



NOVEMBER 5, 2025



IMPLEMENTATION ROADMAP AND PHASING GUIDE

*SEQUENCED MILESTONES AND FINANCING LOGIC FOR SCALABLE
DOMESTICATION AND MONITORING OF INSTITUTIONAL ROLLOUT.*

CREATED BY

EUSL AB

Care to Change the World



Table of Contents

Chapter 1 — Sequencing and Milestones	2
Chapter 2 — Tranche Logic and Financing	4
Chapter 3 — Domestication and Scale-Out.....	5
Chapter 4 — Monitoring and Reporting	6
Final Provision — Entry into Force and Annex Logic	7

Implementation Roadmap and Phasing Guide

Preamble and Applicability. This Roadmap is promulgated under the GSIA Charter and shall be read consistently with Documents 00–19 and the affirmed order of prevalence: mandatory national public law; the GSIA Charter; this Roadmap; and downstream instruments and annexes. The constitutional allocation of functions remains binding. The GSIA SCE sets policy and exercises mandate oversight; GSIA Holding AB maintains canonical standards, clause libraries, evidence taxonomies, templates, and maturity models without operational entanglement; GSIA AB executes under Service Level Agreements (SLAs); DESA-class entities (e.g., SUDESA, CODESA, and regional/national DESA units) are designated recipient-operators; and—where bankability and continuity so require—Hosted Ownership may be employed within ring-fenced perimeters subject to non-attachment, negative pledge, discrete ledgers and bank accounts, and a binding reversion covenant to the Member upon readiness. Publication remains a control: disclosure is presumptive, with lawful redaction and time-limited deferrals by reasoned resolution entered in the deferral register. Controller/processor roles are explicit; DPIAs are undertaken for high-risk processing; identity and access management enforces least-privilege with multi-factor authentication; logs are immutable and time-synchronised; encryption is mandatory in transit and at rest. Domestication proceeds through the gated progression—shadowing → dual-key → lead-role → system handover → legal localisation → readiness certification—verified under Document 09 and reflected in tranche logic under Document 10.

Chapter 1 — Sequencing and Milestones

1.1 Purpose and Constitutional Position. This Chapter codifies the standard sequence, critical path, and milestone structure for launching, operating, and handing over GSIA-mandated programmes. It binds all instruments and schedules, which must be read consistently with the Charter, the Legal Instruments Compendium (Document 07), and the fiduciary, safeguards, and digital trust frameworks (Documents 06 and 12).

1.2 Phased Sequence (Standard Critical Path). Implementation follows six legally significant phases, each with defined entrance criteria, deliverables, and publication acts:

1. Initiation and Mandate Confirmation.

Entrance: SCE resolution approving programme concept, scope, and Host engagement.

Deliverables: Draft SLA (GSIA AB), draft Implementation Agreement (IA), draft HCA clauses (where applicable), initial controller/processor mapping, DPIA scoping, and Publication Plan.

Publication: Mandate synopsis with lawful redaction; entry in Pipeline Register (Document 14).

2. Structuring and Custody Design.

Entrance: Approved term sheet and Parallel Action Resolution (if Hybrid REC applies).

Deliverables: Flowhub custody architecture (discrete accounts/ledgers, escrow/waterfalls, signatory matrices), negative pledge/non-attachment clauses, step-in rights, Hosted Ownership perimeter (if required) with reversion covenant, and EFFORT schema for programme-level transparency.

Publication: Custody design synopsis; DPA templates; procurement plan summary; domestication gate map.

3. **Safeguards, Digital Trust, and Appraisal Readiness.**

Entrance: Completed safeguards screening, draft procurement strategy, completed DPIA(s) for high-risk processing.

Deliverables: ESG instruments; procurement integrity controls; controller/processor registers; IAM baseline; logging and encryption baselines; continuity (RTO/RPO) targets; MEL logic model, baselines, and verification plan; KRI set and escalation thresholds (Document 17).

Publication: Safeguards matrix; MEL and KRI synopses; lawful redaction for sensitive annexes.

4. **Pre-Operations and Shadowing.**

Entrance: Signed SLA/IA; custody accounts opened; authority matrices loaded; data-protection instruments executed.

Deliverables: Live systems dry-run; Learn-by-Doing cohorts onboarded (Document 19); evidence repositories initialised; Publication Register activated; first external validation plan scheduled (Document 09).

Publication: Go-live notice; training schedule; redaction and deferral entries where applicable.

5. **Operations—Dual-Key to Lead-Role.**

Entrance: Shadowing artefacts accepted; dual-key authority enabled.

Deliverables: Measurable throughput under four-eyes and segregation of duties; tranche-condition fulfilment; KRI monitoring and escalations; periodic reconciliations; procurement awards with integrity proofs; MEL verifications; external validations and rectifications; risk appetite/tolerance review (Document 17).

Publication: Quarterly EFFORT dashboards; tranche notices; validations and rectifications with lawful redaction.

6. **Handover—Legal Localisation and Readiness Certification.**

Entrance: External validation concluding acceptable control operation; Class A findings closed.

Deliverables: Key ceremonies; documentation escrow; asset/title transfer (if Hosted Ownership); legal registrations and mandate localisation; readiness certification dossier and issuance; survivals register (audit rights, records, warranties, liabilities).

Publication: Transfer notices; reconciled inventories; readiness certificate and survivals.

1.3 Milestone Catalogue (Authority-Linked). Each phase has **Authority-Linked Milestones (ALMs)** tied to decision rights and countersignature thresholds, including but not limited to: ALM-01 (Term Sheet Approval); ALM-05 (Custody Accounts Activated); ALM-09 (DPIA Completion); ALM-12 (Dual-Key Activation); ALM-15 (First Tranche Release); ALM-18 (Lead-Role Confirmation); ALM-21 (Handover Key Ceremony); ALM-24 (Readiness Certification). Milestones cannot be skipped; deferrals are reasoned, time-limited, and recorded.

1.4 Critical Dependencies and Gating Conditions. Dependencies include execution of DPAs, DPIA approvals, IAM baselines, escrow readiness, procurement plan acceptance, and MEL verification scheduling. Failure to satisfy a gating condition pauses progression and, where risk materialises, triggers protective measures (payment holds, scope reduction, step-in) without prejudicing Member ownership.

1.5 Publication and Evidentiary Standards. Every milestone carries a publication unit with chain-of-custody records, immutable logs, and integrity artefacts (hashes, timestamps). Lawful redaction protects personal data, procurement integrity, and security; deferrals require reasoned resolutions and sunset review.

Chapter 2 — Tranche Logic and Financing

2.1 Purpose and Constitutional Position. This Chapter operationalises tranche logic, financing flows, and fiduciary controls consistent with Flowhub doctrine (Document 03), the Eligibility and Leasing Framework (Document 04), and the Financial Stress and Contingency Manual (Document 10). It binds co-financing, pooled funds, grants, and commission utilisation under ring-fencing with no private distribution.

2.2 Tranche Architecture. Tranches are structured as Conditions-Precedent (CP) → Disbursement → Conditions-Subsequent (CS) cycles, aligned to domestication gates and verified outputs:

- **CP (non-exhaustive):** custody activation; negative pledge/non-attachment recorded; procurement plan approved; safeguards instruments effective; DPIAs complete; IAM/logging/encryption baselines operational; MEL baselines locked; KRI thresholds approved; Publication Plan loaded.
- **Disbursement:** executed from ring-fenced accounts under four-eyes and segregation of duties, with countersignature thresholds calibrated to risk and value; FX hedging permitted solely for risk reduction; no speculative positions (Document 10).
- **CS:** delivery of outputs and MEL verifications; KRI performance within tolerance; reconciliations to zero-variance standard or explained; publication of EFFORT summaries; rectification of findings within agreed timelines.

2.3 Co-Financing and Intercreditor Discipline. Intercreditor deeds preserve ring-fencing, *pari passu* (unless reasoned variance), step-in rights, publication covenants, and audit/access survivals. Waterfalls allocate cash to essential obligations (O&M, safeguards, MEL, liquidity buffers) before discretionary items; Flowhub commission remains within the constitutional baseline ($\leq 5\%$ absent Charter-conforming amendment) and is ring-fenced to governance, assurance, risk, and capacity functions.

2.4 Hosted Ownership Financing. Where Hosted Ownership is used, all inflows and outflows occur within the perimeter: discrete ledgers and bank accounts; escrow arrangements; title and asset registers; no private distribution. Reversion upon readiness is unconditional, with survivals enforced.

2.5 Liquidity, FX, and Counterparty Controls. Liquidity buffers match risk class and cadence; LCR-style metrics and Net Stable Funding-style measures are computed and monitored. FX exposures are matched and hedged to documented needs; counterparties must meet due-diligence standards and concentration limits (Document 10). Breaches trigger escalation and, where necessary, temporary tightening of authority matrices.

2.6 Value-for-Money and Cost Recovery. VfM assessments accompany tranche releases; cost recovery adheres to non-profit, full-cost rules (Document 13). Publication of tranche statements, commission accrual/utilisation, and VfM synopses is mandatory, with lawful redaction.

2.7 Tranche Pause, Restart, and Exit. Material non-conformities (Class A findings, repeated KRI red breaches, or sanctions violations) **pause** tranches. Restart follows verified rectification. Exit/wind-down (Document 10) preserves continuity for essential services, transparency, inventory reconciliations, and reversion of assets where applicable.

Chapter 3 — Domestication and Scale-Out

3.1 Purpose and Constitutional Position. This Chapter codifies the domestication trajectory and the controlled expansion (scale-out) beyond initial jurisdictions, without undermining fiduciary integrity, publication doctrine, data-protection duties, or the no-distribution rule.

3.2 Domestication Gates (Affirmation and Evidence). Progression through shadowing → dual-key → lead-role → system handover → legal localisation → readiness certification is evidence-based: artefacts include reconciled ledgers, controller/processor registers, DPIAs, IAM recertifications, procurement dossiers, MEL verifications, continuity drills, key ceremony minutes, localisation filings, and transfer notices. Each gate has a reasoned SCE acknowledgment and a publication unit with lawful redaction.

3.3 Scale-Out Preconditions. Scale-out to additional geographies or portfolios requires: (i) successful lead-role operation sustained in the initial jurisdiction; (ii) published EFFORT dashboards demonstrating outputs/results and fiduciary conformity; (iii) validated training cohorts and certification issuance (Document 19); (iv) risk appetite and tolerance recalibration (Document 17) for the expanded footprint; and (v) capacity and continuity assessments to avoid over-extension.

3.4 Hybrid REC Parallel Action. In hybrid portfolios, a two-tier domestication model applies: the hybrid layer sets cross-border standards, custody blueprints, reciprocal debarment, and data-sharing protocols; the country layer executes localisation, banking mandates, and legal filings. Parallel Action Resolutions define interlocks, publications, and tranche splits to avoid contagion and maintain pace.

3.5 DESA as Recipient-Operator. Scale-out uses DESA-class entities as recipient-operators rather than general treasuries, to preserve ring-fencing and verifiability. Where a DFI requires sovereign receipting, on-granting or on-lending to DESA includes the same fiduciary controls, publication rules, and reversion covenants, with survivals post-handover.

3.6 Knowledge Transfer and Certification-Led Expansion. Expansion is paced by certified capacity: Tier II/III institutional certifications (Document 19) in the seed jurisdiction become prerequisites for replication; secondments and exchanges are deployed to new sites with documented authority matrices, DPAs/DPIAs, and publication plans. Curriculum localisation is executed before fieldwork; assessments are scheduled with independent sampling.

3.7 Technology, Evidence, and Sovereignty. Scale-out of digital platforms follows the security architecture and data-protection policies (Document 12). Where localisation is mandated, on-shore tenancies or escrow preserve verifiability without unlawful transfers. Evidence repositories are federated: read-only, audited access enables external validation without breaking sovereignty constraints.

3.8 Publication and Public Mandate Continuity. Expansion communications maintain the canonical mandate narrative (Document 18), with EFFORT dashboards reflecting both original and new sites. Deferrals for procurement or investigation sensitivity are reasoned, time-limited, and sunset-reviewed.

Chapter 4 — Monitoring and Reporting

4.1 Purpose and Constitutional Position. Monitoring and reporting convert operational facts into governance decisions, tranche releases, and public trust. They are anchored in the Unified MEL Framework (Document 08), External Validation Protocol (Document 09), Risk Management Framework (Document 17), Compliance and Ethics Code (Document 11), and Financial Transparency (Document 13).

4.2 Monitoring Architecture. Monitoring comprises four integrated streams:

- **Fiduciary Monitoring.** Reconciliations (bank to ledger), authority-matrix overrides, commission accrual/utilisation, procurement integrity sampling, escrow releases, and step-in readiness.
- **Safeguards and ESG Monitoring.** Implementation of E&S instruments, grievance redress timeliness, debarment/sanctions checks, inclusion metrics.
- **Digital Trust Monitoring.** IAM recertifications, access anomalies, DPIA closures, incident response timelines, encryption and logging health.
- **MEL and Results Monitoring.** Indicator tracking, baselines vs. actuals, verification packs, external evaluation scheduling.

4.3 Reporting Cadence and Content. Reporting occurs at defined intervals and events:

- **Monthly:** Fiduciary dashboards, KRI summaries, reconciliation exceptions, procurement pipeline integrity signals.
- **Quarterly:** EFFORT dashboards; MEL indicator updates; ESG/safeguards performance; risk appetite/tolerance review notes; publication register updates and deferral sunseting.
- **Tranche-Linked:** CP and CS evidence packs with third-party attestations as required.
- **Annual:** Consolidated financial statements (where applicable), external audit reports, internal audit synthesis, independent validation summaries, certification status (institutions and individuals), and lessons learned circulars.

All reports are **published** with lawful redaction; executive summaries are issued contemporaneously unless lawfully deferred.

4.4 KRIs, Escalation, and Rectification. Threshold breaches (Document 17, Chapter 3) trigger time-bound escalations: amber (heightened monitoring), red (protective measures), systemic red (incident command and independent validation). Rectification plans assign owners, deadlines, and evidence standards; closures require verification and publication.

4.5 Data Integrity and Chain-of-Custody. Evidence used in reports is sourced from systems with immutable logging, time synchronisation, cryptographic hashing, and role-based access. Where sovereignty restricts access, on-shore escrow and notarised inventories preserve verifiability for external validation.

4.6 Appeals and Public Feedback. Stakeholder feedback and complaints about reports are logged and addressed under Document 11. Material errors prompt republication with change-logs and reasons. Non-retaliation applies to all complainants and contributors.



4.7 Survivals and Archives. Reports, evidence packs, publication units, redaction keys under seal, access logs, and deferral registers are archived for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, audit and access rights, and IP stewardship. Independent validators may be commissioned to opine on monitoring fidelity and reporting compliance.

Final Provision — Entry into Force and Annex Logic

This Roadmap enters into force upon SCE resolution and applies to all new and continuing programmes, subject to lawful localisation and Host Country Agreement terms. Annexes include: (i) Milestone-to-Authority Matrix; (ii) Standard Tranche CP/CS Checklist; (iii) Custody and Waterfall Schematics; (iv) Domestication Gate Evidence Index; (v) EFFORT Dashboard Template; and (vi) Monitoring and Publication Calendars. Where annexes require jurisdictional tailoring, localisation shall not dilute ring-fencing, negative pledge, non-attachment, publication doctrine, controller/processor clarity, domestication gates, or survivals.