NOVEMBER 5, 2025

EXTERNAL VALIDATION AND PEER REVIEW PROTOCOL

Establishing Independent Assurance and Transparent Peer Review Mechanisms for Institutional Integrity and Global Credibility

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

External Validation and Peer Review Protocol

Preamble and Applicability. This Protocol is issued under the authority of the GSIA Charter and shall be read consistently with Documents 00–08 and the prevalence order previously affirmed. It governs the conduct of independent validation, peer review, and related assurance acts over GSIA-mandated programmes, projects, and institutional functions operated through GSIA AB under SLA or, where applicable, through EUSL or other Hosted Ownership SPVs. It binds the GSIA SCE, GSIA Holding AB (in its stewardship role over standards and intellectual property), GSIA AB, Member authorities, and accredited third-party validators and reviewers. Publication is treated as a control; exceptions are reasoned, time-limited, and recorded. Data-protection, fiduciary controls, and domestication gates apply throughout.

Chapter 1 — Independent Assurance Principles

1.1 Purpose and Constitutional Position. Independent assurance is a constitutional safeguard that ensures verifiability of results, propriety of fiduciary conduct, and conformity with the Charter, the Flowhub Trio Plus doctrine, and applicable law. The GSIA SCE retains the mandate to commission, scope, and receive assurance work products. GSIA Holding AB maintains the canonical standards, templates, taxonomies, and evidence libraries that underpin assurance methods, without operational interference. GSIA AB executes operations and cooperates fully with assurance activities under SLA, without power to constrain scope or timing. When Hosted Ownership is in force, the SPV is subject to the same testing, with survival of access, audit, and step-in rights expressly preserved.

1.2 Independence, Objectivity, and Competence. All validators and peer reviewers shall be independent in fact and appearance from the activity, decision, dataset, or instrument under review. Independence is defined by absence of managerial responsibility, financial interest, or decision-making influence over the subject matter within a three-year lookback (or longer if required by national law). Objectivity is maintained through demonstrable methodological neutrality, documented professional scepticism, and recusal where conflicts arise. Competence requires domain expertise appropriate to the mandate (e.g., fiduciary controls, MEL methods, procurement integrity, information security, E&S safeguards), evidenced by qualifications, track record, and continuous professional development aligned with GSIA standards. Accreditation requirements and ongoing fit-and-proper criteria are addressed in Chapter 5.

1.3 Scope and Materiality. Assurance scope is determined by a reasoned resolution of the competent GSIA SCE committee, with reference to risk registers, KRIs, MEL plans, fiduciary exposure, and domestication stage. Materiality thresholds are defined ex ante to focus procedures on matters reasonably capable of influencing Member decisions, public trust, funding tranches, or domestication readiness. Qualitative materiality applies for governance failures, conflicts of interest, sanctionable practices, privacy or sovereignty risks, and ESG non-conformities, even where quantitative thresholds are not met.

1.4 Standards and Evidentiary Basis. Independent assurance shall be performed in accordance with codified GSIA Assurance Standards issued by GSIA Holding AB and adopted by GSIA SCE resolution. These standards incorporate chain-of-custody for evidence, reproducibility of tests, triangulation across data sources, and explicit documentation of assumptions, uncertainties, and limitations.

Evidence shall be sufficient, appropriate, and audit-ready, with provenance, timestamps, and access logs preserved. MEL data governance, encryption in transit and at rest, and role-based access apply at all times. Any use of automated tools or models must be explainable, with validation datasets archived and bias testing recorded.

1.5 Fiduciary Controls and Access Rights. Four-eyes approval, segregation of duties, and calibrated countersignature thresholds are presumptively required for all transactions and changes to system configuration relevant to the assurance subject. Validators shall have full and timely access to ledgers, sub-ledgers, reconciliations, bank statements, contracts, SLAs, DPAs, procurement dossiers, and system logs necessary to reach a conclusion, except where restricted by mandatory law or court order. In such cases, lawful redaction or access in camera may be applied by reasoned and time-limited resolution, with sufficient alternative procedures conducted to avoid scope limitation.

1.6 Publication as a Control. Assurance outputs are subject to publication with lawful redaction of personal data, security-sensitive information, and privileged legal advice. Where publication could defeat ongoing investigations or procurement fairness, a time-limited postponement may be applied by reasoned resolution with a defined review date. Executive summaries shall be published contemporaneously unless lawfully deferred. All exceptions, redactions, and deferrals are logged, justified, and sunset-reviewed.

1.7 Interfaces and Reliance. This Protocol interfaces with the Unified MEL Framework for indicator validation, with the ESG Safeguards Framework for E&S compliance checks, and with the Legal Instruments Compendium for rights of access and survival clauses. It also interfaces with the Flowhub Trio Plus Operating Manual for custody controls and with the Eligibility and Project Leasing Framework for Hosted Ownership verification. Reliance may be placed on qualified external work (e.g., statutory audits or accredited certifications) where independence, scope, and methods meet GSIA equivalence; otherwise, supplementary procedures are required.

1.8 Data Protection and Sovereignty. The controller/processor allocation is determined in the governing instrument for the subject matter. Typically, the GSIA SCE or the competent Member authority acts as controller; GSIA AB and its vendors act as processors. DPIAs are mandatory for reviews involving large-scale personal data, cross-border transfers, special categories of data, or sensitive operational logs. Access is executed under least-privilege IAM, with multi-factor authentication, immutable logs, key management, and encryption aligned to sector standards. Where sovereignty constraints apply, evidence handling and storage locations shall be localised or escrowed to comply with national law while preserving verifiability.

1.9 Domestication Linkage. Assurance findings explicitly reference domestication gates. Shadowing and dual-key stages emphasise control design and operating effectiveness; lead-role and handover stages emphasise sustainability, staffing, legal localisation, and system stewardship. Readiness certification requires an unqualified or acceptably qualified assurance conclusion over core controls, data governance, and fiduciary propriety. Any residual non-conformities must be tracked to closure with deadlines and responsible owners.

1.10 Hosted Ownership Safeguards. Where Hosted Ownership is deployed, assurance must verify title lists, non-attachment, negative pledge, discrete ledgers and bank accounts, reversion covenant mechanics, and survival of audit rights post-handover. No private distribution of value is permissible beyond agreed service consideration. Deviations are sanctionable and trigger remedial actions, including step-in by GSIA SCE under the Charter.

Chapter 2 — Peer Review Panels and Methodology

2.1 Mandate and Composition. Peer Review Panels are constituted by resolution of the GSIA SCE Assurance and Standards Committee to provide independent, expert scrutiny of programmes, institutional controls, and key decisions. Panels are designed to be multidisciplinary, drawing from domains including fiduciary controls, MEL and statistics, procurement integrity, information security and data protection, ESG safeguards, sectoral expertise relevant to the project, and public law. Members serve under letters of appointment specifying term, scope, confidentiality, conflicts regime, and publication duties. GSIA Holding AB proposes methodological standards and maintains the reviewer registry; it does not appoint Panels. GSIA AB has no appointment power and shall not influence composition.

2.2 Eligibility, Conflicts, and Recusal. Panelists must meet fit-and-proper criteria, demonstrate recent, relevant expertise, and sign conflict-of-interest disclosures covering financial, professional, and relational interests within a three-year lookback. A standing recusal protocol applies where a reasonable, informed observer would apprehend bias. The Panel Chair, elected by the Panel at its inaugural session, rules on recusals subject to appeal to the SCE Committee. Any breach of the conflicts regime is grounds for removal and possible sanctions under the Compliance, Audit, and Ethics Code.

2.3 Authority Matrix and Interfaces. The Panel's authority extends to requesting documents, interviewing personnel, inspecting systems and logs, and commissioning specialist testing within approved budgets. It reports to the SCE Committee, not to management. It interfaces with Internal Audit for coordination of testing to avoid duplication, with External Audit for reliance and cross-referencing, with the MEL function for data verification, and with the ESG and Procurement Integrity units for targeted probes. Where the subject matter overlaps an ongoing investigation, the Panel coordinates with the Ethics and Investigations function to preserve evidential integrity.

2.4 Methodological Framework. Panels adopt a transparent, documented methodology anchored in the following elements: scoping and risk-based prioritisation; hypothesis formulation; evidence planning; sampling strategy; test execution; analysis and triangulation; conclusion and grading; management response; and follow-up verification. Methods are proportionate to risk and materiality and must be replicable. Use of statistical sampling shall specify confidence levels, tolerable misstatement, and population definitions. Where qualitative assessments are necessary (e.g., governance culture, decision quality), the Panel shall define criteria and rating scales ex ante and apply inter-rater calibration to minimise subjectivity.

2.5 Evidence Standards and Chain-of-Custody. Evidence must be sufficient and appropriate, with provenance recorded. Electronic evidence requires immutable logging, timestamp synchronisation, and preservation of original formats with cryptographic hashes. Interviews are documented with date, participants, purpose, and key statements; recordings require informed consent and lawful basis. Where access is restricted by law or privilege, the Panel shall seek alternative procedures without compromising independence. Any scope limitation is disclosed, its effect evaluated, and, if necessary, the opinion is modified.

2.6 Grading and Opinions. The Panel issues one of the following overall opinions, supplemented by domain-specific ratings: Unqualified (no material non-conformities); Qualified (material non-conformities present but remediable without undermining objectives); Adverse (pervasive non-conformities undermining objectives); or Disclaimer (insufficient evidence due to scope limitation). Each opinion is accompanied by a reasoned narrative, evidence references, and a corrective

action plan with owners and timelines. Grades feed into tranche decisions, domestication gates, and risk registers.

2.7 Sampling and Triggers. Routine peer reviews follow an annual cycle defined by the SCE Committee, with increased frequency for high-risk portfolios, transition phases (e.g., dual-key to lead-role), and pre-handover readiness. Ad-hoc reviews may be triggered by KRIs, whistleblower reports, procurement anomalies, data protection incidents, significant control failures, or sanctions alerts. In Hosted Ownership, at least one deep-dive review shall be conducted prior to each major financing tranche and prior to title reversion.

2.8 Interaction with Management and Rights of Reply. GSIA AB and relevant Member authorities shall provide timely access and designate liaisons. A draft report is provided for factual accuracy checks, limited to correcting errors and supplying missing evidence, without editorial control over opinions or grades. The right of reply is time-bound; failure to respond does not delay issuance unless essential to avoid material misstatement. Management responses are annexed, and agreed corrective actions are tracked to closure.

2.9 Publication and Redaction Protocol. Final Panel reports, executive summaries, and management action plans are published in accordance with the publication doctrine. Redactions are lawful, narrowly tailored, and time-limited, with a register of redactions maintained for sunset review. Where publication is deferred for procurement integrity or investigation sensitivity, a notice of deferral stating reasons and review date is issued. Panel datasets that include personal data or security-sensitive artefacts are not published; instead, methodological summaries and non-sensitive aggregates are disclosed.

2.10 Data Protection, DPIAs, and Security. For reviews involving personal data or sensitive operational logs, a DPIA shall be completed before fieldwork. Access is governed by least-privilege IAM with multi-factor authentication. Transfers follow controller-approved mechanisms and localisation requirements. Encryption is enforced in transit and at rest; de-identification or pseudonymisation is applied where feasible. Access logs are preserved and independently reviewed. Any data incident detected during review is escalated per the Compliance, Audit, and Ethics Code and reported to the controller within statutory timelines.

2.11 Domestication Alignment. Panel methodologies explicitly test domestication gates. At shadowing, the emphasis is on design adequacy; at dual-key, on joint operating effectiveness; at lead-role, on Member stewardship capacity; at system handover, on documentation completeness and key transfer; at legal localisation, on registration, contracting capacity, and statutory compliance; and at readiness certification, on sustained performance and governance resilience. Findings inform the readiness certificate and any conditions subsequent.

2.12 Hosted Ownership Verification. Where Hosted Ownership applies, the Panel verifies ring-fenced accounts, discrete ledgers, negative pledge compliance, non-attachment to unrelated liabilities, escrow arrangements, title registers, reversion triggers, and survival clauses for audit and records. Any finding suggesting leakage, private distribution, or encumbrance contrary to the no-distribution rule triggers immediate notification to the SCE Committee and provisional protective measures, including payment holds and enhanced monitoring.

2.13 Records, Archiving, and Survivals. Panel workpapers, evidence indexes, correspondence, and decision logs are archived in secure repositories under GSIA Holding AB's stewardship standards and retained for the longer of Charter requirements, statutory periods, or financing covenants. Survivals

include confidentiality, data protection, IP in methods and templates, and audit rights. De-identification schedules are applied where appropriate post-retention.

2.14 Interface to Downstream Chapters. Publication and transparency rules (Chapter 3), rectification and appeals (Chapter 4), and accreditation of validators (Chapter 5) will further detail the doctrines referenced herein, including sanctions for non-cooperation, appeals standards, and accreditation maintenance. Cross-references to Document 10 (stress testing), Document 11 (compliance and ethics), and Document 12 (digital trust) will be operationalised in those instruments without derogating from this Protocol.

Chapter 3 — Publication and Transparency Rules

3.1 Purpose and Constitutional Standing. Publication is a core assurance control that enables verifiability, deters misconduct, and sustains public trust. The GSIA SCE mandates publication of independent assurance outputs and related records, subject only to lawful redaction and time-limited deferrals adopted by reasoned resolution. The GSIA Holding AB maintains canonical templates, taxonomies, and registers for disclosure; GSIA AB, Member authorities, and Hosted Ownership SPVs cooperate fully and without delay.

3.2 Scope of Disclosure. The following materials are presumptively disclosable: executive summaries of reviews; full Panel reports with annexes where lawful; management responses and corrective action plans; grades and conclusions; methodology summaries; and the status of actions to closure. For Hosted Ownership, title registers and escrow summaries are disclosable in form suitable to protect security and commercial sensitivities, with bank identifiers, serial numbers, and security configurations redacted in accordance with lawful necessity.

3.3 Authority Matrix and Countersignature. Publication decisions involving redaction or deferral require four-eyes control and segregation of duties. As a minimum: the Secretariat of the GSIA SCE originates the publication act; the Data Protection Officer confirms lawfulness of personal data handling; Legal confirms privilege and litigation risk; the Chief Information Security Officer (or equivalent) confirms security sensitivities; and the Assurance and Standards Committee (or its delegated officer) issues the reasoned, time-limited resolution. Countersignature thresholds are calibrated by risk and materiality and are recorded in the publication register.

3.4 Redaction Doctrine. Redaction is lawful only to the minimum extent necessary to protect personal data, procurement integrity, security-sensitive information, trade secrets lawfully protected, or privileged legal advice. Redactions are bracketed, reasoned, and time-limited. A redaction key is maintained under seal for audit and sunset review. Where feasible, de-identification or pseudonymisation is preferred over omission. Redactions shall not defeat the intelligibility of findings and reasons.

3.5 Deferral and Sunset Review. Deferral of publication is exceptional, reasoned, and time-limited. Permissible grounds include: protection of ongoing procurement processes; non-interference with active investigations; compliance with a binding court order; and protection of critical infrastructure and system security. Each deferral resolution specifies scope, reasons, a review date, and the responsible officer. On expiry, publication proceeds or deferral is renewed by fresh reasoned resolution; serial deferrals require escalation to the GSIA SCE Board.

3.6 Transparency Registers. The Secretariat maintains: a Publication Register (issued items and dates); a Redaction Register (grounds, scope, duration, approving officers); a Deferral Register (reasons, review

dates, outcomes); a Conflicts and Recusal Register (Panel composition, recusals, replacements, reasons); and an Access Log to disclosure repositories. These registers are themselves published with lawful redaction and updated on a rolling basis.

3.7 Format, Integrity, and Accessibility. Published materials are digitally signed, time-stamped, and accompanied by cryptographic hashes to assure integrity. Executive summaries are provided in accessible formats. Methodology synopses and non-sensitive data aggregates may be provided in machine-readable form to support secondary scrutiny. Any translations are identified as non-canonical; the authoritative language is specified by resolution. Accessibility standards apply to ensure public comprehension without sacrificing legal precision.

3.8 Data-Protection Controls. Controller/processor roles are confirmed for each publication act. Where the GSIA SCE or a Member authority is controller, GSIA AB and vendors act strictly as processors under a DPA. DPIAs are required where publication involves large-scale personal data, cross-border transfers, special categories of data, or sensitive operational logs. IAM enforces least-privilege; logs are immutable and subject to internal audit review. Encryption is enforced in transit and at rest to sector standards.

3.9 Hosted Ownership Transparency. For Hosted Ownership portfolios, publication includes a summary of the ring-fenced perimeter, the negative pledge and non-attachment clauses, the reversion mechanics, and the existence of discrete ledgers and bank accounts. Sensitive identifiers may be redacted, but the existence, scope, and operational separation must be intelligible. Prior to title reversion, a readiness summary referencing domestication gates is published; upon reversion, a transfer notice and inventory reconciliation are published with lawful redaction.

3.10 Interlocks with Other Instruments. Publication provisions are read alongside: the Unified MEL Framework for indicator disclosure; the ESG Safeguards Framework for grievance handling disclosures; the Legal Instruments Compendium for survival of audit, access, and publication rights; the Flowhub Trio Plus Manual for custody-related transparency; and the Compliance, Audit, and Ethics Code for whistleblower protection and investigation integrity. No clause herein negates statutory reporting duties under mandatory national public law.

3.11 Survivals and Archiving. Publication records, underlying workpapers, approval resolutions, and registers are archived in secure repositories according to the longer of Charter requirements, statutory periods, or financing covenants. Survivals include confidentiality, data-protection obligations, intellectual property in templates and methods, and audit rights. De-identification schedules are applied post-retention as appropriate.

Chapter 4 — Rectification and Appeals Process

4.1 Purpose and Principles. This Chapter establishes binding procedures for correcting non-conformities identified by external validation and peer review and for adjudicating appeals. The process is guided by legality, proportionality, timeliness, transparency, and non-retaliation. Publication remains a control; exceptions are reasoned, time-limited, and recorded.

4.2 Classification of Findings and Deadlines. Findings are classified by materiality and risk to programme objectives, fiduciary propriety, data protection, or domestication trajectory. Class A findings (material or systemic) require immediate protective measures and a corrective action plan within thirty calendar days, with implementation milestones agreed by resolution. Class B findings (significant but not systemic) require a plan within forty-five days. Class C findings (minor) require

remediation tracking without formal plan unless escalated by recurrence. Timelines may be adjusted by reasoned resolution where mandatory law, force majeure, or sovereignty constraints apply.

4.3 Corrective Action Plans and Ownership. Management prepares a corrective action plan that specifies the remedy, responsible owner, resourcing, controls affected, evidence of completion, and proposed verification method. Plans must align with the segregation of duties and four-eyes doctrine and must not weaken existing controls absent a reasoned risk-based justification. For Hosted Ownership, plans must confirm preservation of ring-fencing, negative pledge, non-attachment, and reversion covenants. The Panel or the SCE Assurance and Standards Committee approves the plan and assigns verification responsibility to Internal Audit, an independent validator, or the Panel itself.

4.4 Interim Protective Measures. For Class A findings, the SCE Committee may impose interim measures, including payment holds, enhanced monitoring, restricted authority matrices, temporary step-in over specified processes, or suspension of tranche disbursements. In Hosted Ownership cases, escrow triggers and step-in rights may be activated to prevent leakage or encumbrance. Interim measures are reasoned, proportionate, and time-limited, subject to periodic review.

4.5 Verification and Closure. Closure requires independent verification against pre-agreed evidentiary standards and sampling plans. Evidence must be sufficient and appropriate, with chain-of-custody preserved. Where verification reveals partial remediation, a revised timeline may be set with tightened monitoring; repeated slippage escalates to sanctions under the Compliance, Audit, and Ethics Code. Closure decisions, with reasons and evidence references, are recorded and published with lawful redaction.

4.6 Effects on Domestication and Financing. Material unremedied findings suspend progression through domestication gates and may defer readiness certification, tranche releases, or title reversion. Conversely, verified remediation may restore progression. Decisions are reasoned, documented, and subject to appeal as provided herein.

4.7 Reconsideration (Factual Accuracy). Before an appeal on the merits, a time-bound reconsideration window is provided to correct factual errors or submit overlooked evidence. The Panel issues a memorandum addressing each point raised, revising findings if warranted. Reconsideration does not delay interim protective measures unless a stay is granted by reasoned resolution.

4.8 Appeals Body and Jurisdiction. Appeals on the merits lie to an **Appeals Board** constituted by the GSIA SCE and independent of the originating Panel. The Board comprises senior experts in fiduciary controls, MEL, law, and data protection, none of whom served on the original Panel. Its jurisdiction includes challenges to grades, conclusions, material procedures, and imposed measures. Appeals must be filed within twenty business days of publication of the final report or reconsideration memorandum, stating grounds and relief sought.

4.9 Grounds and Standard of Review. Valid grounds include: material error of fact; material error of method; material procedural irregularity causing prejudice; or disproportionality of imposed measures. The standard of review is reasonableness and procedural fairness, not de novo re-trial, save where the Board determines that the original process was pervasively defective or that new, decisive evidence could not reasonably have been presented earlier.

4.10 Procedure and Evidence. The Appellant bears the burden to demonstrate grounds. The Board may request additional documents, conduct hearings, or commission targeted re-testing. Data-protection rules apply; DPIAs are conducted where necessary. Hearings, if any, are recorded; transcripts are

archived. The Board issues a reasoned decision within forty business days of a complete appeal, subject to extension by reasoned resolution.

4.11 Remedies and Outcomes. The Board may uphold the original decision; modify grades or findings; remit specific matters for further testing; adjust or lift interim measures; or substitute a proportionate remedy. Where sanctions are implicated, the Board's decision interfaces with the Sanctions Grid and Enforcement regime in the Compliance, Audit, and Ethics Code, without pre-empting outcomes reserved to that instrument.

4.12 Publication of Appeals and Rectifications. Appeals submissions, schedules, decisions, and resulting corrective actions are published with lawful redaction. Deferrals for investigation sensitivity or procurement integrity follow the doctrine in Chapter 3, with notice of deferral and review date. A consolidated "Rectification and Appeals Docket" is maintained and updated.

4.13 Interface with Dispute Resolution and Law. Nothing in this Chapter displaces contractual dispute resolution mechanisms in Implementation Agreements, SLAs, or Leasing Schedules. Where a Member State invokes dispute provisions under the Legal Instruments Compendium, those procedures apply in parallel; duplication is avoided by coordination orders issued by the SCE Secretariat. Mandatory national public law, including audit and reporting duties, prevails in its lawful domain.

4.14 Protections and Non-Retaliation. Individuals cooperating with reviews, rectifications, or appeals are protected from retaliation under the Compliance, Audit, and Ethics Code and applicable law. Allegations of interference, intimidation, or retaliation are investigated under established protocols and may independently ground sanctions.

4.15 Records, Survivals, and Learning. All rectification and appeals records, including plans, verifications, decisions, and evidence indexes, are archived under stewardship standards and retained for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data protection, IP in methods, and audit rights. A periodic "Lessons and Methods Circular" is issued by GSIA Holding AB to update standards and training content based on anonymised patterns of findings and appeals outcomes.

Chapter 5 — Accreditation of Validators

Preamble and Applicability. This Chapter is issued under the GSIA Charter and shall be read consistently with Documents 00–08 and Chapters 1–4 of this Protocol. It establishes the authority, standards, processes, and survivals for accrediting third-party validators and peer reviewers who undertake independent assurance for GSIA-mandated programmes operated through GSIA AB under SLA or, where applicable, through Hosted Ownership SPVs. The prevalence order previously affirmed remains in force. Publication is treated as a control, with lawful redaction and reasoned, time-limited exceptions. Data-protection roles, fiduciary controls, and domestication gates apply throughout.

5.1 Accreditation Authority and Separation of Functions. The GSIA SCE, acting through its Assurance and Standards Committee, is the sole authority to grant, renew, suspend, or withdraw accreditation. GSIA Holding AB maintains the canonical standards, competency frameworks, examination instruments, registries, and quality-assurance methods, without involvement in live accreditation decisions. GSIA AB and any SPV under Hosted Ownership have no role in conferring accreditation and shall not influence outcomes.

5.2 Eligibility and Fit-and-Proper Criteria. Applicants must demonstrate institutional independence, financial soundness, robust quality systems, and competence proportional to the requested scope (fiduciary, MEL/statistics, procurement integrity, information security and data protection, ESG safeguards, sectoral expertise). Individual lead reviewers must satisfy fit-and-proper requirements including professional qualifications, minimum years of relevant practice, clean disciplinary history, and absence of conflicts per Chapter 2. Independence requires no managerial responsibility, financial interest, or decision-making influence over the prospective assurance subject within a three-year lookback, or longer where required by law.

5.3 Scope of Accreditation and Modularity. Accreditation is modular, specifying domains (e.g., fiduciary controls; MEL verification; ESG compliance; data-protection audits; procurement integrity; sectoral technical validation), permissible methods, and geographic coverage. Scopes may be expanded or narrowed by reasoned resolution following demonstrated competence or identified deficiencies.

5.4 Application Dossier and Verification. Applicants submit a dossier comprising governance documents, ownership and beneficial interest disclosures, quality-assurance manuals, staff competency matrices, sample workpapers and reports, insurance certificates where applicable, data-protection and security controls, and declarations of conflicts. The Secretariat verifies submissions, conducts reference checks, and may commission on-site or remote assessments. Misrepresentation or omission is grounds for refusal or later withdrawal.

5.5 Examinations, Trials, and Equivalence. Accreditation may require passing written examinations, practical case assessments, or supervised pilot engagements. Equivalence recognition for other accreditations or certifications may be granted by reasoned resolution where standards are demonstrably aligned and independence safeguards are equivalent; residual gaps trigger supplementary conditions. Equivalence never waives GSIA publication, data-protection, or domestication requirements.

5.6 Terms, Renewal, and Continuing Professional Development. Accreditation is granted for a fixed term, ordinarily three years, and is renewable upon evidence of sustained competence, quality results, and adherence to publication and ethics requirements. Accredited institutions shall maintain a continuing professional development programme aligned to GSIA standards. Material changes in ownership, governance, key personnel, or control systems must be notified within thirty days and may trigger interim review.

5.7 Quality Reviews and Performance Grading. Accredited validators are subject to periodic quality reviews by GSIA Holding AB's quality team under standards approved by the SCE Committee. Reviews assess methodological rigour, sufficiency and appropriateness of evidence, documentation quality, independence safeguards, data-protection compliance, and timeliness. A performance grade is issued with corrective actions, deadlines, and follow-up verification. Repeated or material deficiencies may suspend access to high-risk assignments, reduce scope, or trigger suspension or withdrawal.

5.8 Conflicts, Recusal, and Rotation. Accredited validators must operate a documented conflicts regime with mandatory disclosures at engagement acceptance and prior to report issuance, and a standing recusal protocol. Lead reviewers rotate off a specific Member or portfolio after a maximum consecutive tenure defined by resolution to preserve independence. Exceptions are reasoned and time-limited, recorded in the Conflicts and Recusal Register, and disclosed in reports.

5.9 Data-Protection and Security Obligations. Accredited validators act as processors under a DPA when processing personal data controlled by the GSIA SCE or a Member authority. Where validators

collect personal data as independent controllers (e.g., for recruitment or internal QA), such processing is strictly segregated. DPIAs are mandatory for high-risk assignments. Validators enforce least-privilege IAM, multi-factor authentication for privileged access, immutable logs, encryption in transit and at rest, and secure evidence repositories. Breaches are reportable within statutory timelines and under GSIA incident protocols.

5.10 Hosted Ownership Safeguards. Validators assigned to Hosted Ownership engagements must demonstrate competence in verifying ring-fencing, non-attachment, negative pledge compliance, discrete ledgers and bank accounts, and reversion mechanics. Evidence handling must respect sovereign localisation rules while preserving verifiability. Findings on leakage or encumbrance contrary to the no-distribution rule are escalated immediately to the SCE Committee.

5.11 Publication and Registers. Accreditation decisions, scopes, current status, performance grades, and any sanctions are published with lawful redaction. The Secretariat maintains an Accreditation Register, a Sanctions and Conditions Register, and a calendar of validity and renewal dates. Deferrals or redactions follow Chapter 3's doctrine and are time-limited with sunset review.

5.12 Sanctions, Suspension, and Withdrawal. Grounds include loss of independence, material quality failures, breach of data-protection obligations, misrepresentation, non-cooperation, or unethical conduct. Sanctions are proportionate and may include warning, conditions, scope reduction, suspension, or withdrawal. Interim protective measures may restrict assignment types pending final decision. Decisions are reasoned, published with lawful redaction, and subject to appeal under Chapter 4.

5.13 Appeals and Due Process. Applicants or accredited entities may appeal refusals, sanctions, suspensions, or withdrawals to the Appeals Board established under Chapter 4. The standard of review is reasonableness and procedural fairness. Remedies include confirmation, modification, or remittal for further review. Publication follows Chapter 3.

5.14 Records, Survivals, and Learning. Accreditation dossiers, quality review workpapers, decisions, and correspondence are archived per Charter, statutory, or covenant periods, whichever is longer. Survivals include confidentiality, data-protection obligations, IP in standards and instruments, and audit rights. GSIA Holding AB issues periodic anonymised circulars to improve methods and training based on accreditation review insights.