Standardisation, csrc.nist.gov, verified April 2026). OMB Memorandum M-23-02, “Migrating to Post-Quantum Cryptography,” directs federal agencies to inventory and prioritise cryptographic systems for migration, with the initial inventory submission deadline of May 2023 now nearly three years past (source: whitehouse.gov/omb, November 2022). The NSA’s Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), published September 2022, sets transition timelines by asset category for National Security Systems (NSS) and their supply chains: software and firmware January 2025, network security devices end 2026, operating systems and browsers 2027, with full transition of legacy cryptography in NSS by 2033. CNSA 2.0 applies directly to National Security Systems and organisations in the NSS supply chain, not universally to US commercial entities. Organisations in the NSS supply chain that have not completed software and firmware transition are non-aligned with the stated CNSA 2.0 timeline and should assess their position against their specific contractual and regulatory obligations. The EU’s Digital Operational Resilience Act (DORA, Regulation 2022/2554) entered full application in January 2025, imposing ICT risk management requirements including cryptographic obligations on financial entities across the EU. The Network and Information Security Directive (NIS2, Directive 2022/2555) required member state transposition by October 2024 and extends comparable obligations to essential and important entities in critical infrastructure and telecommunications.

Beyond the NIST-aligned instruments, a second class of regulatory requirement applies to organisations operating in jurisdictions with independent cryptographic standards bodies. China’s Cryptography Law, administered by the Office of State Commercial Cryptography Administration (OSCCA), mandates nationally approved algorithms (SM2, SM3, SM4) for domestic regulated applications. These requirements are structurally incompatible with a NIST-only architecture and cannot be resolved through cryptographic agility, because the divergence sits at the national approval layer, not the implementation layer. Organisations with Chinese operations require a dual-stack architecture: a NIST-aligned estate for non-Chinese jurisdictions and an SM-family estate for Chinese domestic regulated applications. The operational specifics of the Chinese stack are out of scope for this handbook; organisations in this situation should engage specialists with demonstrated China delivery experience.

Additional regulatory instruments that apply to specific jurisdictions and sectors include: BSI TR-02102 (Germany) which specifies federal algorithm recommendations with parameter requirements diverging from NIST in certain categories; ANSSI position papers (France) which impose an independent algorithm evaluation requirement for systems under French regulatory oversight; CRYPTREC (Japan) which operates an independent PQC algorithm approval process separate from NIST; eIDAS 2.0 implementing acts which impose PQC requirements on qualified trust service providers and European Digital Identity Wallet infrastructure; and 3GPP Release 18/19 which addresses PQC integration for 5G NR security architecture through study items and

emerging specifications. Summary treatment of these instruments appears in Appendix C. Organisations operating under any of these regimes should treat the applicable instrument as an input to Gate 3 architecture approval.

The regulatory intent is unambiguous: cryptographic infrastructure must be modernised, governed, and evidenced. Organisations that treat this as a technical refresh project, something to be managed by the security architecture team with a modest budget allocation, will be in breach of regulatory obligations that apply to them regardless of their awareness of those obligations.

2.1 The Three Failure Modes

Cryptographic transformation programmes fail in three characteristic ways, each rooted in a structural deficit:

- Scope failure: The programme is scoped as algorithm replacement. Key generation, entropy infrastructure, certificate lifecycle, protocol negotiation, and embedded device credentials are treated as separate workstreams or deferred entirely. The result is partial migration, which is not migration at all.
- Governance failure: The programme lacks a gated decision structure. Phases begin before prior phases are closed. Architecture decisions are made without formal sign-off. Vendor dependencies are introduced without supply chain assessment. The programme drifts.
- Evidence failure: The programme cannot prove what it has done. Audit requests produce documentation that describes intent, not execution. Regulators ask for evidence of cryptographic control; they receive policy documents. The gap between claimed posture and provable posture is the residual risk.

F A I L U R E | 0 3

These are not edge cases. They are the modal outcome of cryptographic transformation programmes that are treated as technical projects rather than governed programmes. The SITG model is designed to prevent all three.

2.2 The Harvest Now, Decrypt Later Imperative

Nation-state adversaries are not waiting for quantum computers to become commercially available before acting. The Harvest Now, Decrypt Later (HNDL) strategy, capturing encrypted traffic today for retrospective decryption when cryptographically relevant quantum capability matures, is active. Data encrypted today with RSA or ECDH is being archived by adversaries who intend to decrypt it within the next decade. Multiple national intelligence agencies have publicly acknowledged the threat, and NIST's post-quantum standardisation timeline, with ML-KEM, ML-DSA, and SLH-DSA finalised in 2024 and a federal migration deadline of 2035, reflects the assessment that the window for safe transition is narrowing, not widening.

For any data with a confidentiality requirement extending beyond five years, government communications, financial records, healthcare data, strategic intellectual property, critical infrastructure credentials – the threat window is already open. In financial services, transaction

records, correspondent banking credentials, and SWIFT messaging keys carry confidentiality obligations measured in decades. In defence and government, classified material and diplomatic communications remain sensitive for 25 years or more. In healthcare, patient records carry statutory protection periods of up to 50 years in some jurisdictions. In telecommunications, lawful intercept credentials and subscriber authentication keys are high-value HNDL targets. These are not future risks. They are present-day collection targets whose decryption is deferred, not prevented, by current cryptographic protection. Transformation cannot wait for regulatory compulsion. It is already overdue.

2.3 Sovereignty and Regulatory Complexity

Cryptographic transformation in regulated sectors is not a single-jurisdiction exercise. Financial entities operating under DORA must simultaneously satisfy NIS2 requirements, national competent authority expectations, and, where relevant, US SEC cybersecurity disclosure obligations. Telecommunications operators must navigate ETSI standards, 3GPP security specifications, and national sovereign encryption requirements that may conflict with international interoperability standards.

The SITG model builds sovereign and regulatory alignment into the programme structure, not as a compliance checkbox appended at the end, but as a design constraint that shapes architecture, vendor selection, and evidence artefact production from the outset.

3. The SITG-Consulting Cryptographic Transformation Implementation Model

The SITG-Consulting Cryptographic Transformation Implementation Model is a six-level programme architecture that spans the full lifecycle of cryptographic transformation, from executive mandate to operational assurance. Each level is distinct in its audience, function, and evidence requirements. Each level feeds the next. None can be skipped.

S T R U C T U R E | 0 4

This is not a waterfall model dressed in agile language. It is a gated, wave-based programme where each gate requires verified evidence before progression is permitted. No gate is advisory. All gates are mandatory.

3.1 What Makes This Model Distinct

Three structural features differentiate the SITG model from every other cryptographic transformation approach currently available:

1. It is gated, not phased. Phases can coexist. Gates cannot be bypassed. The distinction matters because governance failures in conventional programmes almost always originate from phase-based thinking, where the organisation moves into the next phase before the prior phase has produced validated outputs. Gates enforce the evidence requirement.
2. It separates execution from operation. Level 3 delivers the transformed state. Levels 4 and 5 operate and prove it. Most programmes conflate delivery and operation, which means that when the delivery team demobilises, the operational capability has not been established. The SITG model requires the operating model to be built and tested before the delivery programme closes.
3. It produces evidence as output, not documentation as afterthought. The eight evidence artefacts defined in Level 5 are programme deliverables. They are not produced for audit consumption. They are produced because the programme cannot demonstrate control without them.

4. Level 0 - The Executive Board View

The transformation begins and ends at board level. Boards are not required to understand cryptography. They are required to hold funding authority, organisational change authority, and accountability, and those are only held at executive level. A programme without board mandate will be descoped at the first budget cycle, deprioritised at the first competing initiative, and abandoned at the first technical setback.

Level 0 defines the strategic shape of the programme in terms boards can mandate, fund, and govern. It operates across four strategic phases that map directly to the 36-month delivery arc.

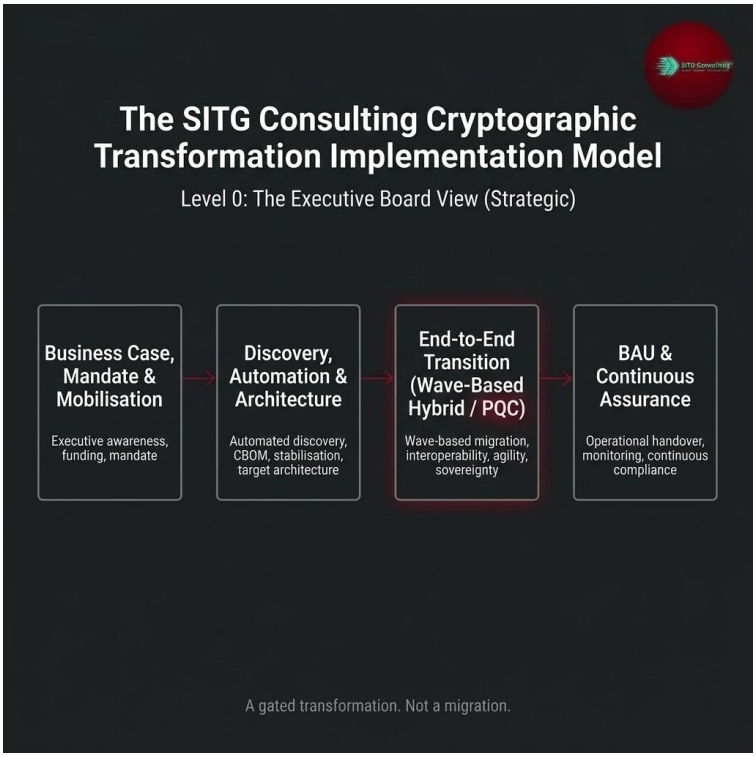

Figure 1: Level 0 - The Executive Board View - *Four strategic phases, each representing a board-level commitment. Execution is gated. Not linear.*

4.0 Tiered Entry: Where the Organisation Starts

Not every organisation enters this programme from the same starting position. Some are in current regulatory breach and must remediate before they can plan. Some have a validated CBOM but no architecture. Some are already mid-transition and need to assess where they are before they continue. Some are starting from zero with no active hard deadlines. The first board-level decision is not whether to run the programme. It is which tier the organisation is entering through. The tier determines the compression of the early phases, the evidence required at Gate 1, and the sequencing of the governance gates.

Tier 1 – Current Regulatory Breach. The organisation has passed one or more regulatory deadlines without completing the required action. Examples as of April 2026 include US national security supply chain organisations that did not meet the CNSA 2.0 software and firmware date of

January 2025; federal agencies that have not submitted compliant inventories under OMB M-23-02; EU financial entities that are not DORA-aligned following full application in January 2025; NIS2-scoped entities in jurisdictions where member state transposition has occurred. Tier 1 does not relax the binary gate principle. Gate 1 still passes before any programme workstream begins. What changes is compression: the Gate 1 evidence pack is built to the minimum viable form (target 45 days rather than the standard 90) because the business case is built around an existing breach condition rather than a future risk. The mandate, funding envelope, governance structure, and regulatory obligation map are all still Gate 1 deliverables. Emergency regulatory notification obligations, where triggered by the existing breach condition, are legal obligations the organisation owes regardless of the programme and are not programme workstreams. Regulatory notification assessment is itself a Gate 1 deliverable and must be completed before Gate 1 closes. Depending on sector and jurisdiction, self-reporting obligations may need to be discharged in parallel with Gate 1 evidence preparation under the organisation's existing legal and compliance function, not under the transformation programme.

Tier 2 – Inventory Complete, Architecture Pending. The organisation has a validated CBOM and may have passed Gate 2 in a prior programme cycle, but has not defined the target architecture, not approved the hybrid strategy, not completed vendor supply chain assessment, and has no sanctioned migration plan. Tier 2 organisations enter at Gate 3 with a catch-up protocol. The existing CBOM must be re-validated against current regulatory scope (Gate 2 reversion) before Gate 3 begins. The early phases compress: the Control phase runs compressed timelines but must still produce the full Gate 3 and Gate 4 evidence set.

Tier 3 – Mid-Transition. The organisation is already executing migration waves under a prior governance structure that does not meet the standard required here. Tier 3 organisations enter with a formal programme assessment and re-baselining step. The existing wave progress is mapped against the model’s gate structure. Gaps are documented. Evidence produced under the prior structure is assessed for acceptability. A revised programme plan is issued before further waves execute. Tier 3 is not a shortcut: the re-baselining step can take three to six months for large estates, but it prevents the compounding risk of continuing to execute waves against an inadequate governance structure.

Tier 4 – Standard Entry. The organisation is not in active regulatory breach, has no prior programme work to re-baseline, and is beginning from a standing start. Tier 4 is the path for which the standard illustrative arc in Section 9 was designed. It remains the least common entry point for the current market: most organisations subject to regulated cryptographic obligations have either passed deadlines, begun prior work, or both. Tier 4 organisations should still not assume 36 months is their number. The DURATION guidance in the Executive Summary applies equally to Tier 4: duration depends on estate scale, jurisdictional complexity, and organisational change capacity.

Tier selection is a board decision, made at Gate 1, documented as a formal entry determination, and revisited only if a Gate reversion event invalidates the original tier assignment (for example, a newly discovered asset category that places a Tier 4 organisation into Tier 1 under CNSA 2.0). The tier does not change the six-level model, the six gates, or the evidence standards. It changes the sequencing, compression, and parallelism of the early phases.

4.1 Phase 1: Business Case, Mandate & Mobilisation

The programme does not begin with discovery. It begins with mandate. This distinction is operationally critical. Discovery without mandate produces findings that have no institutional authority. Architecture without mandate produces recommendations that are overridden by operational priorities. The business case must precede all technical activity.

The mandate establishes: the regulatory and risk basis for transformation, the executive accountabilities, the funding envelope, and the programme governance structure. Without these four elements in place, no downstream phase has the authority it needs to execute.

4.2 Phase 2: Discovery, Automation & Architecture

With mandate in place, automated discovery of the cryptographic estate begins. This is not a manual audit. Manual audits of cryptographic infrastructure are episodically useful and structurally inadequate. The cryptographic estate – certificates, keys, algorithms, protocols, embedded credentials, Public Key Infrastructure (PKI) hierarchies, Key Management System (KMS) configurations – is too large, too distributed, and too dynamic for point-in-time manual discovery to produce a reliable baseline.

Automated discovery produces the Cryptographic Bill of Materials (CBOM), the machine-readable inventory of all cryptographic material, its location, its algorithm, its key size, its expiry, and its owner. The CBOM is the single source of truth for all subsequent risk prioritisation, architecture decisions, and migration wave planning.

4.3 Phase 3: End-to-End Transition (Wave-Based Hybrid/PQC)

Transition execution is wave-based, not monolithic. The first wave addresses the highest-risk assets, those with the longest data shelf life, the broadest exposure, and the weakest current cryptographic posture. Subsequent waves address lower-risk domains in order of priority established by the risk assessment.

Hybrid cryptography, the parallel operation of classical and Post-Quantum Cryptographic (PQC) algorithms during transition, is not a temporary compromise. It is a deliberate risk management strategy that maintains backward compatibility while establishing quantum-resistant protection on the highest-priority traffic. The transition does not flip to pure PQC until interoperability testing, regulatory alignment, and sovereign compliance requirements are all satisfied.

4.4 Phase 4: BAU & Continuous Assurance

The transformation programme does not end with migration. It ends when the organisation can demonstrably operate, monitor, and continuously assure its cryptographic infrastructure as a managed capability, not as a project. BAU transition is a formal gate. It requires the operating model to be established, the monitoring capability to be live, and the evidence artefact regime to be in continuous production.

A gated transformation. Not a migration. This distinction is operational. A migration has a start and an end. A transformation has a steady state, a continuously operated and evidenced cryptographic capability that the organisation sustains indefinitely.

5. Level 1 - The Programme View (Tactical)

Level 1 translates the board's strategic mandate into a structured programme with four execution phases, each with defined scope, outputs, and gate requirements. This is the level at which programme managers, transformation executives, and senior technical leads operate. It is the level that converts executive intent into accountable delivery.

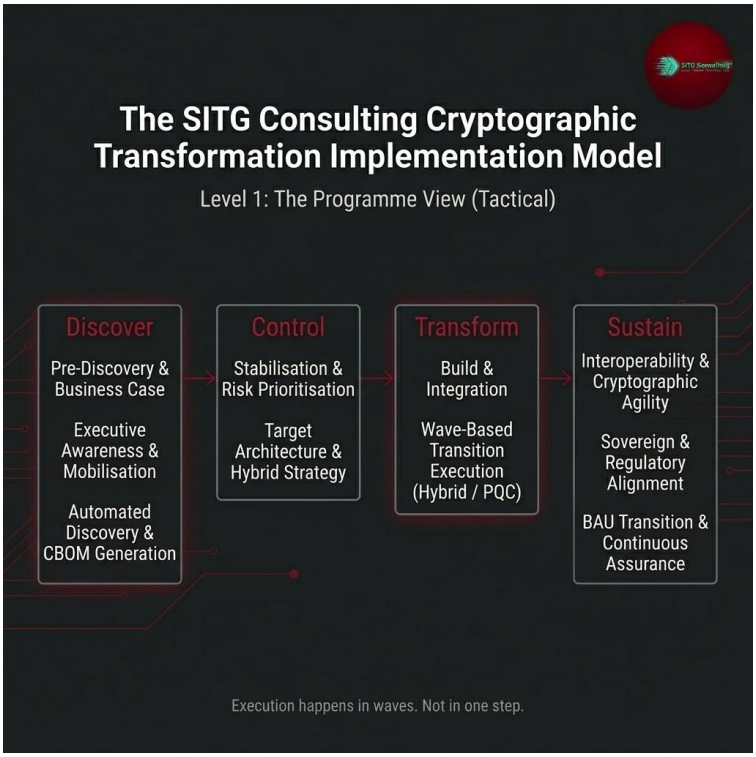

Figure 2: Level 1 - The Programme View - *Four execution phases: Discover, Control, Transform, Sustain. Execution happens in waves. Not in one step.*

5.1 Discover

The Discover phase has three components that must be completed in sequence before Control begins:

- Pre-Discovery & Business Case: The Cryptographic Bill of Materials (CBOM) scope is defined. The business case baseline is established. Regulatory obligations are mapped. The board mandate is documented.
- Executive Awareness & Mobilisation: Executive stakeholders are briefed. Accountability structures are established. Programme governance is constituted. This establishes the decision-making architecture on which all subsequent governance depends.
- Automated Discovery & CBOM Generation: The cryptographic estate is discovered through automated tooling. The CBOM is generated, validated, and published as the authoritative inventory. Manual sampling validates automated outputs.

5.2 Control

Control is the most underestimated phase in cryptographic transformation programmes. It is tempting to accelerate through control and into transition, the transition deliverables are visible, tangible, and auditable. Control is not. But without control, transition has no validated starting point and no defensible architecture.

- Stabilisation & Risk Prioritisation: The CBOM is analysed against the risk model. Assets are classified by sensitivity, longevity, exposure, and migration complexity. Waves are sequenced. The highest-risk assets are identified for first-wave treatment.
- Target Architecture & Hybrid Strategy: The target cryptographic architecture is defined. Algorithm selections are made. The hybrid operation strategy is documented. The Operating Model (Level 4) is designed. Vendor and supply chain requirements are established.

5.3 Transform

Transform is where the architecture becomes reality. Two workstreams run in parallel:

- Build & Integration: PKI hierarchies are rebuilt for PQC. KMS configurations are updated. Hardware Security Modules (HSMs) are reconfigured or replaced. Continuous Integration/Continuous Deployment (CI/CD) pipelines are modified to enforce cryptographic policy. Certificate lifecycle automation is deployed.
- Wave-Based Transition Execution (Hybrid/PQC): Migration waves execute against the prioritised asset list. Each wave has defined success criteria, rollback procedures, and evidence requirements. No wave progresses to production without interoperability testing and formal sign-off.

5.4 Sustain

Sustain is the transition from programme to operation. It has three components that must all be operational before the programme closes:

- Interoperability & Cryptographic Agility: Interoperability is validated across all protocol layers, vendor integrations, and cross-domain connections. Cryptographic agility, the ability to swap algorithms rapidly in response to vulnerabilities or standards changes, is designed in, tested, and documented.
- Sovereign & Regulatory Alignment: All deployed cryptographic configurations are validated against applicable sovereign and regulatory requirements. Where conflicts exist between interoperability requirements and sovereign obligations, resolution strategies are documented and formally approved.
- BAU Transition & Continuous Assurance: The operating model is handed over to the operational team. Monitoring is live. Evidence production is continuous. The programme governance structure is replaced by the ongoing operational governance structure.

EXECUTION | 06

Execution happens in waves. Not in one step. The wave structure is not a concession to complexity. It is the risk management mechanism. Early waves validate assumptions. Later waves benefit from what early waves learned.

6. Level 2 - Governance Gates

The governance gate structure is the mechanism by which the SITG model prevents the programme drift, scope compression, and evidence failure that characterise failed cryptographic transformation programmes. Six gates span the programme lifecycle. Each gate requires validated evidence before the programme may proceed. Each gate is a formal SteerCo decision point. No gate is advisory.

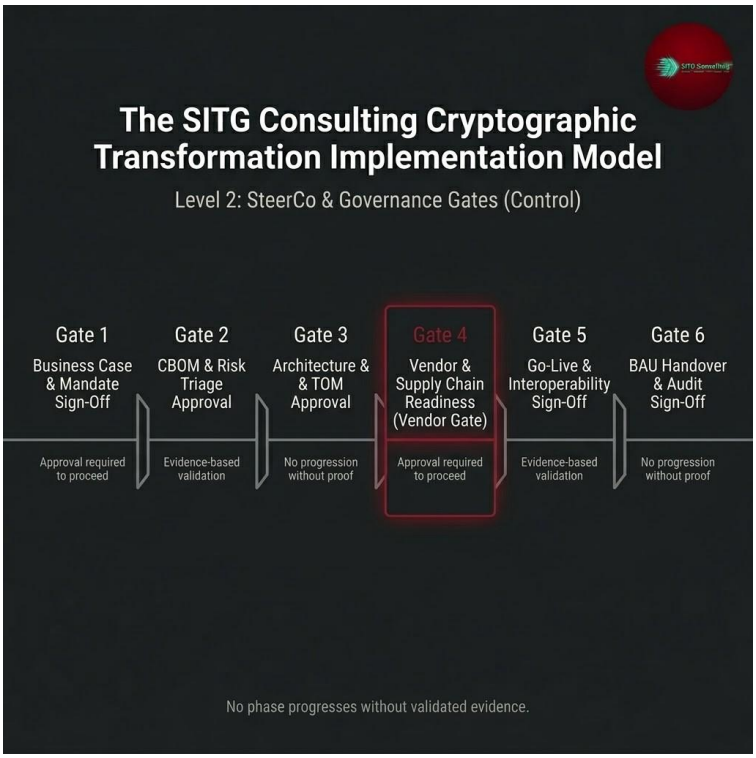

Figure 3: Level 2 - Governance Gates - *Six mandatory gates. No phase progresses without validated evidence. Gate 4 (Vendor & Supply Chain) is highlighted as the most commonly failed gate in practice.*

Gate	Requirements to Pass
Gate 1: Business Case & Mandate Sign-Off	Documented business case with quantified risk exposure. Board-approved mandate. Funding authorisation. Programme governance constituted. Without these four artefacts, no work proceeds.
Gate 2: CBOM & Risk Triage Approval	Complete CBOM validated against sampling audit. Risk classification applied. Wave sequence proposed and agreed. Evidence basis confirmed. Approval is evidence-based - the CBOM must be complete, not indicative.
Gate 3: Architecture & TOM Approval	Target architecture documented and formally approved. Target Operating Model (TOM) designed. Vendor selection framework established. Hybrid strategy approved. No build activity commences without Gate 3 approval.
Gate 4: Vendor & Supply Chain Readiness	All critical vendors assessed for cryptographic supply chain integrity. PQC-capable vendor certifications verified. Contractual obligations for cryptographic assurance confirmed. This gate is the most commonly failed in practice - and the most consequential.

Gate 5: Go-Live & Interoperability Sign-Off	Interoperability testing complete across all integration points. Wave transition validated in staging environment. Rollback procedures tested and approved. No production transition without Gate 5 sign-off.
Gate 6: BAU Handover & Audit Sign-Off	Operating model operational and evidenced. Monitoring live. All evidence artefacts produced and audit-ready. Regulatory reporting obligations confirmed as met. Programme formally closed.

Gate Deliverables Summary

Each gate closes against a defined set of deliverables. A gate is not passed on the basis of activity descriptions or intent statements. It is passed on the basis of these deliverables being present, validated, and approved.

Gate 1 deliverables: board-approved business case with quantified risk exposure; executive mandate document with named accountabilities; funding authorisation for the programme envelope; programme governance structure (SteerCo terms of reference, escalation paths, reporting cadence); regulatory obligation map applicable to the organisation; tier entry determination (Tier 1 through Tier 4) with supporting rationale.

Gate 2 deliverables: validated CBOM with confidence tier distribution documented per Section 7.1; independent sampling audit report; risk classification applied across the five-dimension scoring model; vendor-constrained asset register (extracted from standard scoring flow); wave sequence proposal with supporting risk rationale; jurisdiction tagging applied to all in-scope assets where multi-jurisdictional operations are confirmed; SteerCo acceptance of residual risk in Low and Attestation-only confidence tiers.

Gate 3 deliverables: target cryptographic architecture document with algorithm selections and supporting justification; Target Operating Model specification; hybrid strategy with classical-to-PQC transition rules; jurisdiction-differentiated requirements matrix where applicable, including dual-stack architecture specification where OSCCA or equivalent regimes are in scope; vendor selection criteria and assessment framework; cryptographic agility design with tested algorithm swap procedure; regulatory mapping confirmation signed by legal, regulatory, and technical stakeholders.

Gate 4 deliverables: vendor assessment report for each critical supplier, including cryptographic supply chain documentation; PQC-capable vendor certifications verified against published NIST or equivalent validation lists; contractual obligations for cryptographic assurance executed, with specific algorithm support timescales and remediation terms; vendor constraint register with mitigation plans for vendor-blocked assets; supply chain integrity statement; residual vendor risk register.

Gate 5 deliverables: interoperability test reports covering all integration points for the wave in scope; staging environment validation evidence; tested rollback procedure with execution record; wave-specific pre-migration and post-migration CBOM state; sovereign and regulatory alignment confirmation for the jurisdictions in scope; operational readiness confirmation from the receiving operational teams; classical cryptographic material decommissioning evidence for the assets in wave scope (key zeroisation records, certificate revocation confirmations, HSM slot destruction attestations as applicable); go-live authorisation from the SteerCo.

Gate 6 deliverables: operating model handover record with all six operational functions confirmed as live; monitoring and telemetry validation; all eight evidence artefact categories in continuous production; Cryptographic Risk Committee terms of reference adopted; regulatory

reporting obligations confirmed as met; audit-ready evidence package; formal programme closure authorisation; gate reversion machinery operational per Section 12.3.

Gates are binary. A gate is either passed on the evidence or it is not passed. “Close enough” is not a category. “Under pressure” is not a category. Programme momentum, executive commitment, vendor relationships, and budget cycle optics are not permitted inputs to gate decisions. Any override of a gate hold is itself a governance failure and must be logged, escalated to the standing risk committee, and treated as a programme risk for the duration of the programme. The gate structure only functions if this discipline is held; once it is softened, the evidence-driven basis of the entire model collapses.

Each gate is also a decision point that creates a record of evidence accepted and judgements made at a specific moment in time. These records carry accountability consequences under multiple regulatory frameworks, including DORA, NIS2, sector-specific supervisory regimes, and jurisdiction-specific cryptographic obligations. Organisations should obtain qualified legal advice in their jurisdiction and sector on the accountability consequences of specific gate decisions. The handbook does not offer legal opinion on individual liability exposure at any gate.

6.1 Gate 4: The Vendor Gate - The Most Consequential Checkpoint

Gate 4 deserves specific treatment because it is the gate most frequently bypassed, and the one whose bypass has the most severe downstream consequences.

Cryptographic transformation is, in part, a supply chain exercise. The algorithms an organisation deploys are implemented in libraries, HSMs, network equipment, and embedded firmware that it procures from vendors. If those vendors have not validated their PQC implementations, have not assessed their own supply chain for cryptographic backdoors, and have not committed contractually to cryptographic agility on defined timescales, the organisation’s cryptographic posture depends on vendor behaviour it cannot control.

Gate 4 requires proof, not assurance, not commitment, that each critical vendor has been assessed, that their cryptographic supply chain is documented, and that contractual obligations for ongoing cryptographic assurance have been established. Organisations that accept vendor assurance letters in place of evidence at Gate 4 will encounter the consequences at Gate 6, when the audit finds the gaps.

The harder question is what happens when a critical vendor cannot pass Gate 4 and no alternative vendor exists. A core banking platform, a telecommunications network function vendor, a legacy OT supplier with no published PQC roadmap: these situations are common and Gate 4 as stated does not resolve them. Three outcomes are available and must be selected explicitly, documented at Gate 4, and recorded against the affected assets in the CBOM.

Outcome A: Replace. The vendor is replaced with an alternative that can pass Gate 4. This is the cleanest outcome where commercially and operationally feasible and is the default path for non-critical vendors.

Outcome B: Conditional pass with remediation plan. Where replacement is not feasible within the programme horizon, Gate 4 may pass conditionally for the affected vendor relationship. The conditional pass requires a documented vendor remediation plan signed by both parties with a committed date for full Gate 4 compliance, an explicit residual risk statement approved by the SteerCo, and a mandatory quarterly re-review cadence until resolved. A conditional pass is a

formal governance state, not an informal workaround. It is recorded in the Gate 4 evidence pack and disclosed in regulatory reporting where required.

Outcome C: Board escalation. Where the residual risk exceeds the SteerCo's delegated authority or where the vendor is systemically critical with no acceptable remediation plan, the matter escalates to the board for an accept-and-disclose decision. The board either accepts the risk with documented reasons and disclosure obligations discharged, or it directs that the affected business activity be scoped out of the cryptographically-secured estate, or it sanctions commercial action against the vendor. This is not a routine outcome and any board-level accept decision remains open to gate reversion under Section 6.2 if conditions change.

GOVERNANCE | 07

No phase progresses without validated evidence. This is the operating principle of the entire model. It is stated explicitly in the governance structure so that it cannot be negotiated away under programme pressure.

6.2 Gate Reversion: When a Passed Gate Must Be Reopened

Gates are not one-way doors. Over the life of a multi-year programme operating against an evolving regulatory, technical, and vendor landscape, events will occur that invalidate evidence accepted at a previously passed gate. A previously-approved architecture may be overtaken by a newly disclosed algorithm vulnerability. A vendor whose PQC roadmap was accepted at Gate 4 may abandon that roadmap or fail commercially. A regulatory instrument current at Gate 3 may be amended in ways that change its applicability. A newly issued national guidance may render a jurisdiction-specific architecture decision non-compliant. If the governance structure has no mechanism to reopen a previously-passed gate, these events degrade the programme silently rather than triggering a formal response.

Gate reversion is the formal reopening of a previously-passed gate following a triggering event. Three trigger categories apply:

- Category A (immediate): algorithm vulnerability disclosure affecting a deployed or approved algorithm; hard deadline change in a regulatory instrument in scope; new regulatory obligation taking effect that was not captured in the original gate evidence; vendor commercial failure affecting a critical supply chain dependency. Category A triggers require formal gate re-examination within five working days of detection.
- Category B (scheduled): new algorithm approvals or standards publications that do not invalidate existing choices but change the available design space; updated sector guidance that affects architecture decisions; vendor roadmap changes that remain within the commitment envelope but alter delivery sequencing. Category B triggers require formal architecture review within 30 days of identification.
- Category C (logged): theoretical vulnerabilities under academic discussion; early-stage legislative proposals; roadmap announcements from standards bodies. Category C triggers are logged, tracked, and reviewed at the next scheduled programme governance cycle.

Gate reversion is a structural part of the model, not an exception to it. The operational machinery that drives it – source monitoring, change classification, gate condition versioning, and escalation

– is set out in Section 12. During the programme phase, gate reversion authority sits with the SteerCo. During BAU, it transfers to the Cryptographic Risk Committee.

7. Level 3 - Engineering & Operational Execution

Note: From this section onwards, the handbook shifts from executive and programme-level guidance to technical and operational detail. The intended audience for Sections 7–12 is security architects, cryptographic engineers, PKI specialists, and operational leads. Executive readers may wish to proceed directly to Section 13 for the concluding argument.

Level 3 is where the programme delivers. It operates across six engineering workstreams that run concurrently during the Transform phase, coordinated through the programme governance structure, and sequenced by the wave execution plan. This level is addressed to the security architects, cryptographic engineers, PKI specialists, DevSecOps leads, and operational teams who do the work.

Level 3 is not a technical specification. It is an execution model. It defines what must be delivered, in what sequence, with what evidence, across each workstream. The specific technical choices, algorithm selections, library versions, HSM configurations, are made within this structure, not around it.

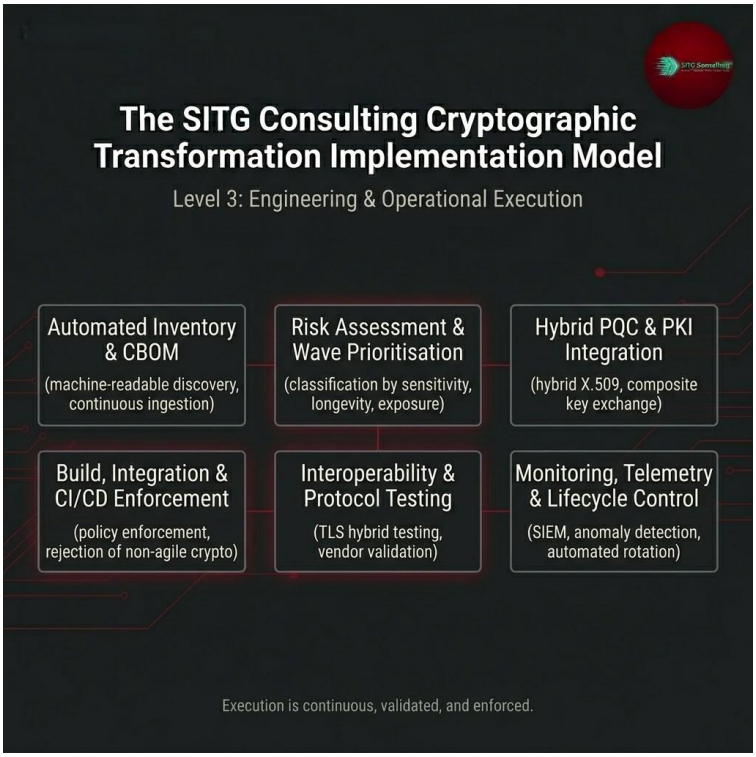

Figure 4: Level 3 - Engineering & Operational Execution - *Six concurrent workstreams. Execution is continuous, validated, and enforced. Not sequential.*

7.1 Automated Inventory & CBOM

At Level 3 the CBOM is a live operational feed. Automated scanning continuously ingests new cryptographic assets as the estate changes, new certificates issued, new services deployed, new

keys generated. The CBOM is the authoritative basis for migration planning, transition tracking, and regression detection across every wave.

The technical requirement is machine-readable discovery with continuous ingestion, not periodic scanning. Cryptographic estates change continuously. A CBOM that is refreshed quarterly is a historical record, not an operational control.

Completeness is not a binary property of the CBOM. Automated discovery has a structural ceiling: network-visible PKI assets and certificate infrastructure are reliably discoverable, while firmware in embedded devices, operational technology with proprietary cryptographic implementations, acquired subsidiary estates, and third-party SaaS environments are opaque to standard scanning. Treating the CBOM as either complete or incomplete understates the residual risk in the opaque categories. The CBOM must therefore carry a confidence tier against each asset category as a deliverable property, approved at Gate 2. The four tiers are:

- **High confidence.** Assets directly discoverable through network scanning, certificate transparency logs, or PKI management systems. Independent sampling validation is required at Gate 2 and should produce no material discrepancies.
- **Medium confidence.** Assets discoverable through software composition analysis, SBOM ingestion, or application-level integration. Coverage is a function of the SBOM discipline of the development pipeline and may be incomplete for legacy components.
- **Low confidence.** Assets in firmware, embedded devices, operational technology, and legacy middleware where discovery requires targeted binary analysis or vendor cooperation. Coverage is partial by definition. Known gaps must be explicitly documented rather than silently omitted.
- **Attestation-only.** Assets in third-party SaaS, managed cloud services, and opaque supplier environments where the organisation has no direct visibility and relies on vendor attestation. Attestation-only assets carry a distinct risk profile and must be tracked with defined re-attestation cycles.

The handbook does not prescribe the tools, techniques, or discovery methods used to produce the CBOM. The confidence tier is a property the delivered CBOM must carry. How the delivery team reaches the required coverage is their own engineering decision. Gate 2 pass requires that the confidence tier distribution is documented, that known-unknown categories are explicitly declared, and that the proportion of assets in Low and Attestation-only tiers is approved as acceptable residual risk by the SteerCo.

Acceptance at Gate 2 requires more than the tier distribution itself. The organisation must define and document numeric thresholds for each tier in its Gate 2 deliverable package. The handbook does not prescribe the specific numbers; those are an organisational decision justified against risk appetite documented at Gate 1. As a practical benchmark, an organisation pressed to name a target for the High confidence tier would typically aim for ninety-five per cent discoverable coverage of network-visible assets, with the remaining asset categories distributed across Medium, Low, and Attestation-only according to the inherent discoverability of each category. The benchmark is illustrative, not mandatory. What is mandatory is that thresholds exist, are numeric, are approved at Gate 2, and are enforceable at re-examination. The SteerCo's acceptance of Low and Attestation-only proportions must be supported by a documented residual risk assessment including estimated asset counts in each tier, justification for non-discovery, and a remediation plan with timeline to improve the confidence distribution over the programme lifetime and into BAU. The remediation plan is tracked as a continuous assurance obligation and is reviewed by the Cryptographic Risk Committee on a defined cadence after BAU transition. A

CBOM that passes Gate 2 without an accompanying improvement plan for its Low and Attestation-only proportions is not complete.

7.2 Risk Assessment & Wave Prioritisation

Wave prioritisation is not a ranking exercise. It is a risk management decision that must be formally documented and approved. Before the scoring model is applied, vendor-constrained assets are extracted from the standard flow: assets whose migration is gated by a vendor's PQC roadmap or hardware availability timeline are not scored against the other assets, because their sequencing is determined by factors outside the risk model. These assets are managed through the Gate 4 residual risk protocol and re-entered into the wave plan when the vendor constraint clears. Assets that remain in the standard flow are classified against five dimensions:

- Sensitivity: the classification and regulatory obligation of the data the cryptographic material protects.
- Longevity: the required confidentiality period of the data, which determines the HNDL exposure window.
- Exposure: the attack surface of the asset, network-facing services have higher exposure than air-gapped systems.
- Business criticality: the operational impact of service disruption to the dependent business process, weighted by recovery time objective. An asset with moderate sensitivity that supports a customer-facing authentication service carries materially higher business criticality than an asset of equivalent sensitivity supporting a cold-storage archive. Business criticality prevents the risk model from recommending wave sequences that are technically defensible and operationally untenable.
- Regulatory visibility: the degree to which the asset is under active supervisory scrutiny, subject to imminent audit, or named in recent regulatory guidance. Assets under active examination are elevated above their baseline risk score because the cost of non-compliance is concentrated rather than diffuse.

The intersection of these five dimensions produces the wave priority score. The weighting applied to each dimension is a deliberate organisational choice and must be justified against the risk appetite documented at Gate 1. The scoring methodology must be documented and approved at Gate 2. It cannot be revised during execution without formal change control because wave priority changes affect the risk profile of all assets not yet migrated. Where a Tier 1 organisation operates under a hard statutory deadline such as CNSA 2.0, the deadline category overrides the standard scoring output: assets in scope of the deadline are sequenced to meet the statutory date regardless of where they would otherwise fall in the risk-scored order. This override is itself a Gate 1 decision, not an in-flight reclassification.

7.3 Hybrid PQC & PKI Integration

PKI integration is the most architecturally complex workstream in the programme. The certificate hierarchy must be rebuilt to support hybrid X.509 certificates, certificates that carry both classical and post-quantum public keys, enabling verification by both legacy and PQC-capable relying parties during the transition period.

IETF drafts cited in this section are subject to change before final RFC publication. Implementers must verify current status at datatracker.ietf.org and should not treat draft specifications as stable

implementation targets. Composite key exchange, the simultaneous use of classical ECDH and ML-KEM in a combined key agreement, must be implemented at the Transport Layer Security (TLS) layer, the VPN layer, and any other protocol layer where key agreement occurs. Implementation should align with current IETF drafts, including draft-ietf-tls-hybrid-design and draft-ietf-pquip-hybrid-signature-spectrums (draft status as of April 2026). Hybrid X.509 certificate profiles should follow draft-ietf-lamps-pq-composite-sigs and related LAMPS working group outputs. All implementations must be tested against relying party implementations before production deployment.

7.4 Build, Integration & CI/CD Enforcement

Cryptographic policy enforcement at the CI/CD layer is non-negotiable in a programme that claims cryptographic agility. Software that uses non-agile cryptography, hardcoded algorithms, pinned library versions, vendor-specific APIs that cannot be swapped, is cryptographic liability manufactured by the development process.

CI/CD enforcement means that every build is checked for cryptographic policy compliance before it progresses to staging. Non-compliant builds are rejected. The policy is defined in machine-readable format that can be updated as standards evolve. The CI/CD gate is not advisory.

7.5 Interoperability & Protocol Testing

Interoperability testing is the validation layer between engineering delivery and production transition. For hybrid PQC deployments, interoperability testing must cover: TLS hybrid handshake across all supported client versions, cross-vendor certificate validation, protocol negotiation fallback behaviour, and performance impact at operational load.

Vendor validation, confirming that third-party implementations produce compatible outputs, must be completed before Gate 5 sign-off. Interoperability failures discovered in production cannot be patched without impacting service availability and triggering incident management obligations.

7.6 Monitoring, Telemetry & Lifecycle Control

The monitoring capability built at Level 3 is the foundation of the Level 4 operating model. It must be live and validated before the programme transitions to BAU. Monitoring covers: certificate expiry and renewal, algorithm compliance drift, key rotation events, anomalous cryptographic operations, and Security Information and Event Management (SIEM) integration for cryptographic incident detection.

Automated rotation, the systematic renewal of cryptographic material before expiry without manual intervention, is the operational baseline for a programme that claims continuous assurance. Manual certificate management at enterprise scale is not sustainable and is not a basis for regulatory compliance.

8. Level 4 & 5 - Operating Model & Evidence

The operating model (Level 4) and evidence regime (Level 5) are the terminal deliverables of the programme, and the criteria against which the programme is ultimately judged. An organisation that has completed technical migration but cannot operate the resulting state, and cannot prove that it has done so, has not completed the programme. It has completed a project and left the governance gap open.

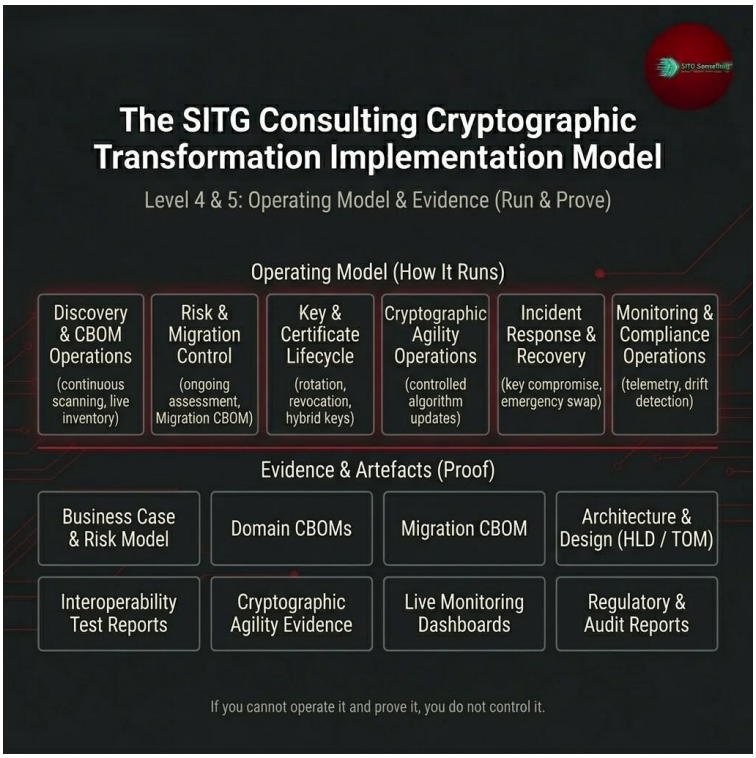

Figure 5: Level 4 & 5 - Operating Model & Evidence - *If you cannot operate it and prove it, you do not control it. Six operational functions. Eight evidence artefacts.*

8.1 The Operating Model (Level 4) - How It Runs

Six operational functions constitute the cryptographic operating model. These are not roles or departments. They are operational capabilities that must be staffed, tooled, and governed on a permanent basis:

E V I D E N C E | 0 8

Evidence is not documentation. Documentation describes what was planned. Evidence proves what was done, what the result was, and what the current state is. The distinction determines whether a programme survives regulatory scrutiny.

9. The Transformation Roadmap

This section presents an illustrative 36-month roadmap aligned to the implementation model levels. It is structured across four time horizons – Months 0–3, 3–9, 9–24, and 24–36 – corresponding to the four strategic phases of the Level 0 board view. The 36-month arc is one possible programme shape, not the default. It reflects Tier 4 entry (no active breach, clean baseline) for a mid-complexity single-jurisdiction estate. Real programmes vary from eighteen months to ten years depending on the factors set out in Section 4.0 (Tiered Entry). The roadmap is risk-driven and wave-based. It is not a Gantt chart. Phase durations shown here are indicative only; actual timelines are determined by the risk profile, estate scale, jurisdictional complexity, vendor readiness, and organisational change capacity of the specific organisation.

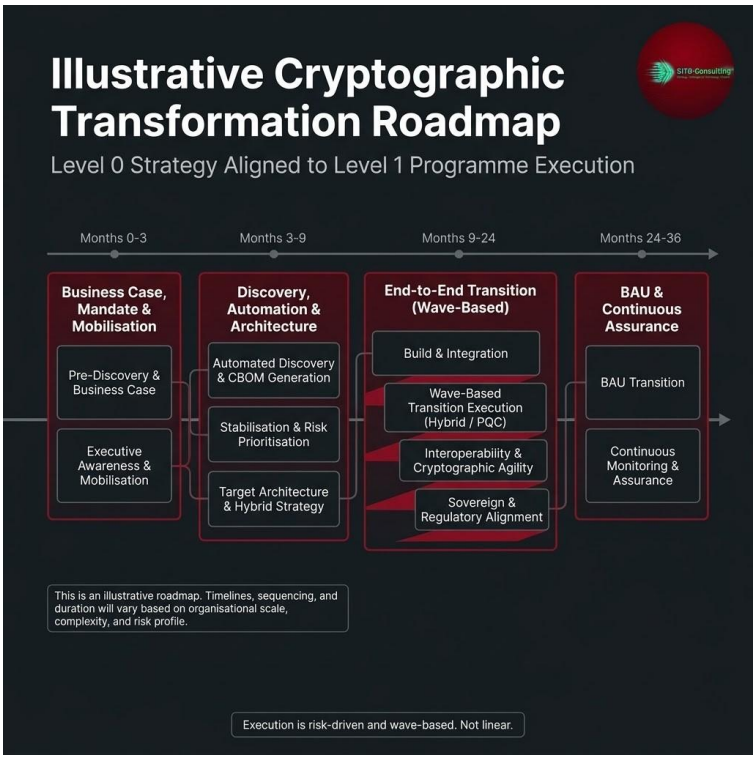

Figure 6: The 36-Month Transformation Roadmap - *Level 0 strategy aligned to Level 1 programme execution. Execution is risk-driven and wave-based. Not linear.*

9.1 Months 0–3: Business Case, Mandate & Mobilisation

The first 90 days are governance days, not engineering days. Two workstreams run in parallel:

- Pre-Discovery & Business Case: The cryptographic risk exposure is quantified against applicable regulatory obligations and threat timelines. The business case is structured for board consumption. The programme budget and governance model are defined.
- Executive Awareness & Mobilisation: The board and executive leadership team are briefed to the level required to discharge their accountability. Programme sponsorship is formally assigned. The SteerCo is constituted. Gate 1 is convened and passed.

The 90-day constraint on this phase is deliberate. Organisations that spend six months on mandate and mobilisation are typically experiencing governance dysfunction, competing priorities, unclear accountability, or inadequate executive sponsorship, that will recur throughout the programme if not resolved before discovery begins.

Phase 1 deliverables: board-approved business case; executive mandate with named accountabilities; funding authorisation for the programme envelope; SteerCo terms of reference and governance structure; regulatory obligation map; tier entry determination; Gate 1 pass record.

9.2 Months 3–9: Discovery, Automation & Architecture

Three workstreams define this phase:

- Automated Discovery & CBOM Generation: Tooling is deployed, the estate is scanned, and the CBOM is produced. Gate 2 (CBOM & Risk Triage Approval) is passed when the CBOM is validated and the risk classification is approved.
- Stabilisation & Risk Prioritisation: The risk model is applied to the CBOM. Wave sequence is defined. Assets requiring immediate attention, due to high exposure, long data shelf life, or regulatory urgency, are identified for expedited treatment.
- Target Architecture & Hybrid Strategy: The cryptographic target architecture is designed. The hybrid strategy is defined. The Target Operating Model is documented. Gate 3 (Architecture & TOM Approval) is passed. Gate 4 (Vendor & Supply Chain) is conducted and passed.

Phase 2 deliverables: validated CBOM with confidence tier distribution; independent sampling audit; five-dimension risk classification; vendor-constrained asset register; wave sequence proposal; jurisdiction tagging applied across the estate where multi-jurisdictional; target architecture document; Target Operating Model; hybrid strategy; vendor assessment reports with executed contractual obligations; Gate 2, Gate 3, and Gate 4 pass records.

9.3 Months 9–24: End-to-End Transition (Wave-Based)

The transition phase is the longest and most operationally intensive. Four workstreams execute concurrently:

- Build & Integration: PKI rebuild, KMS reconfiguration, HSM upgrade, and CI/CD enforcement are delivered. The infrastructure for PQC operation is in place.
- Wave-Based Transition Execution: Migration waves execute in priority order. First-wave assets are migrated to hybrid PQC. Subsequent waves follow at intervals determined by the wave execution plan. Gate 5 is passed for each wave before production transition.
- Interoperability & Cryptographic Agility: Interoperability validation runs continuously as each wave completes. Cryptographic agility capability is built, tested, and documented.
- Sovereign & Regulatory Alignment: Regulatory compliance validation runs in parallel with technical delivery. No wave transitions to production without sovereign and regulatory alignment confirmed.

Phase 3 deliverables: rebuilt PKI hierarchy supporting hybrid X.509; reconfigured KMS and HSM estate; CI/CD cryptographic policy enforcement in production; per-wave pre-migration and post-migration CBOM states; per-wave interoperability test reports; per-wave rollback execution records; cryptographic agility capability built and tested; per-wave sovereign and regulatory

alignment confirmations; per-wave Gate 5 pass records; updated Migration CBOM tracking cumulative transition state.

9.4 Months 24–36: BAU & Continuous Assurance

The final phase is the transition from programme to operation. Two workstreams close the programme and open the operating model:

- BAU Transition: The operating model is handed over. Operational teams are trained. Governance transitions from programme SteerCo to operational governance. Gate 6 (BAU Handover & Audit Sign-Off) is passed when all evidence artefacts are produced and the operating model is confirmed as live.
- Continuous Monitoring & Assurance: The monitoring capability is operating. CBOM is live. Compliance reporting is continuous. The programme is formally closed.

Phase 4 deliverables: operating model handover record with all six Level 4 functions confirmed live; Cryptographic Risk Committee terms of reference adopted; live monitoring dashboards operational; all eight Level 5 evidence artefact categories in continuous production; gate reversion machinery operational per Section 12.3; regulatory reporting obligations confirmed as met; audit-ready evidence package; Gate 6 pass record; formal programme closure authorisation.

10. Risk-Driven, Wave-Based Execution

Wave-based execution is the operating principle that resolves the apparent paradox of cryptographic transformation: the estate is too large to migrate simultaneously, but any partial migration creates a two-tier security posture that must be managed as risk, not ignored as process.

Waves are not sprints, iterations, or batches. They are structured migration events with defined scope, defined success criteria, defined rollback procedures, and defined evidence requirements. Each wave is approved at a governance gate before transition to production. Each wave produces evidence of its own execution. Each wave's lessons inform the planning of the next.

10.1 Wave Design Principles

- Risk-first sequencing: The first wave always addresses the highest-risk assets. This is not a pilot or proof-of-concept. It is the live migration of the most consequential material. Starting with low-risk assets to build confidence is programme management that serves the programme manager's comfort, not the organisation's risk profile. Vendor-constrained assets identified under Section 7.2 are excluded from the standard wave scoring and are managed under the Gate 4 residual risk protocol. They re-enter the wave plan when the vendor constraint clears, following the process set out in Section 7.2.
- Atomic execution where achievable: Each wave migrates a defined set of assets completely. Partial wave completion, assets left in transition state, creates operational and audit complexity that compounds across subsequent waves. Waves are designed to be completable within defined time windows. Atomicity is not universally achievable. Certain asset categories carry distributed cryptographic state that cannot be migrated in a single bounded event: database encryption hierarchies, distributed caching and session management, hardware-bound keys in HSMs and TPMs, and code-signing key populations in active CI/CD ecosystems. These non-atomic categories must be identified before wave scope is finalised and governed explicitly: the operational controls applied during the transition window, the maximum permissible duration of the non-atomic state, the monitoring in place to detect exploitation of the incomplete state, and the evidence produced at close must all be documented and approved as part of the wave plan. Non-atomic waves must have tested rollback procedures for their atomic sub-components and a separate documented governance track for the distributed state that cannot be rolled back, including compensating controls, containment procedures, and a defined point of no return beyond which forward recovery replaces rollback as the primary remediation mechanism. Non-atomic waves do not progress to production without this governance in place.
- Evidence at wave close: No wave is considered complete until its evidence package is produced. The evidence package includes the pre-migration CBOM state, the post-migration CBOM state, interoperability test results, and regulatory alignment confirmation.
- Rollback tested before transition: Rollback procedures are tested in staging before each wave transitions to production. The existence of a rollback procedure is not sufficient. Its operation must be validated.

Wave failure is a governance event, not a programme crisis.

Real programmes have waves that fail. The handbook treats wave failure as a defined state with three outcomes, each with its own governance response. State one: rollback successful. The wave is reverted to its pre-migration state, the CBOM is restored to the baseline, and the wave is

re-planned under Gate 5 re-examination before the next attempt. No gate reversion is triggered for prior gates. State two: rollback partial. Some assets are restored, others are left in an intermediate state that cannot be cleanly rolled back. This is managed under the non-atomic wave governance track defined in the atomic execution principle above: compensating controls, containment procedures, and a defined point of no return are invoked, and the incomplete state is documented as a known residual risk on the Migration CBOM. State three: rollback failed. The wave cannot be returned to its pre-migration state and the deployed change cannot be completed. This triggers immediate escalation to the Cryptographic Risk Committee and a mandatory Gate 3 re-examination, because a failure of this category indicates that the architecture approved at Gate 3 does not survive execution as designed. Wave failure classification is a SteerCo decision during the programme phase and a Cryptographic Risk Committee decision in BAU. A failed wave is never closed without a classified failure record and an agreed remediation path.

RISK | 09

The wave structure is the risk management mechanism, not the delivery mechanism. It exists to ensure that at no point does the organisation have a cryptographic posture it cannot describe, cannot defend, and cannot recover from.

10.2 Managing Hybrid Operation Risk

During wave-based transition, the organisation operates a hybrid cryptographic posture: some assets protected by PQC, others still running classical algorithms. This hybrid posture is unavoidable and must be managed as an explicit operational state, not as a temporary condition that receives reduced governance attention.

Hybrid operation risk has three components:

1. Downgrade attack surface: Protocol negotiation that permits fallback to classical algorithms creates an attack surface that adversaries can exploit to force weaker cryptographic protection. Hybrid operation must enforce minimum acceptable algorithm standards at the protocol layer, with classical algorithms permitted only where PQC interoperability cannot be confirmed.
2. CBOM currency: The boundary between PQC-migrated and not-yet-migrated assets must be tracked with precision throughout the hybrid operation period. An outdated CBOM during hybrid operation is a compliance risk. Regulators who ask for the current state of migration will receive an inaccurate answer.
3. Operational complexity: Operating two algorithm families simultaneously increases operational complexity. The monitoring capability must cover both. The incident response procedures must address both. The key lifecycle management must handle both.

11. Sovereignty, Interoperability, and Regulatory Alignment

Sovereign cryptographic requirements and international interoperability standards are in tension. That tension is not resolvable by choosing one over the other. It must be designed through.

11.1 The Sovereignty Constraint

Sovereign cryptographic requirements vary by jurisdiction and sector. Government and defence environments in multiple jurisdictions require nationally approved algorithms, nationally approved hardware, and, in some cases, nationally approved key management infrastructure. These requirements may prohibit or restrict the use of algorithms approved by other national standards bodies, including NIST, unless specific bilateral assurance arrangements are in place.

Telecommunications operators face a parallel set of constraints through 3GPP security specifications and national security obligations imposed by communications acts and national cybersecurity authorities. The introduction of PQC algorithms into 5G NR key derivation functions, SIM credential management, and network function authentication must satisfy both 3GPP standardisation requirements and national regulatory expectations that may not be synchronised with the 3GPP timeline.

11.2 The Interoperability Requirement

Interoperability is a commercial and operational necessity. An organisation that deploys PQC algorithms that its counterparties, customers, and suppliers cannot support has not improved its security. It has created an operational barrier. Interoperability testing must validate that hybrid PQC implementations work correctly across every integration point, not just the internal ones.

For financial services entities, this means validating PQC interoperability with correspondent banks, payment network infrastructure, and regulatory reporting systems. For telecommunications operators, it means validating interoperability with roaming partners, interconnect carriers, and emergency services infrastructure. For critical infrastructure operators, it means validating interoperability with operational technology vendors whose PQC support timelines may be significantly longer than IT system timelines.

11.3 Designing Through the Tension

The SITG model addresses the sovereignty-interoperability tension through five design principles:

1. Cryptographic agility as the resolution mechanism for implementation-layer divergence: An architecture that can switch algorithms without service disruption can satisfy different sovereign requirements in different contexts without requiring multiple parallel cryptographic estates, provided the divergence sits at the implementation layer. Agility does not eliminate the tension. It makes it manageable. Agility does not resolve national-approval-layer divergence: where a jurisdiction mandates algorithms that are not on the NIST-approved list and will not accept NIST algorithms regardless of implementation,

agility has nothing to swap between. This case is addressed by the dual-stack pattern below.

2. Regulatory mapping as a design input: Sovereign and regulatory requirements are mapped at Gate 3, not discovered at Gate 6. Architecture decisions are made with regulatory constraints in scope. The Target Architecture document is approved by legal, regulatory, and technical stakeholders simultaneously.
3. Contractual obligations on vendors: Vendors whose products are in scope for PQC migration must commit contractually to algorithm support timescales, interoperability testing participation, and cryptographic supply chain transparency. This is Gate 4. Vendors who cannot make these commitments are not compliant with the programme requirements.
4. Sovereign alignment validation per wave: Each wave's regulatory alignment confirmation includes sovereign compliance validation for the jurisdictions applicable to the assets in scope. This is not a single programme-level exercise. It recurs for each wave because the regulatory landscape is evolving during the programme execution period.
5. Dual-stack architecture for structurally incompatible jurisdictions: Where a jurisdiction mandates a nationally approved cryptographic stack that is incompatible with the NIST-aligned baseline at the algorithm level rather than the parameter level, the organisation operates parallel cryptographic estates. The canonical case is China: OSCCA requires SM2, SM3, and SM4 for domestic regulated applications, and these algorithms are not substitutable with NIST PQC regardless of agility architecture. The dual-stack pattern maintains a NIST-aligned estate for non-Chinese jurisdictions and a separate SM-family estate for Chinese domestic regulated applications. Each stack carries its own CBOM, its own target architecture, its own gate evidence, and its own operating model. The two stacks are governed as separate programmes under a single board mandate. The operational specifics of building and running the SM-family stack are out of scope for this handbook: organisations in this position should engage specialists with demonstrated delivery experience in the Chinese regulatory environment. The dual-stack pattern is named here because the alternative, attempting to force a single architecture across incompatible jurisdictions, produces a programme that satisfies neither regulator and stalls at Gate 3.

S O V E R E I G N T Y | 1 0

Sovereignty is not a compliance checkbox. It is an architectural constraint that shapes algorithm selection, hardware procurement, key management architecture, and the contractual structure of every vendor relationship in the programme.

---

12. Continuous Assurance & BAU Integration

Continuous assurance is the operational state in which the organisation can demonstrate, at any point, without advance notice, that its cryptographic infrastructure is operating as designed, that its posture matches its policy, and that its evidence artefacts are current and audit-ready.

This is a regulatory expectation, explicit in DORA, NIS2, and NIST SP 800-53, and implicit in every other framework that imposes continuous monitoring requirements on critical systems. Continuous assurance is the required state. The requirement is to build and sustain it.

12.1 The Four Pillars of Continuous Assurance

- Live inventory (CBOM currency): The cryptographic inventory must reflect the current state of the estate, updated continuously as changes occur. A CBOM that is weeks or months old is not evidence of continuous assurance. It is evidence of periodic snapshots.
- Automated lifecycle management: Certificate rotation, key renewal, and credential refresh must be automated. Manual lifecycle management at enterprise scale produces the gaps, expired certificates, rotated keys without record, missed renewal events, that create both operational incidents and audit findings.
- Real-time monitoring and drift detection: Cryptographic configuration drift, the divergence of deployed configurations from approved policy due to change activity, vendor updates, or operational workarounds, is the primary source of compliance degradation in mature programmes. Real-time drift detection catches it. Periodic audits do not.
- Continuous evidence production: Regulatory and audit reports must be producible on demand, not assembled in response to audit notification. The evidence artefact regime must be part of normal operations, not a mobilisation response.

12.2 BAU Governance: From Programme to Operation

The programme SteerCo is a temporary governance structure. BAU requires a permanent governance structure that maintains accountability for the cryptographic operating model on an ongoing basis. The BAU governance model includes:

- Cryptographic Risk Committee: A standing committee with executive membership that reviews the cryptographic risk posture on a defined cycle, approves algorithm changes, and has authority to direct remediation activity.
- Operational performance reporting: Regular reporting to the CIO/CISO on CBOM currency, certificate lifecycle health, incident statistics, and compliance posture. This reporting must be substantive, based on operational telemetry, not self-assessment.
- Annual assurance review: An annual review of the cryptographic operating model against current regulatory requirements, current threat intelligence, and current algorithm standards. The PQC landscape will continue to evolve, new algorithm guidance, new vulnerability findings, new regulatory expectations, and the operating model must evolve with it.

12.3 Gate Reversion Monitoring and Re-examination Machinery

Section 6.2 establishes the principle that a passed gate may be reopened when subsequent events invalidate its evidence basis. This section defines the operating machinery that detects those events, classifies them, and initiates formal re-examination. Without this machinery the gate reversion principle degrades to advisory guidance. Gate reversion is an operating function of the Cryptographic Risk Committee and is performed continuously through the programme execution period and into BAU.

Source monitoring operates on defined cadences against the regulatory and technical sources that feed each gate. Cadences are calibrated to the rate of change of the source, not set uniformly. NIST CSRC publications and CISA advisories are monitored weekly. NSA and sector-specific advisories (CNSA 2.0 scope changes, OSCCA updates) are monitored weekly. The EU Official Journal, BSI, ANSSI, and NCSC guidance are monitored on a biweekly to monthly cycle defined per source based on that source's publication cadence and change velocity. 3GPP and ETSI publication streams are monitored quarterly. IETF datatracker activity for relevant working groups (TLS, LAMPS, PQUIP) is monitored monthly. The organisation's own subscription to regulatory intelligence, whether delivered in-house or through retained counsel, must cover each of these sources as a continuous obligation.

Detected changes are classified on the three-category basis established in Section 6.2. Category A events require formal gate re-examination within five working days of detection and may trigger regulatory notification assessment in parallel. Category B events require architecture or operational review within thirty days. Category C events are logged, indexed against the affected gate, and reviewed at the next scheduled assurance review. Classification is performed by the Cryptographic Risk Committee and is recorded with the underlying source and the rationale.

Gate condition versioning is maintained as an evidence artefact in its own right. Each gate holds a versioned record of the regulatory instruments, algorithm standards, and vendor commitments current at time of passage. When a monitored source issues a material change, the versioned record identifies which gates are affected and which specific conditions within those gates require re-examination. Without versioning, the question "was this gate passed under the current rules or an earlier set" cannot be answered, and the governance structure becomes undefendable under audit.

The Cryptographic Risk Committee's remit under this section is explicit: it owns the gate reversion process, holds authority to reopen any passed gate on the basis of a classified change event, and is accountable to the board for the continued validity of gate conditions across the programme lifetime and the BAU operating model. This remit must be established in the committee's terms of reference at Gate 6 and remain in force indefinitely thereafter. Any gate reversion event triggers a mandatory update of the evidence artefacts affected by the reverted condition. Depending on the gate and the trigger, this may include the CBOM, the target architecture document, the vendor assessment and register, the wave prioritisation record, the interoperability test evidence, or the operating model documentation. The updated artefacts form part of the re-examination evidence package and are recorded against the gate's versioned condition history. A reverted gate is not closed again until the affected evidence artefacts have been updated, reviewed, and approved under the same standard that applied to the original gate passage.

BAU transition is a gate, not a natural programme conclusion. If the programme reaches Month 36 without a functioning operating model, a current CBOM, live monitoring, and audit-ready evidence artefacts, the programme has not concluded. It has stalled at Gate 6.

13. Conclusion: If You Cannot Operate It and Prove It, You Do Not Control It

The cryptographic transformation mandate is real, it is time-bounded, and it is consequential. Organisations that fail to execute it will face regulatory enforcement, operational exposure, and the systemic risk of cryptographic infrastructure that cannot resist the adversarial environment of the quantum era.

The SITG-Consulting Cryptographic Transformation Implementation Model is the architecture for executing that mandate correctly. It is gated, which means governance cannot be bypassed. It is wave-based, which means execution is risk-ordered. It is evidence-driven, which means the programme produces proof, not documentation. And it is operationally grounded, which means it ends with a functioning operating model, not a migration report.

T R A N S F O R M A T I O N | 1 2

Cryptographic transformation is not a migration. It is a gated, evidence-driven, multi-year programme that must be operated and proved. The organisations that understand this distinction and build their programmes accordingly will meet regulatory requirements and will retain control of their cryptographic posture in a threat environment that is not waiting for them to be ready.

13.1 The Decisive Argument

There is a version of this programme that fails under audit. Appoint a cryptographic migration workstream. Commission a discovery exercise. Produce a report. File it. Move on. In two years, when the regulator asks for evidence, assemble what documentation exists and hope it is sufficient.

There is another version. Appoint a transformation programme with a board mandate. Build the CBOM. Gate the architecture. Assess the vendors. Execute in waves. Build the operating model. Produce the evidence. When the regulator asks, the evidence is already there, not assembled for the audit but produced continuously as the normal output of a functioning programme.

The difference between these two versions is not technical. It is governance. The SITG model provides the governance architecture. What the organisation provides is the decision to use it.

The decisions made in the next twelve months will determine which version of this programme your organisation is running in year three.

SITG-Consulting | Cryptographic Transformation Group

Execution is risk-driven and wave-based. Not linear.

Appendix A: Glossary of Acronyms and Defined Terms

Acronym / Term	Definition
3GPP	3rd Generation Partnership Project. International standards body for mobile telecommunications.
BAU	Business as Usual. The steady-state operational posture following programme closure.
CBOM	Cryptographic Bill of Materials. Machine-readable inventory of all cryptographic assets, algorithms, keys, certificates, and their attributes across the estate.
CI/CD	Continuous Integration / Continuous Deployment. Automated software build, test, and deployment pipeline.
Cryptographic Agility	The operational capability to swap cryptographic algorithms rapidly across the estate in response to vulnerabilities, standards changes, or regulatory requirements, without service disruption.
DORA	Digital Operational Resilience Act. EU regulation imposing ICT risk management, incident reporting, and resilience testing obligations on financial entities.
ECDH	Elliptic Curve Diffie-Hellman. Classical key agreement protocol based on elliptic curve cryptography.
ETSI	European Telecommunications Standards Institute.
Gate	A mandatory governance checkpoint requiring validated evidence before programme progression. Gates cannot be bypassed or treated as advisory.
HNDL	Harvest Now, Decrypt Later. Adversarial strategy of capturing encrypted data today for retrospective decryption when quantum capability matures.
HSM	Hardware Security Module. Tamper-resistant hardware device for cryptographic key generation, storage, and operations.
KMS	Key Management System. Infrastructure for the generation, distribution, rotation, and revocation of cryptographic keys.
ML-DSA	Module-Lattice-Based Digital Signature Algorithm (FIPS 204). NIST post-quantum digital signature standard.
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism (FIPS 203). NIST post-quantum key exchange standard.
NIS2	Network and Information Security Directive (EU). Imposes cybersecurity obligations on essential and important entities in critical infrastructure and telecommunications.
PKI	Public Key Infrastructure. The framework of certificate authorities, registration authorities, and certificate management systems that underpin digital trust.
PQC	Post-Quantum Cryptography. Cryptographic algorithms designed to resist attack by both classical and quantum computers.
RSA	Rivest–Shamir–Adleman. Classical public-key cryptosystem vulnerable to quantum factoring attacks.
SIEM	Security Information and Event Management. Platform for real-time monitoring, correlation, and alerting of security events.
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm (FIPS 205). NIST post-quantum digital signature standard.
TLS	Transport Layer Security. Cryptographic protocol securing communications over computer networks.

TOM	Target Operating Model. The design specification for how the cryptographic capability will be operated, governed, and sustained after programme closure.
Wave	A structured migration event with defined scope, success criteria, rollback procedures, and evidence requirements. Waves are risk-sequenced, not arbitrary batches.
3GPP Release 18/19	3rd Generation Partnership Project technical specification releases addressing PQC integration for 5G NR security architecture through study items and emerging specifications, covering key derivation, SIM credentials, and network function authentication. As of April 2026, PQC in 3GPP is not fully standardised in mandatory form. Applicable to telecommunications operators.
ANSSI	Agence nationale de la sécurité des systèmes d'information. French national cybersecurity authority which issues position papers requiring independent algorithm evaluation for systems under French regulatory oversight.
BSI TR-02102	German federal algorithm recommendations published by the Bundesamt für Sicherheit in der Informationstechnik, specifying cryptographic parameter requirements that diverge from NIST in certain categories.
CNSA 2.0	Commercial National Security Algorithm Suite 2.0 published by the NSA in September 2022. Imposes hard transition deadlines by asset category for National Security Systems and their supply chains, including software and firmware by January 2025, network security devices by end 2026, operating systems and browsers by 2027, and full transition by 2033.
CRYPTREC	Cryptography Research and Evaluation Committees, Japan. Operates an independent PQC algorithm approval process separate from NIST. Applicable to organisations with Japanese regulated operations.
Dual-Stack Architecture	An architectural pattern in which an organisation operates two parallel cryptographic estates to satisfy structurally incompatible national regulatory regimes. The canonical case is a NIST-aligned estate for non-Chinese jurisdictions paired with an SM-family estate for Chinese domestic regulated applications under OSCCA.
eIDAS 2.0	EU Regulation on electronic identification and trust services, in its 2024 revision. Imposes PQC requirements on qualified trust service providers and European Digital Identity Wallet infrastructure.
Gate Reversion	The formal reopening of a previously passed governance gate when subsequent events invalidate its evidence basis. Triggers include algorithm vulnerability disclosure, material regulatory change, vendor failure, or architecture non-conformance. Gate reversion is a structural part of the model; the machinery is set out in Section 12.3.
Jurisdiction-Differentiated Architecture	An architectural approach in which cryptographic assets are tagged by their governing regulatory jurisdiction, and target architecture decisions are made against jurisdiction-specific requirements matrices feeding into Gate 3. The approach accommodates organisations operating under multiple divergent regulatory regimes.
OSCCA	Office of State Commercial Cryptography Administration. The Chinese regulatory body administering the Cryptography Law of the People's Republic of China. Mandates nationally approved algorithms (SM2, SM3, SM4) for domestic regulated applications, structurally incompatible with a NIST-only architecture.
SM2	Chinese public-key cryptographic algorithm based on elliptic curves, mandated by OSCCA for digital signatures and key exchange in domestic regulated applications.
SM3	Chinese cryptographic hash function, mandated by OSCCA for integrity and authentication functions in domestic regulated applications.
SM4	Chinese symmetric block cipher, mandated by OSCCA for encryption of data in domestic regulated applications.

Tiered Entry	A programme entry determination, made at board level during Gate 1, classifying the organisation into one of four tiers based on current regulatory compliance posture and prior programme state. Tier 1 is current regulatory breach; Tier 2 is inventory complete but architecture pending; Tier 3 is mid-transition under prior governance; Tier 4 is standard entry from a clean baseline.

Appendix B: Sources and References

All sources verified as of April 2026. Readers should confirm current status before reliance, as standards and regulatory instruments may be updated.

NIST FIPS 203 – Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM). Published August 2024. csrc.nist.gov/pubs/fips/203/final

NIST FIPS 204 – Module-Lattice-Based Digital Signature Algorithm (ML-DSA). Published August 2024. csrc.nist.gov/pubs/fips/204/final

NIST FIPS 205 – Stateless Hash-Based Digital Signature Algorithm (SLH-DSA). Published August 2024. csrc.nist.gov/pubs/fips/205/final

NIST Post-Quantum Cryptography Standardisation – Programme overview and timeline. csrc.nist.gov/projects/post-quantum-cryptography

OMB Memorandum M-23-02 – "Migrating to Post-Quantum Cryptography." November 2022. whitehouse.gov/wp-content/uploads/2022/11/M-23-02-Migrating-to-Post-Quantum-Cryptography.pdf

NIST SP 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organisations. csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

EU Regulation 2022/2554 (DORA) – Digital Operational Resilience Act. eur-lex.europa.eu

EU Directive 2022/2555 (NIS2) – Network and Information Security Directive. eur-lex.europa.eu

ISO/IEC 27001:2022 – Information Security Management Systems. iso.org

IETF draft-ietf-tls-hybrid-design – Hybrid key exchange in TLS 1.3. Draft status. datatracker.ietf.org

IETF draft-ietf-lamps-pq-composite-sigs – Composite PQC signatures for X.509 certificates. Draft status. datatracker.ietf.org

EU General Data Protection Regulation (GDPR) – Regulation 2016/679. eur-lex.europa.eu

CNSA 2.0 – Commercial National Security Algorithm Suite 2.0. National Security Agency, September 2022. Hard transition deadlines for National Security Systems and their supply chains. nsa.gov/cybersecurity

OSCCA Cryptography Law of the People's Republic of China – Administered by the Office of State Commercial Cryptography Administration. Mandates SM2, SM3, SM4 for domestic regulated applications. oscca.gov.cn

BSI TR-02102 – Technical Guideline on Cryptographic Mechanisms. Bundesamt für Sicherheit in der Informationstechnik. bsi.bund.de

ANSSI Position Papers on PQC – Agence nationale de la sécurité des systèmes d'information. ssi.gouv.fr

CRYPTREC – Cryptography Research and Evaluation Committees, Japan. Independent PQC algorithm approval process. cryptrec.go.jp

eIDAS 2.0 – EU Regulation 2024/1183 amending Regulation (EU) 910/2014 on electronic identification and trust services. European Digital Identity Wallet infrastructure. eur-lex.europa.eu

3GPP Release 18/19 – 3rd Generation Partnership Project Technical Specifications for 5G NR security. PQC integration requirements expected through Release 19. 3gpp.org

Appendix C: Jurisdictional Regulatory Instruments (Summary Treatment)

This appendix summarises regulatory instruments that receive summary treatment in Section 2. CNSA 2.0 and OSCCA are covered in the main body and are not repeated here. The five instruments below impose obligations on organisations operating in the relevant jurisdictions and should be treated as inputs to Gate 3 architecture approval where applicable. All references verified as of April 2026; readers should confirm current status before reliance.

BSI TR-02102 (Germany)

Published by the Bundesamt für Sicherheit in der Informationstechnik, TR-02102 is the German federal technical guideline on cryptographic mechanisms. It specifies recommended algorithms and parameter sizes for federal use and for organisations subject to German regulatory oversight. BSI has issued migration planning guidance for post-quantum cryptography with recommended completion of planning activities by 2025. In certain parameter categories BSI recommendations diverge from NIST baselines, which matters for organisations operating jointly under both regimes. Organisations subject to TR-02102 should map their target architecture decisions against the current BSI technical guideline at Gate 3 and re-map when BSI publishes revised guidance. Relevant to organisations with German federal customers, German critical infrastructure operations, and German subsidiaries of multinational financial entities subject to BaFin supervision.

ANSSI (France)

The Agence nationale de la sécurité des systèmes d'information is the French national cybersecurity authority. ANSSI issues position papers on post-quantum cryptography that impose an independent algorithm evaluation requirement for systems under French regulatory oversight. ANSSI's position is that PQC algorithms require national-level evaluation before deployment in sensitive systems, and that reliance on NIST validation alone is not sufficient for French regulatory purposes in certain categories. Organisations subject to ANSSI oversight should treat ANSSI position papers as binding inputs to Gate 3 architecture approval and must confirm the current ANSSI position on each deployed algorithm before production transition. Relevant to organisations with French government customers, operators of essential services under French national transposition of NIS2, and qualified operators of vital importance (OIV).

CRYPTREC (Japan)

The Cryptography Research and Evaluation Committees operate under joint sponsorship of Japanese government agencies. CRYPTREC maintains the e-Government Recommended Ciphers List which determines acceptable cryptographic algorithms for Japanese government systems and, by extension, influences the technology choices of Japanese regulated industries. CRYPTREC operates an independent PQC algorithm evaluation process separate from NIST. As of April 2026, the CRYPTREC PQC algorithm list is not finalised. Organisations subject to CRYPTREC should treat Gate 3 architecture approval as provisional for CRYPTREC-governed assets until the final list is published, and must include a gate reversion trigger for CRYPTREC publication events. Relevant to organisations with Japanese government customers, Japanese

banking operations supervised by the Financial Services Agency, and Japanese critical infrastructure operators.

eIDAS 2.0 (European Union)

eIDAS 2.0 (Regulation 2024/1183) amends the original eIDAS Regulation and introduces the European Digital Identity Wallet. The implementing acts impose specific cryptographic requirements on qualified trust service providers and on the wallet infrastructure. Member states are required to make European Digital Identity Wallets available to citizens within timelines defined by the relevant Implementing Acts, with national transposition schedules varying across the EU. Organisations that are qualified trust service providers should consult the national transposition schedule applicable to their jurisdiction for the deadlines they face and should not assume a single EU-wide deployment date. PQC transition for wallet infrastructure and qualified signatures is on the critical path for affected providers. Organisations that are qualified trust service providers, issuers of European Digital Identity attributes, or operators of relying-party services for the wallet should treat eIDAS 2.0 implementing acts and their applicable national transposition as hard inputs to Gate 3 and should plan Gate 5 production transition against the specific deadlines in scope. Relevant to qualified trust service providers across the EU, banks operating under PSD2 strong customer authentication using eIDAS trust services, and public-sector issuers of digital credentials.

3GPP Release 18/19

The 3rd Generation Partnership Project is the standards body for mobile telecommunications. Releases 18 and 19 address PQC integration for 5G NR security architecture through study items and emerging specifications, covering key derivation functions, SIM credential management, subscriber authentication, and network function authentication. As of April 2026, PQC in 3GPP is not fully standardised in mandatory form; work is ongoing through study items and draft specifications. Release 19 specification finalisation is currently expected late 2026, subject to 3GPP plenary decisions. 3GPP specifications are implemented by equipment vendors with a lag, which means operators will face a period during which network equipment PQC support is incomplete and must be managed as explicit residual risk. Telecommunications operators should track 3GPP publication streams, treat ratified specifications as vendor readiness triggers at Gate 4, and build their wave sequencing around the expected availability of PQC-capable equipment from each critical vendor. Relevant to mobile network operators, telecommunications equipment vendors, SIM card issuers, and enterprises operating private 5G networks.

Appendix D: Evidence Artefact Composition and Approval

This appendix elaborates the eight evidence artefact categories introduced in Section 8.2, specifying for each the required elements, the approval authority, and the retention and versioning expectations. It does not prescribe templates, schemas, or tooling. It defines the composition an artefact must have to pass the relevant gate and to survive subsequent audit. A transformation lead uses this appendix as the acceptance standard against which the delivery team's work is tested. The specialist engagements that produce the artefacts operate against the standard described here; how they meet the standard is their own engineering decision.

Where an artefact is referenced both by gate (Section 6 Gate Deliverables Summary) and by category (Section 8.2), this appendix is the authoritative reference for its required composition. Gate and phase deliverable lists remain the authoritative reference for which artefacts must exist at which point in the programme lifecycle.

D.1 Baseline CBOM

Required elements. Enumerated inventory of cryptographic assets in scope, each asset identified by a unique reference; asset type classification (certificate, key, cryptographic module, cryptographic service, protocol endpoint, algorithm instance); cryptographic material described by algorithm, key length, and parameter profile; discovery method recorded against each asset; confidence tier applied (High, Medium, Low, Attestation-only) with the numeric threshold justifying the tier; jurisdiction tag for each asset where multi-jurisdictional operations are in scope; owner or responsible team named against each asset; known-unknown declarations for asset categories where discovery could not be completed; timestamp of discovery and scheduled re-scan cadence; links to source evidence (scan output, SBOM entry, attestation record).

Required approvals. SteerCo at Gate 2. Independent sampling audit report attached and signed by a party external to the delivery team before SteerCo approval.

Retention and versioning. Retained for the lifetime of the programme and for the period required by the applicable regulatory retention schedule after BAU transition. Versioned on every material change and on every gate reversion event affecting the CBOM.

D.2 Migration CBOM

Required elements. All Baseline CBOM elements; current migration state per asset (not started, in progress, migrated, decommissioned, vendor-blocked, deferred); pre-migration state and post-migration state recorded per asset at the point of wave transition; wave identifier against each migrated asset; decommissioning status for superseded classical cryptographic material (key zeroisation, certificate revocation, HSM slot destruction); residual classical cryptography in the estate quantified and categorised; cumulative transition progress expressed as a proportion of scope by asset count and by risk weight.

Required approvals. SteerCo at Gate 5 for each wave. Cryptographic Risk Committee for cumulative state at defined assurance cadence in BAU.

Retention and versioning. Versioned at every wave close. Full historical state retained for the regulatory retention period. Superseded versions are archived, not deleted.

D.3 Target Architecture Document and Architecture Decision Records

Required elements. Target cryptographic architecture described at logical and physical layers; algorithm selections with supporting justification referencing applicable standards and regulatory inputs; hybrid strategy defining classical-to-PQC transition rules and the conditions under which pure PQC operation is permitted; jurisdiction-differentiated requirements matrix where multi-jurisdictional operations are in scope; dual-stack architecture specification where OSCCA or equivalent regimes apply; cryptographic agility design including the tested algorithm swap procedure and the control points at which agility is exercised; key management architecture; PKI hierarchy design; interoperability boundary definitions; architecture decision records capturing each material decision with alternatives considered, rationale, and dissenting positions where applicable.

Required approvals. SteerCo at Gate 3. Legal, regulatory, and technical stakeholders sign the regulatory mapping confirmation before SteerCo approval. Architecture decision records are signed by the named architecture authority.

Retention and versioning. Versioned on every material change. Every version retained. Gate reversion events affecting architecture are recorded against the version history with the trigger, the classification, and the re-examination outcome.

D.4 Vendor Assessment Evidence and Supply Chain Documentation

Required elements. Vendor register listing every critical supplier whose products or services sit within the cryptographic boundary; per vendor, the cryptographic supply chain documentation (component provenance, third-party dependencies, sub-supplier declarations); per vendor, validation evidence for PQC implementation against NIST or equivalent approved lists; per vendor, contractual obligations for algorithm support, remediation terms, and notification timelines for vulnerability disclosure; residual vendor risk register categorising each vendor by readiness evidence; for any vendor that passed Gate 4 conditionally, the documented remediation plan, the approved residual risk statement, and the quarterly re-review cadence record.

Required approvals. SteerCo at Gate 4. Board approval for any vendor escalation outcome. Procurement or supplier management function signs the contractual obligations.

Retention and versioning. Versioned on every vendor status change. Conditional pass records versioned on every quarterly re-review. Retained for the regulatory retention period applicable to supply chain records.

D.5 Wave Execution Evidence

Required elements. Wave identifier and scope (asset list, jurisdictions, integration points); pre-migration CBOM state snapshot; post-migration CBOM state snapshot; interoperability test reports covering all integration points in wave scope; staging environment validation evidence; tested rollback procedure with execution record; go-live authorisation record; wave failure classification where applicable (rollback successful, rollback partial, rollback failed) with the governance response recorded; for non-atomic waves, the documented compensating controls, the containment procedures, the declared point of no return, and the evidence produced at wave close.

Required approvals. SteerCo at Gate 5 for each wave. Receiving operational teams confirm operational readiness before go-live authorisation. Wave failure classification is a SteerCo decision during the programme phase and a Cryptographic Risk Committee decision in BAU.

Retention and versioning. One evidence pack per wave. Retained for the regulatory retention period. Wave packs are not versioned after wave close; subsequent changes produce new wave evidence under gate reversion or new wave scope.

D.6 Sovereign and Regulatory Alignment Confirmations

Required elements. Per jurisdiction in scope, the applicable regulatory instruments identified with publication references; the mapping from each instrument to the architecture decisions, deliverables, and gates affected; per wave, the regulatory alignment confirmation for the jurisdictions covered by that wave; where dual-stack architecture is in scope, separate alignment confirmations for each stack; legal sign-off against each jurisdiction confirmation; record of any open regulatory interpretation held under qualified legal advice.

Required approvals. Legal function, regulatory function, and technical authority. SteerCo acceptance at Gate 3 for the programme-level mapping and at Gate 5 for each wave's alignment confirmation.

Retention and versioning. Versioned on every material regulatory change under the gate reversion process. Superseded versions retained with the trigger event recorded.

D.7 Cryptographic Agility Test Evidence

Required elements. Documented agility capability covering the scope of deployed algorithms; defined algorithm swap procedure; test scenarios exercised; test cadence approved by the Cryptographic Risk Committee with a minimum annual exercise and additional exercises on every material algorithm change event; test execution records including date, scope, outcome, and any defects identified; remediation status of defects.

Required approvals. Cryptographic Risk Committee approves the test cadence and reviews the test results. The agility design is approved at Gate 3 as part of the Target Architecture Document.

Retention and versioning. Test records retained indefinitely within BAU. Historical test evidence forms part of the audit trail and is not overwritten by subsequent tests.

D.8 Operating Model Handover and BAU Evidence

Required elements. Operating model handover record confirming that all six Level 4 functions are live and staffed or contracted; monitoring and telemetry validation evidence; Cryptographic Risk Committee terms of reference adopted and in force; regulatory reporting obligations confirmed as met with the supporting evidence; gate reversion machinery operational per Section 12.3 including source monitoring cadences, change classification process, and escalation routing; continuous assurance reporting cycle defined and exercised at least once before Gate 6 closure; formal programme closure authorisation signed by the SteerCo and the board.

Required approvals. SteerCo at Gate 6. Board sign-off on programme closure. Cryptographic Risk Committee confirms its remit and terms of reference before handover completes.

Retention and versioning. Handover record retained permanently as part of the organisation's governance history. BAU evidence is produced continuously on the cadence established at Gate 6 and retained per regulatory schedule.

Legal Notice and Copyright Statement

Disclaimer This handbook is provided for general information only. It does not constitute legal, regulatory, financial, investment, cybersecurity, or technical advice. Organisations should obtain independent professional advice before acting on any information contained in this document. References to regulatory frameworks (including DORA, NIS2, GDPR, and NIST publications) are for contextual orientation only and do not constitute compliance guidance. Regulatory compliance depends on jurisdictional interpretation, organisational context, and implementation specifics; organisations should obtain qualified legal advice before relying on this document for compliance purposes.

SITG-Consulting makes no representations or warranties regarding the accuracy, completeness or suitability of the information contained in this publication. SITG-Consulting accepts no liability for any loss or damage arising from reliance on this document.

Confidentiality and Use Restrictions This document may contain confidential or proprietary information belonging to SITG-Consulting. It is supplied solely for the use of the intended recipient. By accessing this document, the recipient agrees not to disclose, distribute or reproduce its contents without written authorisation from SITG-Consulting.

Any evaluation, benchmarking or comparison of SITG-Consulting implementation models or intellectual property against third-party offerings is not permitted without prior written consent.

Intellectual Property Notice All methodologies, implementation models, diagrams, CBOM structures, taxonomies and terminology contained in this document are the intellectual property of SITG-Consulting. This includes, without limitation, cryptographic readiness models, PQC migration structures, governance schemas, diagnostic tools, and risk profiling constructs.

Use of these materials outside SITG-Consulting advisory engagements is prohibited.

No Endorsement or Warranty References to third-party standards, vendors, cloud platforms, or regulatory bodies are for context only and do not imply endorsement or affiliation. All trademarks, service marks and product names are the property of their respective owners.

Version Control Only the latest authorised version of this document may be relied upon. SITG-Consulting reserves the right to amend, update or withdraw this publication at any time without notice.

Governing Law This document and any dispute arising from it shall be governed by and interpreted in accordance with the laws of England and Wales. The courts of England and Wales shall have exclusive jurisdiction.

Contact SITG-Consulting Strategy | Intelligence | Technology | Growth

Email: info@sitg-consulting.com

Tel: +66 97 217 6658