NOVEMBER 5, 2025

COMPLIANCE, AUDIT, AND ETHICS CODE

CODIFYING GOVERNANCE STANDARDS THROUGH RIGOROUS AUDIT, ETHICAL OVERSIGHT, AND ISO-ALIGNED CERTIFICATION

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

Compliance, Audit, and Ethics Code

Preamble and Applicability

Preamble. This Code is promulgated under the GSIA Charter and shall be read consistently with Documents 00–10 and the prevalence order previously affirmed. Mandatory national public law prevails within its lawful domain, followed by the GSIA Charter, this Code, and downstream instruments and annexes. The GSIA constitutional logic remains binding: the **GSIA SCE** holds the public mandate, membership, and oversight; GSIA Holding AB exercises stewardship over standards, intellectual property, and canonical methods; GSIA AB performs operations exclusively under Service Level Agreements; and, where necessary, Hosted Ownership may be executed through EUSL or other GSIA-approved SPVs to achieve bankability and continuity within a ring-fenced perimeter and with an explicit, binding reversion covenant to the Member upon readiness, without any private distribution of value beyond agreed service consideration.

Publication functions as a control. Disclosure is presumptive, subject only to lawful redaction and time-limited deferral by reasoned resolution recorded in the publication register. Fiduciary integrity is ensured by four-eyes approvals, segregation of duties, calibrated countersignature thresholds, discrete ledgers and bank accounts, and negative pledge and non-attachment clauses. Data-protection and digital trust controls apply at all times: controller/processor allocations are explicit per instrument; DPIAs are triggered for high-risk processing; identity and access management enforces least-privilege and multi-factor authentication; logs are immutable and time-synchronised; encryption is applied in transit and at rest. Domestication follows gated progression—shadowing, dual-key, lead-role, system handover, legal localisation, and readiness certification—tested by independent assurance and external validation pursuant to Document 09. Nothing herein derogates Hosted Ownership safeguards or the no-distribution rule.

Chapter 1 — Internal Audit Framework

1.1 Mandate and Independence. Internal Audit is established by resolution of the GSIA SCE Board as an independent, objective assurance and advisory function providing reasonable assurance on governance, risk management, control, and compliance across GSIA-mandated programmes, GSIA AB operations under SLA, GSIA Holding AB stewardship processes relevant to standards and IP, and, where applicable, Hosted Ownership SPVs. Internal Audit has unrestricted access to records, systems, premises, personnel, and decision forums necessary to fulfil its mandate, except where limited by mandatory law; in such cases, lawful in-camera access or alternative procedures shall be authorised by reasoned, time-limited resolution. Internal Audit reports functionally to the SCE Audit and Ethics Committee and administratively to the SCE Secretary-General or equivalent officer. GSIA AB management has no authority to constrain scope, timing, or reporting.

1.2 Scope and Audit Universe. The audit universe encompasses the enterprise, programmes, projects, funds, processes, systems, and third-party arrangements material to public-interest outcomes. Coverage includes fiduciary controls (treasury, payments, procurement, asset management), financial reporting and disclosures, compliance with the Charter and Instruments Compendium, ESG safeguards and grievance mechanisms, MEL data governance and indicator integrity, data protection and security, business continuity and disaster recovery, counterparty onboarding and surveillance, Hosted Ownership ring-fencing and reversion mechanics, domestication gate readiness, and publication

doctrine execution. Special reviews may be commissioned by the SCE Committee in response to key risk indicator breaches, whistleblower reports, significant incidents, or transition milestones.

1.3 Standards and Methods. Internal Audit operates under the GSIA Internal Audit Standards maintained by GSIA Holding AB and adopted by SCE resolution. Methods are risk-based, evidence-centric, and replicable, with explicit planning, scoping, materiality thresholds, hypothesis formulation, sampling, testing, analysis, grading, and follow-up. Workpapers document procedures performed, evidence obtained, conclusions reached, and linkages to findings. Evidence integrity is preserved by chain-of-custody records, timestamp synchronisation, and cryptographic hashes for electronic artefacts. Use of automated tools and analytics is documented and validated; models are explainable and bias-tested where relevant.

1.4 Risk-Based Plan and Authority Matrix. An annual risk-based audit plan is prepared with reference to the enterprise risk taxonomy (Document 17), programme risk registers, KRIs, funding tranches, domestication stages, and Hosted Ownership exposures. The plan is approved by the SCE Audit and Ethics Committee and may be revised by reasoned resolution upon trigger events. Authority matrices enforce internal independence: planning and scoping are owned by Internal Audit; access is facilitated by management but not conditioned by it; four-eyes and segregation of duties apply to audit approvals and report issuance.

1.5 Reporting, Grading, and Publication. Internal Audit issues reports with reasoned narratives, sufficient references to evidence, and gradings of findings by materiality and systemic impact. Management responses and time-bound corrective action plans are appended. Reports are published with lawful redaction; deferrals for investigation or procurement integrity are exceptional, reasoned, time-limited, and entered in the deferral register with a sunset review date. Executive summaries are ordinarily published contemporaneously.

1.6 Follow-Up, Rectification, and Escalation. Corrective actions are tracked to closure against pre-agreed evidentiary standards. Persistent slippage, repeated significant findings, or unremedied material non-conformities trigger escalation to the SCE Audit and Ethics Committee and, where warranted, to the Sanctions Grid and Enforcement regime. Where risks threaten tranche releases, domestication progression, or title reversion, the Committee may impose interim protective measures, including tightened authority matrices, payment holds, or step-in over specified processes, proportionate and time-limited.

1.7 Coordination with External Assurance and Oversight. Internal Audit coordinates with External Audit (Chapter 2) for reliance on controls testing and to avoid duplication, with independent validators and Peer Review Panels under Document 09, with the Compliance Investigations function for integrity matters, with the MEL function for indicator verification coordination, and with the ESG and Procurement Integrity units for targeted probes. Reliance is documented and contingent on independence and method equivalence; otherwise, supplementary procedures are performed.

1.8 Data-Protection, Security, and Sovereignty. Where Internal Audit processes personal data or sensitive logs controlled by the GSIA SCE or a Member authority, it acts as a processor under a DPA. DPIAs are mandatory for high-risk audits, especially those involving cross-border transfers or special category data. IAM enforces least-privilege with multi-factor authentication; access and activity logs are immutable and reviewed independently. Encryption is mandatory in transit and at rest. Where sovereignty constraints require localisation, evidence repositories and archives are hosted accordingly, with escrowed integrity artefacts to preserve verifiability.

1.9 Hosted Ownership Safeguards. Audits of Hosted Ownership verify ring-fenced accounts and ledgers, negative pledge and non-attachment compliance, asset registers and title lists, escrow arrangements, cash waterfalls, and reversion covenant mechanics. Any indication of leakage, encumbrance, or private distribution contrary to governing instruments triggers immediate notification to the SCE Audit and Ethics Committee and protective measures. Audit rights and access survive handover as stipulated in the Legal Instruments Compendium.

1.10 Quality Assurance and Improvement. Internal Audit maintains a documented quality assurance and improvement programme, including supervisory reviews, periodic internal assessments, peer quality reviews by GSIA Holding AB's standards unit, and at least triennial independent external assessments commissioned by the SCE Committee. Results, improvement actions, and implementation status are reported to the SCE Committee and published with lawful redaction.

1.11 Records, Survivals, and Confidential Reporting. Workpapers, evidence indexes, approvals, and correspondence are archived securely for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, IP in templates and methods, and audit rights. A confidential reporting channel to Internal Audit is maintained for staff and partners to flag control failures without fear of retaliation, interfacing with the Ethics Hotline for investigations as set out in Chapter 3 of this Code.

Chapter 2 — External Audit Standards

2.1 Appointment and Independence. External Auditors are appointed by the GSIA SCE General Assembly or Board on recommendation of the Audit and Ethics Committee, following open, competitive procurement or a justified single-source process where mandated by law. Appointment letters and engagement terms enshrine independence in fact and appearance, rotation of key audit partners within prescribed terms, and prohibitions on non-audit services that may impair independence. External Auditors report to the SCE Audit and Ethics Committee; GSIA AB management has no authority to constrain scope, timing, or reporting.

2.2 Scope of Audit and Opinions. External Audit covers, as applicable, the statutory financial statements of the GSIA SCE, consolidated or combined statements where required, GSIA AB and GSIA Holding AB (as needed for group assurance), and special-purpose financial statements or agreed-upon procedures for programmes, projects, funds, and Hosted Ownership portfolios. The scope includes evaluation of financial reporting frameworks, internal control over financial reporting, compliance with negative pledge and non-attachment clauses in Hosted Ownership, and, where mandated, limited assurance on selected non-financial disclosures that are material to public-interest outcomes. Opinions may be unmodified, qualified, adverse, or disclaimers, supported by Key Audit Matters where applicable.

2.3 Group and Component Auditor Coordination. Where component auditors are engaged for subsidiaries, SPVs, or geographically dispersed operations, the Group Auditor issues instructions, evaluates competence and independence, reviews component work, and performs additional procedures where risks are significant. Materiality is set at group and component levels with qualitative overlays for public-interest and fiduciary considerations. Reliance on component work is documented and proportionate to assessed risk.

2.4 Materiality and Risk Assessment. Materiality considers quantitative benchmarks and qualitative factors, including potential impact on Member decisions, tranche logic, domestication gates, Hosted Ownership reversion, and public trust. Risk assessment incorporates enterprise and programme risk

registers, prior audit findings, internal audit results, KRIs, stress testing outputs (Document 10), and IT general controls as delineated in Document 12.

2.5 Access, Evidence, and IT Controls. External Auditors have unrestricted access to records, systems, premises, and personnel necessary to obtain sufficient appropriate evidence, subject to mandatory legal constraints managed via in-camera access or lawful alternative procedures authorised by reasoned resolution. IT general controls over identity and access, change management, operations, and data integrity are tested where relevant to the audit. Use of automated tools, data analytics, and CAATs is documented and validated; populations and sampling frames are preserved with integrity artefacts.

2.6 Hosted Ownership Assertions. For Hosted Ownership portfolios, External Auditors evaluate assertions that project assets and cash are ring-fenced in discrete ledgers and bank accounts; that negative pledge and non-attachment clauses are effective; that title registers and escrow constructs are accurate; and that no private distribution of value has occurred beyond agreed service consideration. Deviations are reported as findings and may result in modified opinions or emphasis paragraphs, with immediate notification to the SCE Audit and Ethics Committee.

2.7 Fraud, Non-Compliance, and Sanctions Considerations. External Auditors design procedures responsive to risks of material misstatement due to fraud or non-compliance with laws and regulations, including procurement integrity, sanctions, and anti-corruption controls. Suspected or identified instances are communicated promptly to the SCE Audit and Ethics Committee and to the Compliance Investigations function for action under the Sanctions Grid, without prejudicing legal obligations to report to competent authorities where applicable.

2.8 Communication with Those Charged with Governance. External Auditors communicate the planned scope and timing, significant risks, significant findings, uncorrected misstatements and their effect, significant deficiencies in internal control, independence confirmations, and qualitative aspects of accounting practices. Management letters include recommendations, management responses, and timelines. Communications are documented and preserved; summaries are published with lawful redaction pursuant to the publication doctrine.

2.9 Publication and Transparency. Audited financial statements, audit opinions, and management letter summaries are published, subject to lawful redaction of sensitive identifiers or security-sensitive content. Deferrals for market sensitivity or investigation integrity are reasoned, time-limited, and recorded in the deferral register with a sunset review. The authoritative version is digitally signed and time-stamped; any translations are identified as non-canonical.

2.10 Data-Protection, Sovereignty, and DPIAs. Where External Audit involves processing of personal data or sensitive operational logs, the GSIA SCE or Member authority ordinarily acts as controller and the External Auditor as an independent controller for audit evidence; where processing is conducted on behalf of the controller, a DPA is executed. DPIAs are required for high-risk processing or cross-border transfers. Evidence repositories must enforce encryption in transit and at rest, least-privilege IAM with multi-factor authentication, immutable logging, and retention aligned to statutory and Charter requirements. Sovereignty constraints are respected through evidence localisation or escrow while preserving auditability.

2.11 Coordination with Internal Audit and Validators. External Auditors consider the work of Internal Audit for risk assessment and potential reliance, evaluate Internal Audit's objectivity and competence, and determine the extent of use. They also review outputs of independent validation and Peer Review

Panels (Document 09) for context and risk cues, without abdicating their own evidence responsibilities. Coordination avoids duplication and reduces burden while maintaining independence.

2.12 Going Concern and Contingencies. External Auditors evaluate the appropriateness of going concern assumptions for entities and programmes within scope, considering liquidity buffers, stress testing results, contingent liabilities, and the availability of funding tranches subject to domestication or other conditions. Where material uncertainty exists, adequate disclosure is required; otherwise, a modified opinion or emphasis paragraph may be warranted.

2.13 Records, Survivals, and Quality. Audit documentation is retained by the External Auditor for statutory periods and at least the Charter minimum, whichever is longer. Survivals include confidentiality, data-protection obligations, access rights for regulator-mandated inspections, and publication registers. External Auditors are subject to quality reviews by their professional regulators and may be requested to participate in GSIA post-engagement reviews; summaries are published with lawful redaction.

2.14 Dispute Resolution and Appeals Interface. Disagreements regarding access, scope limitations, or publication are escalated to the SCE Audit and Ethics Committee for resolution and, where necessary, to the Appeals Board under Document 09 Chapter 4. Contractual dispute mechanisms in engagement letters and the Legal Instruments Compendium apply in parallel, coordinated to avoid duplication.

Chapter 3 — Ethics Hotline and Investigations

3.1 Mandate and Scope. The Ethics Hotline and Investigations function is established by resolution of the GSIA SCE as an independent mechanism to receive, triage, and investigate allegations of misconduct, including fraud and corruption, collusion and coercive practices, obstruction, data-protection and cybersecurity breaches, procurement integrity violations, conflicts of interest, retaliation, and other breaches of the Charter, this Code, or applicable law. Its jurisdiction extends to GSIA SCE organs for oversight purposes, GSIA AB and its contractors under SLA, GSIA Holding AB processes where relevant to stewardship and standards, and Hosted Ownership SPVs within their ring-fenced perimeters. Nothing herein limits mandatory reporting to competent national authorities.

3.2 Confidential Reporting Channels and Accessibility. Multiple reporting channels are maintained to ensure accessibility and confidentiality: secure web intake with end-to-end encryption; dedicated telephone lines with call-masking; a monitored postal route; and in-person reporting to designated Ethics Officers. Anonymous reporting is permitted where lawful and practically verifiable. All channels display clear notices on scope, protections, and data-protection information. Accessibility accommodations are ensured for language, disability, and field contexts.

3.3 Protection and Non-Retaliation. Non-retaliation is categorical. Any adverse action, threat, or intimidation against reporting persons, witnesses, or cooperating staff constitutes a Class A violation under Chapter 4. Protective measures may include confidentiality shields, reassignments, access restrictions for implicated parties, and interim relief. Allegations of retaliation are prioritised and investigated expeditiously. Protections apply irrespective of investigation outcomes, provided the report was made in good faith.

3.4 Intake, Triage, and Case Registration. All reports are timestamped, assigned a unique case identifier, and entered into a secure case-management system with immutable logging. Triage occurs within defined timelines, ordinarily ten business days, to assess jurisdiction, plausibility, materiality, and immediate risk to people, assets, evidence, or public interest. Cases are categorised for

investigation, referral to management for administrative handling, cross-referral to Internal Audit or the MEL or ESG functions, or closure with reasons. Triage records and reasons are preserved for audit and publication with lawful redaction.

3.5 Independence, Conflicts, and Recusal. Investigations are conducted by personnel independent of line management over the subject matter. A formal conflicts check precedes case assignment; investigators, counsel, and subject-matter experts with actual or perceived conflicts recuse and are replaced. The Head of Investigations reports functionally to the SCE Audit and Ethics Committee and administratively to the SCE Secretariat; GSIA AB management has no authority to constrain scope, timing, or reporting.

3.6 Investigation Planning and Standard of Proof. Each case proceeds under a written plan setting out allegations, legal and policy bases, issues to prove, evidentiary sources, methods, and anticipated timelines. The standard of proof is the balance of probabilities for administrative determinations; where sanctions with disqualification or debarment are contemplated, a clear and convincing evidence standard is applied. Criminal thresholds and referrals to national authorities are evaluated under applicable law without prejudicing administrative proceedings.

3.7 Evidence Handling and Digital Forensics. Evidence collection preserves authenticity and integrity. Electronic artefacts are acquired using forensically sound methods; hash values, acquisition logs, and chain-of-custody records are maintained. Physical evidence is sealed, logged, and stored securely. Access to evidence repositories is governed by least-privilege IAM with multi-factor authentication; logs are immutable and time-synchronised. Data minimisation is applied, and privileged legal materials are segregated.

3.8 Interviews and Procedural Fairness. Interviews are conducted under a documented protocol, with identity verification, lawful basis, and process explanations given. Interviewees may be accompanied by a support person where lawful and practicable. Notes or recordings (with informed consent where required) are retained, indexed, and cross-referenced to the case file. Subjects of investigation are given an opportunity to respond to material allegations prior to conclusion, unless doing so would compromise urgent protective measures or a parallel criminal inquiry; any such deferral is reasoned, time-limited, and recorded.

3.9 Interim Protective Measures. Where credible risk to people, assets, evidence, or public interest is identified, interim measures may be imposed by reasoned resolution: preservation holds, payment holds, access suspensions, enhanced monitoring, temporary reassignment, or step-in over specified processes. Measures are proportionate, time-limited, and subject to periodic review. For Hosted Ownership, escrow triggers and perimeter locks may be activated to prevent leakage or encumbrance, consistent with negative pledge and non-attachment.

3.10 Data-Protection Roles, DPIAs, and Sovereignty. The controller for investigation data is ordinarily the GSIA SCE or, where agreed and lawful, the competent Member authority. The Investigations function and engaged vendors act as processors under a DPA. DPIAs are mandatory for high-risk investigations, especially those involving special category data, cross-border transfers, or extensive system log analysis. Localisation and sovereignty constraints are respected through in-country processing or escrow arrangements while preserving verifiability and chain-of-custody.

3.11 Coordination with Internal/External Audit, Validators, and Authorities. Coordination protocols ensure de-confliction with Internal Audit, External Audit, Peer Review Panels, and independent validators under Document 09. Where allegations implicate criminal conduct, corruption, or sanctions

offences, referrals to competent authorities are made consistent with law, with preservation of evidence and cooperation duties. Engagement with authorities does not extinguish GSIA's administrative investigation or sanctions mandate.

3.12 Reporting, Publication, and Registers. At conclusion, a reasoned investigation report sets out findings of fact, analysis, conclusions, and recommendations, with appendices of evidence indexes and procedural history. Reports are provided to the SCE Audit and Ethics Committee and to affected Member authorities as appropriate. Publication follows the doctrine that disclosure is a control: executive summaries and outcomes are presumptively published with lawful redaction of personal data, security-sensitive information, and privileged legal advice; deferrals are reasoned, time-limited, and entered in the deferral register. A consolidated Investigations Register records case identifiers, allegations, outcomes, sanctions referrals, publications, redactions, and deferrals.

3.13 Domestication and Hosted Ownership Alignment. At shadowing, Member personnel observe hotline and investigation processes; at dual-key, joint intake review and protective-measure approvals apply; at lead-role and handover, Members assume primary responsibility under local law, with GSIA oversight until readiness certification. Legal localisation of hotline channels, confidentiality and witness protections, data localisation, and publication practices is completed as a domestication gate. In Hosted Ownership, investigation authority includes step-in over the ring-fenced perimeter; the reversion covenant and survival clauses ensure audit and access rights continue post-handover for defined periods.

3.14 Records, Survivals, and Organisational Learning. Case files, evidence repositories, decision logs, sanctions referrals, and publication records are archived securely for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, audit and access rights, IP in methods and templates, and publication registers. GSIA Holding AB issues anonymised Lessons and Methods Circulars to update standards, training, and accreditation requirements based on patterns of allegations, control failures, and outcomes.

Chapter 4 — Sanctions Grid and Enforcement

4.1 Purpose and Principles. This Chapter establishes a binding, proportionate, and predictable sanctions regime to deter and remediate misconduct, protect public interest, and preserve fiduciary integrity. Enforcement adheres to legality, reasonableness, proportionality, consistency, transparency with lawful redaction, timeliness, the right to be heard, and non-retaliation. Sanctions do not derogate mandatory national public law and operate in parallel with contractual remedies and legal proceedings.

4.2 Taxonomy of Violations. Violations are categorised by conduct and gravity, including administrative non-compliance with controls or reporting duties; negligent breach of fiduciary controls; reckless misconduct jeopardising assets, data, or public interest; wilful misconduct; fraud, corruption, embezzlement, collusion, coercive or obstructive practices; procurement integrity violations including bid-rigging and conflicts concealment; data-protection breaches including unlawful processing, unauthorised disclosure, or security failures; sanctions and export-control violations; retaliation against whistleblowers or witnesses; and failure to cooperate with assurance, investigations, or audits. Repeated lesser violations may aggregate to a higher tier.

4.3 Sanction Types and Ranges. Sanctions range from written warning with mandatory remedial training; performance improvement and corrective action plans; formal reprimand; restitution, disgorgement, or clawback of undue gains; temporary suspension of duties, authorities, or access; reassignment or demotion; financial penalties where contractually authorised; termination of

employment or contract for cause; portfolio-level restrictions, including payment holds and authority matrix tightening; suspension or termination of participation in programmes; disqualification of individuals from GSIA-mandated roles; debarment of entities from GSIA-financed procurements for defined terms; step-in over specified processes; and referral to competent authorities. For Hosted Ownership, escrow activation and perimeter locks are available protective measures and may accompany sanctions.

4.4 Aggravating and Mitigating Factors. Sanction calibration considers aggravating factors such as leadership involvement, concealment, coercion or retaliation, systemic harm, beneficiary harm, recurrence, and obstruction of investigations; and mitigating factors such as self-reporting, cooperation, prompt remediation, restitution, limited impact, and credible compliance improvements. Past conduct, training records, and role criticality are relevant. Reasoned decisions document factors considered and their weight.

4.5 Procedures and Due Process. Prior to sanction, the subject receives written notice of alleged violations, evidence basis, and proposed sanctions, with a time-bound opportunity to respond and present exculpatory or mitigating evidence. Hearings may be held where proportionate. The standard of proof is balance of probabilities, or clear and convincing evidence for disqualification or debarment. Decisions are made by the SCE Audit and Ethics Committee or its designated Sanctions Panel under an authority matrix preserving independence and four-eyes approval. Interim protective measures may be imposed where necessary without prejudicing the right to be heard.

4.6 Enforcement Across Entities and Counterparties. Sanctions apply to staff, consultants, suppliers, implementing partners, and financial counterparties subject to GSIA jurisdiction or contractual privity. Cross-entity enforcement within the GSIA ecosystem is enabled through reciprocal recognition of sanctions decisions, subject to reasonableness review. Debarment decisions may be notified to relevant public authorities and development partners consistent with law and cooperation agreements, with lawful redaction.

4.7 Financial Remedies and Value Protection. Restitution, disgorgement, and clawback are pursued to restore project value; amounts recovered are credited to the ring-fenced perimeter or to Member-designated public accounts. No private distribution of recovered value is permitted. Set-off may be applied against amounts otherwise payable under contracts, subject to law and due process. Insurance recoveries and subrogation are pursued where applicable, without impeding criminal or administrative proceedings.

4.8 Impact on Domestication, Tranches, and Hosted Ownership. Material violations may suspend progression through domestication gates, defer readiness certification, and trigger tranche holds. In Hosted Ownership, credible evidence of leakage, encumbrance, or private distribution triggers immediate protective measures, including payment freezes, escrow activation, and step-in, pending investigation and adjudication. Reversion to the Member proceeds when readiness is achieved and material violations are remedied or bounded by enforceable conditions subsequent.

4.9 Publication, Registers, and Rehabilitation. Sanctions decisions are published with lawful redaction, including the nature of violation, sanctioned party (subject to privacy and security considerations), sanction type and duration, and any conditions. A Sanctions Register is maintained and updated; deferrals are reasoned, time-limited, and sunset-reviewed. Rehabilitation is available upon evidence of sustained compliance improvements, restitution where applicable, and successful completion of conditions. Early termination or reduction of sanctions is by reasoned resolution and published.

4.10 Appeals and Interface with Investigations and Audit. Sanctioned parties may appeal to the Appeals Board under Document 09, Chapter 4, within prescribed timelines, stating grounds such as material error of fact or method, procedural irregularity, or disproportionality. Appeals do not automatically stay protective measures; a stay may be granted by reasoned resolution where risk permits. Internal Audit may validate remediation; the Investigations function retains jurisdiction over new evidence or retaliation allegations.

4.11 Data-Protection and Sovereignty in Enforcement. Sanctions processing that involves personal data is conducted under explicit controller/processor allocations and DPAs. DPIAs are conducted for high-risk processing or cross-border transfers. Publication balances transparency and privacy through lawful redaction and de-identification where feasible. Where national law mandates secrecy or restricts disclosures, publication deferrals are time-limited and entered in the deferral register, with the narrowest possible scope.

4.12 Records, Survivals, and Monitoring. Sanctions case files, decisions, evidence indexes, publication and deferral records, and monitoring reports are archived for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, audit and access rights, and publication registers. Compliance with sanctions conditions is monitored and reported periodically; non-compliance triggers escalation and may result in reinstatement or enhancement of sanctions.

Chapter 5 — ISO Alignment and Certification

Preamble to Chapter 5. This Chapter is issued under the GSIA Charter and shall be read consistently with Documents 00–10 and Chapters 1–4 of this Code. It codifies alignment with international management system standards and the method for attaining and maintaining third-party certifications as instruments of assurance, discipline, and public trust. The prevalence order previously affirmed remains in force. Publication is treated as a control, with lawful redaction and reasoned, time-limited deferrals recorded in the publication register. Data-protection roles (controller/processor), DPIA triggers, IAM, immutable logs, and encryption apply. Domestication gates and readiness certification are preserved. Hosted Ownership remains ring-fenced, subject to non-attachment, negative pledge, discrete ledgers and bank accounts, and a reversion covenant with no private distribution of value.

5.1 Purpose and Constitutional Position. ISO alignment and accredited certifications are adopted to operationalise the Charter's requirements for governance, fiduciary controls, security, quality, and environmental and social safeguards. Certifications do not substitute for GSIA standards but provide externally verifiable evidence that core controls and processes operate to recognised international benchmarks. The GSIA SCE sets certification policy by resolution; GSIA Holding AB maintains canonical mappings between GSIA controls and relevant ISO clauses; GSIA AB executes implementation under SLA without authority to dilute scope; and Hosted Ownership SPVs apply the same standards within their ring-fenced perimeter.

5.2 Scope of Alignment. GSIA aligns, at minimum and as relevant, to the following management system families as mapped by GSIA Holding AB: information security (ISO/IEC 27001 and aligned 27002 controls for technical measures), privacy information management (ISO/IEC 27701), business continuity (ISO 22301), quality management (ISO 9001) for service delivery under SLAs, anti-bribery management (ISO 37001) in procurement and contracting, compliance management (ISO 37301), and, as context requires, asset management (ISO 55001) and IT service management (ISO/IEC 20000-1). ESG-related standards are integrated through Document 06; alignment here ensures coherence, not duplication.

5.3 Separation of Functions and Independence. GSIA Holding AB maintains the control-to-clause mapping, model policies, procedures, and record templates, and curates a library of objective evidence exemplars. It does not perform internal audits for certification purposes. Internal Audit (Document 11, Chapter 1) tests design and operating effectiveness of aligned controls; External Certification Bodies conduct certification audits. GSIA AB implements and operates controls under SLA; management shall not influence scoping or findings of internal or external audits.

5.4 Integrated Management System (IMS). An Integrated Management System is established to avoid siloed compliance and to ensure single-source control ownership, cross-referenced procedures, unified risk registers, and consolidated corrective and preventive action (CAPA) tracking. The IMS incorporates policy architecture, control catalogues, procedures and work instructions, records matrices, training curricula, and management review protocols, with cross-walks to the Legal Instruments Compendium and Flowhub Trio Plus doctrine.

5.5 Certification Strategy and Phasing. Certification is phased by materiality and risk. Information security and business continuity are prioritised for platforms hosting MEL, treasury, identity, and evidence repositories; anti-bribery and compliance management are prioritised for procurement and contracting; privacy is prioritised where personal data processing is integral to programme delivery. Hosted Ownership environments may achieve scoped certifications covering the ring-fenced perimeter, with sovereign constraints addressed through localised controls and evidence repositories.

5.6 Evidence, Records, and Publication. Objective evidence is preserved contemporaneously: risk assessments, DPIAs, statements of applicability, asset inventories, access reviews, training records, incident logs, internal audit reports, management reviews, corrective actions, and test results. Certification scopes, audit summaries, nonconformities and corrective actions, and certificate validity data are published with lawful redaction; deferrals for security sensitivity are reasoned, time-limited, and recorded.

5.7 Internal Audit and Management Review. Internal Audit plans incorporate ISO-aligned control testing to support readiness and surveillance. Management reviews are held at least annually, evaluating performance against objectives, incidents, CAPA status, risk and opportunity changes, resource adequacy, and improvement decisions. Records of reviews are preserved and feed the Publication Register in summary form.

5.8 Corrective Actions and Sanctions Interface. Nonconformities identified by internal or external audits generate CAPAs with owners, timelines, and verification methods. Failure to implement CAPAs within agreed timelines, or recurrence indicating systemic weakness, escalates under the Sanctions Grid (Chapter 4) and may temporarily limit authority matrices or trigger step-in for specific processes until remediation is verified.

5.9 Data-Protection and Sovereignty Considerations. For ISO/IEC 27001 and 27701 implementations, controller/processor roles are codified; DPIAs and records of processing activities are integrated into the IMS. Where sovereignty constraints require evidence localisation, certification bodies are provided in-country access or escrowed evidence under confidentiality and non-disclosure, preserving auditability. Encryption, key management, and immutable logging operate as baseline controls.

5.10 Domestication and Readiness. At shadowing, Member personnel are trained on IMS structure; at dual-key, they participate in internal control operation and audit preparation; at lead-role, they co-chair management reviews; at handover, the IMS segment is transferred, localised to national law, and

subjected to a readiness verification; readiness certification may rely on valid external certificates and unqualified internal audit conclusions over core domains.

5.11 Certification Bodies and Due Diligence. External certification bodies are accredited by recognised national accreditation bodies and vetted under counterparty standards for independence, competence, sanctions screening, and quality. Engagement letters preserve access, publication, and confidentiality doctrines. Findings are reasoned and published with lawful redaction; surveillance and recertification cycles are planned and funded.

5.12 Records, Survivals, and Continuous Improvement. IMS records, audit evidence, decisions, and certificates are archived for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, IP in mappings and templates, and audit rights. GSIA Holding AB issues periodic updates to mappings and model controls, reflecting lessons learned, new threats, and standards revisions; change logs are published.