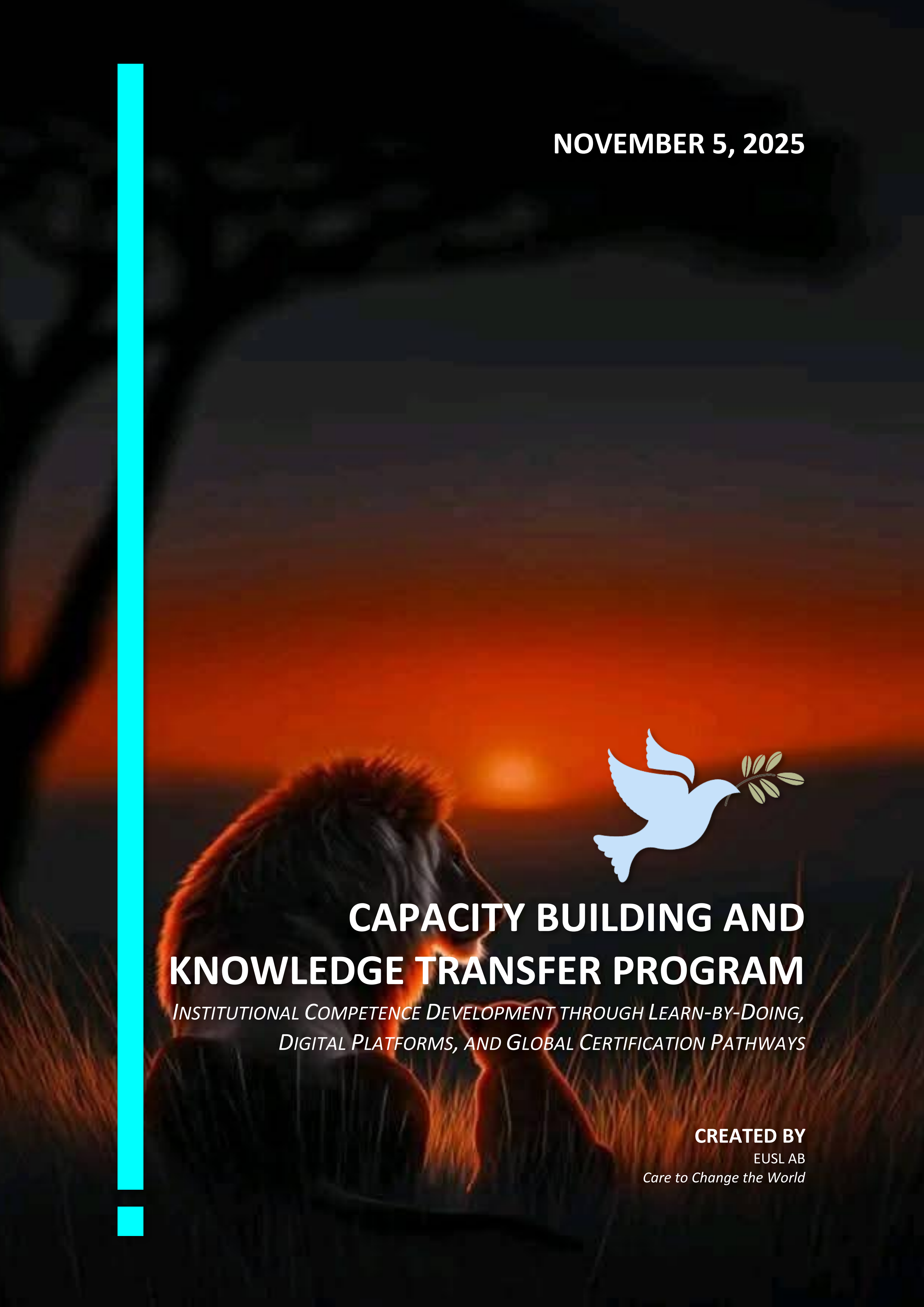
NOVEMBER 5, 2025



CAPACITY BUILDING AND KNOWLEDGE TRANSFER PROGRAM

Institutional Competence Development through Learn-by-Doing, Digital Platforms, and Global Certification Pathways

CREATED BY

EUSL AB

Care to Change the World

Table of Contents

Capacity Building and Knowledge Transfer Program

Preamble and Applicability. This Program is promulgated under the GSIA Charter and shall be read consistently with Documents 00–18 and the established order of prevalence: mandatory national public law; the GSIA Charter; this Program; and downstream instruments and annexes. The constitutional allocation of functions remains binding. The GSIA SCE sets policy and exercises oversight; GSIA Holding AB maintains canonical curricula, standards, clause libraries, and evidence taxonomies without operational entanglement; GSIA AB executes delivery under Service Level Agreements (SLAs); DESA-class entities (e.g., SUDESA, CODESA and regional/national DESA units) are designated recipient-operators and the locus of institutionalisation; 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 recorded 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. Capacity actions are synchronised to domestication gates—shadowing → dual-key → lead-role → system handover → legal localisation → readiness certification—and verified under Document 09.

Chapter 1 — Learn-by-Doing Curriculum

1.1 Purpose and Constitutional Position. The Learn-by-Doing Curriculum is the binding pedagogical architecture by which GSIA translates its standards, fiduciary controls, and digital trust doctrines into sustained institutional capability within DESA entities and competent Member authorities. It privileges practical, supervised operation of live systems over classroom abstraction, aligns with tranche logic, and culminates in readiness certification without diluting ring-fencing, publication doctrine, or controller/processor duties.

1.2 Separation of Functions. The SCE approves curriculum frameworks by resolution. GSIA Holding AB curates canonical syllabi, method libraries, assessment rubrics, and evidence packs; it does not operate live training environments. GSIA AB delivers instruction in situ under SLA, including coaching during shadowing and dual-key stages. DESA entities host the operational environment and trainees, and progressively assume lead-role stewardship. Agenda 74 Agency may be appointed as initial performer to accelerate stand-up, with a scheduled draw-down of its presence at lead-role.

1.3 Curriculum Structure and Modules. The curriculum is modular and cumulative, with sequenced Core Tracks and Applied Practicums:

1. **Core Tracks (mandatory):**
   a) **Fiduciary Controls and Flowhub Custody.** Ring-fencing; negative pledge; non-attachment; escrow/waterfalls; four-eyes and segregation of duties; countersignature thresholds; step-in mechanics; discrete ledgers and bank accounts; publication of commission and cost-recovery registers.
   b) **Procurement Integrity and ESG Safeguards.** Conflict management; market-soundings; sanctions screening; complaints and debarment interfaces; grievance redress mechanisms;

publication of awards.
c) **Digital Trust and Data Protection.** Controller/processor allocation; lawful bases; DPIAs; IAM least-privilege and recertification; immutable logging; encryption; localisation and escrow with integrity artefacts; incident response and breach notification.
d) **MEL and Independent Verification.** Indicator logic; baselines; sampling; verification packs; external validation interfaces; EFFORT presentation linking Expenditure, Financing sources, Flowhub custody, Outputs, Results, and Transition.
e) **Domestication Operations.** Gate criteria; key ceremonies; documentation escrow; legal localisation; readiness certification evidence; survivals (audit rights, records, warranties, liabilities).
f) **Continuity and Treasury Stress.** RTO/RPO targets; restore drills; liquidity buffers and KRIs; hedge policy (risk-reduction only); counterparty monitoring; crisis communications.

2. **Applied Practicums (live, supervised):**
a) **Shadowing Practicum.** Trainees observe and document live custody, procurement, MEL, and data-protection operations; produce a gap log mapped to standards.
b) **Dual-Key Practicum.** Trainees execute defined approvals and tasks with joint sign-off (e.g., payment batches; access grants; award notices; MEL verification uploads).
c) **Lead-Role Practicum.** Trainees (now custodians) operate end-to-end processes with GSIA oversight; run a full tranche cycle from conditions precedent to tranche release; complete a restore test; publish registers with lawful redaction.
d) **Handover Practicum.** Conduct key ceremony; migrate signatory matrices; lodge localisation filings; publish transfer notices and reconciliations.

1.4 Learning Artefacts and Evidence. Each module produces assessable artefacts: completed DPIAs; access recertification attestations; reconciled ledgers; procurement dossiers; MEL verification notes; publication units; restore test reports; and domestication registers. Artefacts are version-controlled, hash-anchored, and archived. Where sovereignty restricts export of personal or sensitive operational data, artefacts are maintained **in-country** with escrowed integrity proofs to preserve verifiability.

1.5 Assessment, Certification, and Publication. Assessments combine instructor observation, artefact review, and independent validation samples. Provisional Certification may be issued upon successful dual-key operation; Full Operational Certification requires sustained lead-role performance without material findings over a defined period, verified by external validation. Certificates, rubrics, and conditions (if any) are published with lawful redaction; deferrals are reasoned, time-limited, and recorded with sunset review.

1.6 Inclusion, Accessibility, and Non-Retaliation. Cohorts must include personnel from DESA entities, competent Member authorities, women-led and locally-led organisations, and oversight bodies. Materials are available in relevant languages and accessible formats. Participants and whistleblowers are protected by non-retaliation provisions under the Compliance, Audit, and Ethics Code.

1.7 Hosted Ownership Specifics. Where Hosted Ownership is active, practicums occur inside the ring-fenced perimeter. Financial artefacts reflect discrete accounts and ledgers; communications disclose perimeter existence, covenant protections, and reversion mechanics, with identifiers redacted for security. Handover practicum completes reversion steps; survivals remain in force as stipulated.

1.8 Records, Survivals, and Interfaces. Syllabi, enrolment and attendance, artefacts, assessment records, certifications, publication units, and deferral registers are archived per the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, audit and access rights, and IP stewardship by Holding AB. Interfaces exist with Document 18 (Knowledge Diplomacy), Document 11 (sanctions, investigations, non-retaliation), and Document 12 (digital trust).

Chapter 2 — Secondments and Exchanges

2.1 Purpose and Constitutional Position. Secondments and exchanges are structured, time-bound deployments designed to accelerate capability transfer, de-risk operational transitions, and embed GSIA doctrines—without compromising fiduciary safeguards, data-protection duties, or publication rules. They are instruments of domestication, not labour substitution.

2.2 Separation of Functions and Appointment. The SCE authorises secondments by reasoned resolution specifying scope, term, authority matrix, and publication requirements. GSIA Holding AB curates standard terms, conflict disclosures, and evaluation templates. GSIA AB administers deployments under SLA; DESA entities host secondees and name counterpart owners. Agenda 74 Agency may supply initial performers early in the cycle, with ramp-down milestones.

2.3 Instruments and Minimum Clauses. Each secondment or exchange uses an Appointment and Secondment Agreement (ASA) or Exchange Protocol (EP) containing: (i) mandate and scope; (ii) decision rights and countersignature thresholds; (iii) conflict-of-interest and recusal clauses; (iv) controller/processor allocation; (v) DPIA triggers and data-use restrictions; (vi) publication schedule and lawful redaction plan; (vii) confidentiality and IP stewardship (non-exclusive, royalty-free licences for public-interest use); (viii) grievance and non-retaliation provisions; and (ix) domestication linkage (target gate and readiness criteria).

2.4 Authority Matrices and Safeguards. Secondees do not hold unilateral authority over fiduciary or data-protection decisions. Authority matrices require dual-key approval for payments, access grants, procurement awards, tranche releases, and publication deferrals. All actions are executed from ring-fenced accounts and systems with immutable logs and least-privilege IAM. Break-glass invocations are logged and reviewed post-event.

2.5 Data-Protection, Sovereignty, and Publication. Where processing involves personal data or sensitive logs, a DPIA is conducted before deployment. Processing follows controller instructions under a DPA; localisation mandates are respected through on-shore processing or escrow. Publications arising from deployments (playbooks, lessons notes) are issued with lawful redaction and change-logs; deferrals are reasoned, time-limited, and recorded.

2.6 Exchange Typologies.
a) **Inbound Secondments to DESA.** GSIA AB or partner agency personnel seconded to DESA to establish custody, procurement, MEL, or digital trust baselines; exit upon completion of dual-key targets. b) Outbound Secondments from DESA/Authorities. DESA or Member staff seconded to GSIA AB delivery teams to learn portfolio-level standards, then return to lead role.

c) **Peer-to-Peer Exchanges.** Exchanges between DESA entities across countries or within hybrid-REC portfolios to harmonise methods; governed by a common EP and reciprocal recognition of debarments and sanctions.

d) **Academic/Professional Attachments.** Time-bound placements with UCE/UACE partners under data-use agreements and publication covenants; practical outputs are open-method artefacts.

2.7 Performance Management and Certification. Each deployment has a Workplan with deliverables mapped to domestication gates. Performance is reviewed at mid-term and completion against evidentiary criteria (e.g., reconciliations without material variance; DPIAs completed; restore tests passed; publication registers current). Successful completion yields a Deployment Certificate; non-performance triggers remedial coaching or early termination per ASA/EP.

2.8 Financing, Ring-Fencing, and Value-for-Money. Costs are financed from Member subscriptions, ring-fenced Flowhub commission (≤5% absent a Charter-conforming amendment), grants and pooled funds, or DFI technical assistance windows. Budgets are held in discrete ledgers and bank accounts; value-for-money assessments accompany disbursements; summaries are published with lawful redaction.

2.9 Hosted Ownership and Hybrid REC Application. In Hosted Ownership, deployments operate within the perimeter; authority matrices and publication rules follow the perimeter's instruments; reversion mechanics and survivals are explicitly rehearsed. In hybrid-REC portfolios, a two-tier deployment model applies: master-level standardisation and country-level localisation, with parallel action resolutions defining interlocks.

2.10 Complaints, Non-Retaliation, and Sanctions Interface. Complaints regarding conduct, conflicts, or interference are investigated under the Compliance, Audit, and Ethics Code. Verified breaches may ground sanctions (warning, conditions, removal, debarment), publication of findings with lawful redaction, and referral to competent authorities where mandated. Non-retaliation protections extend to hosts, secondees, and witnesses.

2.11 Records, Survivals, and Assurance. ASAs/EPs, conflicts registers, authority matrices, workplans, deliverables, evaluations, certificates, publication units, redaction keys under seal, and access logs are archived per 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 compliance and effectiveness of deployments.

Chapter 3 — Certification Pathways

3.1 Purpose and Constitutional Position. Certification Pathways constitute the binding, multi-tier credentialing regime by which GSIA attests to the competency of institutions and individuals to design, operate, and steward controls associated with fiduciary integrity, data protection, procurement integrity, MEL verification, and domestication. Certificates evidence capability; they do not confer operational mandates beyond those granted by governing instruments.

3.2 Separation of Functions and Independence. The **SCE** approves certification frameworks by resolution and authorises issuance of institutional and individual certificates. **GSIA Holding AB** maintains canonical standards, examination banks, practical assessment rubrics, and equivalency mappings; it is not party to issuing operational mandates. **GSIA AB** administers examinations and practicums under SLA and maintains records. External validators and Peer Review Panels (Document 09) provide independent sampling and spot checks; their opinions are published with lawful redaction.

3.3 Certification Tiers. Certification follows a three-tier structure, with clear scope, duration, and survivals:

1. **Tier I — Provisional Operator (Dual-Key Readiness).**
   Scope: Demonstrated grasp of standards and supervised execution of defined controls under dual-key arrangements.

Requirements: Completion of Core Tracks (Chapter 1 §1.3) and Shadowing and Dual-Key Practicums; submission of assessable artefacts (DPIAs, reconciliations, access recertifications, procurement dossiers, MEL verifications, publication units).
Authority: Operate only with joint countersignature and within authority matrices.
Duration: Up to 12 months, renewable once by reasoned resolution with time-bound remediation plan.
Publication: Certificate and rubric published with lawful redaction.

2. **Tier II — Lead-Role Operator (Operational Stewardship).**
   Scope: Sustained end-to-end operation of controls within a DESA or competent Member authority with GSIA oversight.

   Requirements: Successful Lead-Role Practicum; unqualified or acceptably qualified independent validation over a defined observation period; closure of Class A findings; continuity drills passed (RTO/RPO); EFFORT-style transparency current.
   Authority: Operate within local authority matrices; initiate tranche conditions subject to SCE-approved thresholds; authorise publications within doctrine.
   Duration: 24–36 months.
   Publication: Certificate, conditions (if any), and validation synopsis published.

3. **Tier III — Handover Custodian (Readiness Certification).**
   Scope: Institutional readiness for system handover and legal localisation with survivals intact.
   Requirements: Completion of handover practicum; key ceremonies executed; localisation filings complete; inventory and title reconciliations unqualified; data-protection governance embedded (controller/processor registers, DPIAs, incident plans); fiduciary and publication doctrine embedded; Hosted Ownership reversion executed where applicable.
   Authority: Assumes full custodianship within national legal frameworks; GSIA role transitions to advisory/assurance.

   Duration: 36 months (re-validation cycle by reasoned resolution).
   Publication: Readiness Certificate and survivals register published with lawful redaction.

3.4 Individual Certification Tracks. Individuals may obtain role-specific credentials aligned to authority matrices, including: (i) Custody & Treasury Operator; (ii) Procurement Integrity Officer; (iii) Data Protection & Digital Trust Lead; (iv) MEL & Independent Verification Lead; (v) Publication & Records Officer; and (vi) Continuity & DR Coordinator. Each track has knowledge exams, scenario-based assessments, and practicum sign-offs. Certificates are personal, non-transferable, and time-bound; misuse grounds sanctions (Document 11).

3.5 Equivalency and Recognition. Equivalency may be granted by reasoned resolution where external certifications demonstrate material alignment to GSIA standards (e.g., privacy or continuity management certifications). Equivalency never waives GSIA publication doctrine, ring-fencing, negative pledge, non-attachment, or domestication obligations. Conditions may include bridging modules or supervised practicums.

3.6 Publication and Registers. The Secretariat maintains Institutional Certification and Individual Credential Registers, published with lawful redaction (names, scope, dates, conditions, expiry). Deferrals for privacy or security are reasoned, time-limited, and sunset-reviewed. A Rectification Docket records corrective actions and re-assessments.

3.7 Revocation, Suspension, and Appeals. Certificates may be suspended or revoked upon: (i) material non-conformities; (ii) sanctionable practices; (iii) lapse of conditions; or (iv) false representations. Decisions are reasoned and published. Appeals lie to the Appeals Board under Document 09; protective measures remain pending outcome unless a reasoned stay is granted.

3.8 Hosted Ownership Specifics. Certification scopes in Hosted Ownership portfolios expressly reference ring-fenced perimeters, discrete ledgers/bank accounts, negative pledge/non-attachment, escrow/waterfalls, reversion mechanics, and survivals (audit rights, records, warranties, liabilities). Issuance of Tier III requires verified execution of reversion and publication of transfer notices and reconciliations with lawful redaction.

3.9 Records, Survivals, and Assurance. Exam scripts, artefacts, instructor notes, validation summaries, certificates, revocation decisions, appeals, and publication units are archived for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection duties, audit and access rights, and IP stewardship by GSIA Holding AB.

Chapter 4 — Digital Learning Platforms

4.1 Purpose and Constitutional Position. Digital Learning Platforms (DLPs) are the secure, governed environments through which GSIA delivers curricula, practicums, assessments, artefact repositories, and evidence packs at scale. They are instruments of public-interest education and capacity transfer; they are not marketing channels. DLPs must comply with the publication doctrine, data-protection obligations, and domestication gates and must be capable of lawful localisation and escrow to respect sovereignty.

4.2 Separation of Functions and Governance. The SCE approves platform architecture, tenancy governance, and localisation policies by resolution. GSIA Holding AB maintains canonical content libraries, control catalogues, assessment banks, and metadata taxonomies and defines evidence standards and retention. GSIA AB administers platforms under SLA, including identity management, access provisioning, logging, monitoring, and content workflows. Third-party vendors operate strictly as **processors** under DPAs; sub-processors require prior notification and a right to object on reasoned grounds.

4.3 Security and Digital Trust Baselines. DLPs implement: (i) least-privilege IAM with role engineering aligned to authority matrices; (ii) multi-factor authentication for privileged roles; (iii) immutable logging of access, content changes, assessments, and credential issuance; (iv) encryption in transit and at rest with GSIA-controlled keys where feasible; (v) segmentation of Hosted Ownership perimeters with separate directories, key vaults, and audit spaces; (vi) change control and code-signing for platform updates; and (vii) periodic restore tests aligned to RTO/RPO targets. Break-glass access is logged and subject to post-event review.

4.4 Content Lifecycle and Publication. Content follows a governed lifecycle: authoring → legal/DPO review → standards review by Holding AB → SCE sign-off → publication. All content (modules, exams, practicum guides, checklists, templates) is version-controlled and hash-anchored. Public content is published with lawful redaction and catalogued in an Open Methods Library; restricted content (e.g., assessment keys) is access-controlled and audited. Retirements and corrections are issued with change-logs and timestamps.

4.5 Data-Protection, DPIAs, and Sovereignty. DLP operations process personal data (enrolments, assessments, certifications) and potentially special category data in field simulations. Prior to activation in any jurisdiction, a **DPIA** is conducted to confirm lawful bases, minimisation, localisation/transfer mechanisms, retention, and data-subject rights handling. Where cross-border restrictions apply, GSIA deploys **on-shore tenancy** or **escrow** with integrity artefacts (hashes, timestamps) to preserve verifiability without exporting restricted data.

4.6 Evidence Repositories and Artefact Handling. Practicum artefacts (DPIAs, reconciliations, procurement dossiers, MEL verification notes, publication units, handover inventories) are stored in **evidence repositories** with chain-of-custody, cryptographic hashing, and notarised inventories. Access is time-bound, logged, and reviewed by Internal Audit; validators and Peer Review Panels receive read-only, audited access under Document 09.

4.7 Assessment Delivery and Proctoring. High-stakes assessments use proctoring methods proportionate to risk and local law (e.g., secure browsers, session recording with consent where lawful, identity verification, randomised item banks). Accommodations are provided consistent with accessibility requirements. Assessment artefacts (scores, item-level responses, proctoring logs) are retained per defined schedules and are accessible for appeals and quality assurance.

4.8 Interoperability and Open Standards. DLPs support standards-based content packaging and telemetry to enable portability between national platforms and the GSIA ecosystem. APIs are exposed under access controls for DESA systems to synchronise enrolments, completions, and credential status. Interoperability never derogates data-protection or publication doctrines; integrations are DPIA-gated.

4.9 Hosted Ownership and Hybrid REC Deployment. In Hosted Ownership, DLP instances are deployed within the ring-fenced perimeter, using separate directories, key vaults, and audit domains, and are financed through ring-fenced ledgers. In Hybrid REC portfolios, a two-layer approach applies: a regional instance for standards content and cross-border exchanges and national instances for localised practicums and certification records, linked through controlled federation agreements.

4.10 Transparency, Registers, and Deferrals. A **Learning Transparency** Register is maintained and published, listing course releases, assessment windows, credential issuance counts, and applicable deferrals. Deferrals for security, exam integrity, or personal-data protection are reasoned, time-limited, and sunset-reviewed. Public dashboards present EFFORT-style views linking capacity expenditures to outputs (modules delivered), results (certifications), and transition milestones (domestication gates reached).

4.11 Value-for-Money and Financing. DLP financing follows Document 13: Member subscriptions, ring-fenced Flowhub commission (≤5% absent a Charter-conforming amendment), grants and pooled funds, or DFI technical assistance. Budgets are held in discrete accounts and ledgers; procurements follow ESG and integrity rules; VfM assessments and summaries are published with lawful redaction.

4.12 Records, Survivals, and Assurance. Platform configuration baselines, access logs, DPIAs, DPAs, sub-processor notices, content approvals, assessment banks, credential issuance records, publication units, and deferral registers are archived per the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, audit and access rights, and IP stewardship by GSIA Holding AB. Independent validators may be commissioned to opine on platform conformity to security, data-protection, publication, and domestication requirements.