NOVEMBER 8, 2025

COMPLIANCE, AUDIT, AND ETHICS CODE

THREE -LINES OVERSIGHT: INTERNAL AUDIT, EXTERNAL ASSURANCE, WHISTLEBLOWING AND INVESTIGATIONS, SANCTIONS, AND ISO -ALIGNED COMPLIANCE ARCHITECTURE WITH PUBLIC DISCLOSURE

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

Compliance, Audit, and Ethics Code

Preamble

This Code constitutes the binding compliance, assurance, and ethics instrument for GSEA custodial bodies and their implementing counterpart (SLUC), including Components and programmes conducted under DESA, PCPP, and PCGG. It preserves the separation-of-functions doctrine established under Agenda 2074 by allocating implementation to SLUC and independent oversight to GSEA structures and external validators. The Code is harmonised with the OECD Guidelines for Multinational Enterprises (2023 Update), the UN Guiding Principles on Business & Human Rights (UNGPs), the IIA Global Internal Audit Standards (IPPF), COSO Internal Control—Integrated Framework, and external assurance comparators such as IAASB ISAs and ISAE 3000 (Revised). Where personal data are implicated, the Code requires compliance with GDPR.

Chapter 1 — Internal Audit Framework

1.1 Mandate and Independence.

Internal Audit (IA) is established as an independent, objective assurance and advisory function that reports functionally to the Audit & Risk Committee of the GSEA Board and administratively to the GSEA Secretariat, in accordance with the IIA Global Internal Audit Standards and the IIA Three Lines Model. IA shall have unrestricted access to records, personnel, and physical assets necessary to discharge its mandate.

1.2 Scope and Risk-Based Planning.

IA covers governance, risk management, and control across all entities and programmes, including ESG safeguards implementation, fiduciary controls, procurement integrity, digital governance, information security, and MEL reliability. An annual, risk-based plan is prepared using a documented universe and risk assessment aligned with COSO and approved by the Audit & Risk Committee.

1.3 Method and Coordination.

IA engagements follow generally accepted internal auditing practices and coordinate with second-line functions (Compliance, Safeguards, MEL) to avoid duplication while preserving independence. Where external auditors rely on internal audit work or vice versa, coordination shall follow applicable guidance to protect objectivity and quality.

1.3 Quality and Professionalism.

IA maintains a Quality Assurance and Improvement Program (QAIP) with ongoing monitoring, periodic internal assessment, and an external assessment at least every five years, as required by the IIA Standards. Staff competence is supported through continuing professional development and relevant certifications.

1.4 Reporting and Follow-Up.

IA issues reports with graded findings, risk implications, and time-bound management actions. Management responses are tracked to closure, with overdue high-risk actions escalated to the Audit & Risk Committee.

Chapter 2 — External Audit Standards

2.1 Financial Statements and Going Concern.

Annual financial statements of GSEA and SLUC entities shall be audited in accordance with the International Standards on Auditing (ISAs) issued by the IAASB, including evaluation of going concern (ISA 570) and key audit matters where applicable. Independence follows the IESBA International Code of Ethics.

2.2 Non-Financial and ESG Assurance.

Assurance over non-financial disclosures—including safeguards, MEL indicators, and sustainability metrics—is performed under **ISAE 3000 (Revised)**; where greenhouse-gas statements are assured, **ISAE 3410** may be applied. Public-sector funds (where applicable) may be reviewed with reference to **INTOSAI** pronouncements.

2.3 IT and Cybersecurity Certifications.

Where certification audits are pursued for information security or business continuity, these shall be conducted by accredited bodies under **ISO/IEC 17021-1**, against **ISO/IEC 27001** (ISMS) and **ISO 22301** (BCMS).

2.4 Deliverables and Transparency.

External auditors provide an opinion, management letter, and, where applicable, assurance statements on non-financial information. Public disclosure follows Agenda 2074 transparency and the publication norms referenced in Document 09.

Chapter 3 — Ethics Hotline and Investigations

The Group shall maintain a confidential, multi-channel Ethics Hotline and a formal investigations function to surface, assess, and resolve allegations of misconduct across all entities and programme streams, including SLUC and its Components. The Hotline is designed to be accessible to employees, contractors, beneficiaries, suppliers, and the public, with protections against retaliation consonant with the remedy and non-retaliation expectations of the UN Guiding Principles on Business & Human Rights (UNGPs) and the truthful-communication and remediation ethos of the OECD Guidelines for Multinational Enterprises (2023 Update) (UNGPs; OECD Guidelines 2023). The operating model adheres to best-practice whistleblowing standards under ISO 37002 – Whistleblowing Management Systems and embeds compliance governance pursuant to ISO 37301 – Compliance Management Systems (ISO 37002; ISO 37301).

Reports may be lodged in named or anonymous form via secure web intake, telephone, or in-person channels. Personally identifiable information and case evidence are processed under a strict need-to-know regime and protected in accordance with GDPR and the Group’s ISMS/Privacy extensions under ISO/IEC 27001 and ISO/IEC 27701 (GDPR; ISO/IEC 27001; ISO/IEC 27701). Intake includes immediate triage to classify alleged violations (e.g., fraud, corruption, procurement collusion, GBV/SEAH, human-rights risks, data-protection incidents), followed by assignment to an investigator independent of implicated functions. Conflicts of interest are screened and documented; case leadership is transferred where independence could be impaired.

Investigations follow a documented protocol: plan and scope definition; evidence preservation and chain-of-custody; interviews using trauma-informed techniques where GBV/SEAH is alleged; analysis and findings; and a reasoned conclusion with recommended actions. GBV/SEAH cases employ survivor-centred, confidential handling aligned with MDB good practice and UNGPs non-retaliation principles. Where allegations involve environmental and social safeguard breaches or fiduciary risks, investigators coordinate with second-line functions without compromising independence, and promptly notify external funders where required by contract. All cases are tracked to closure with time-bound management actions; substantiated cases lead to sanctions under Chapter 4, control remediation, and disclosure in aggregated annual ethics reports. Case files are retained per legal-hold rules and GDPR-compliant schedules.

Chapter 4 — Sanctions Grid and Enforcement

Enforcement measures shall be applied consistently, proportionately, and with due process. The Sanctions Grid establishes calibrated consequences for individuals, suppliers, and member organisations, taking account of intent, materiality, recurrence, cooperation, remediation, and self-disclosure. Disciplinary measures for personnel span written warnings, suspension, reassignment, demotion, and termination for cause. Organisational measures include remediation orders, enhanced monitoring, financial clawbacks, suspension or termination of membership or eligibility, and, for suppliers or grantees, contract termination and debarment for defined periods. Publication of sanctions shall follow transparency rules while observing legitimate confidentiality and safety constraints, consistent with OECD Guidelines (2023) disclosure expectations and the transparency ethos reflected in the World Bank Access to Information Policy (OECD Guidelines 2023; World Bank ATI).

Vendor and partner sanctions mirror leading development-finance practices; where appropriate, the Group may recognise or coordinate with multilateral sanctions regimes, drawing on the comparators of the World Bank Sanctions System and peer MDB frameworks (World Bank Sanctions). All enforcement decisions are reasoned and documented; respondents are afforded the right to be heard and to appeal under Document 09. Corrective-action plans are mandatory for reinstatement or probation and shall address root causes, control redesign, training, and independent verification. Enforcement data are analysed annually to identify systemic risks and to update the Grid.

Chapter 5 — ISO Alignment and Certification

SLUC and GSEA shall operate an integrated management-system architecture designed for certifiability and continuous improvement across compliance, anti-bribery, information security, privacy, and business continuity domains. The governing intention is to maintain demonstrable conformance to certifiable standards where proportionate, and to publish statements of applicability, certification scopes, and surveillance outcomes pursuant to Agenda 2074 transparency.

The compliance backbone is an ISO-aligned system that maps policy, risk, control, and assurance layers to ISO 37301 (Compliance Management Systems) and embeds a whistleblowing subsystem aligned with ISO 37002. Anti-bribery controls are formalised to the level required by ISO 37001, including risk assessment, due diligence, financial and non-financial control integration, and case-management pathways. Information-security governance is implemented through an ISO/IEC 27001-conformant ISMS, with domain controls referencing ISO/IEC 27002, cloud control guidance from ISO/IEC 27017, and public-cloud PII processing safeguards under ISO/IEC 27018. Privacy management extends the ISMS with ISO/IEC 27701, thereby operationalising GDPR’s accountability principle within a certifiable management-system construct. To preserve public-purpose continuity, critical operations, facilities, and supplier interfaces are governed by a Business Continuity Management System conformant with ISO 22301. Where appropriate, risk-management design principles are drawn from ISO 31000, and sustainable-procurement practices from ISO 20400 to reinforce ethical supply-chain stewardship.

Certification audits shall be performed by accredited certification bodies operating under ISO/IEC 17021-1, with cross-recognition preferences for signatories to the IAF MLA and ILAC MRA to ensure international acceptance. Multi-site sampling and risk-based scoping will be used to reflect SLUC's regional footprint; high-materiality processes (procurement, privileged IT operations, grievance and investigations) shall be included in every certification and surveillance cycle. Statements of applicability, nonconformity registers, corrective-action plans, and surveillance-visit summaries shall be maintained and disclosed in public summaries consistent with Agenda 2074's transparency code.

Supply-chain assurance will require tier-1 vendors supporting critical services to evidence relevant certifications (27001/27701/22301 or sectoral equivalents) or to accept contractual audit rights and remediation schedules. Where certification is not proportionate, SLUC will apply targeted control attestations and independent limited-assurance engagements under ISAE 3000 (Revised); greenhouse-gas assertions, when material, may be assured against ISAE 3410.