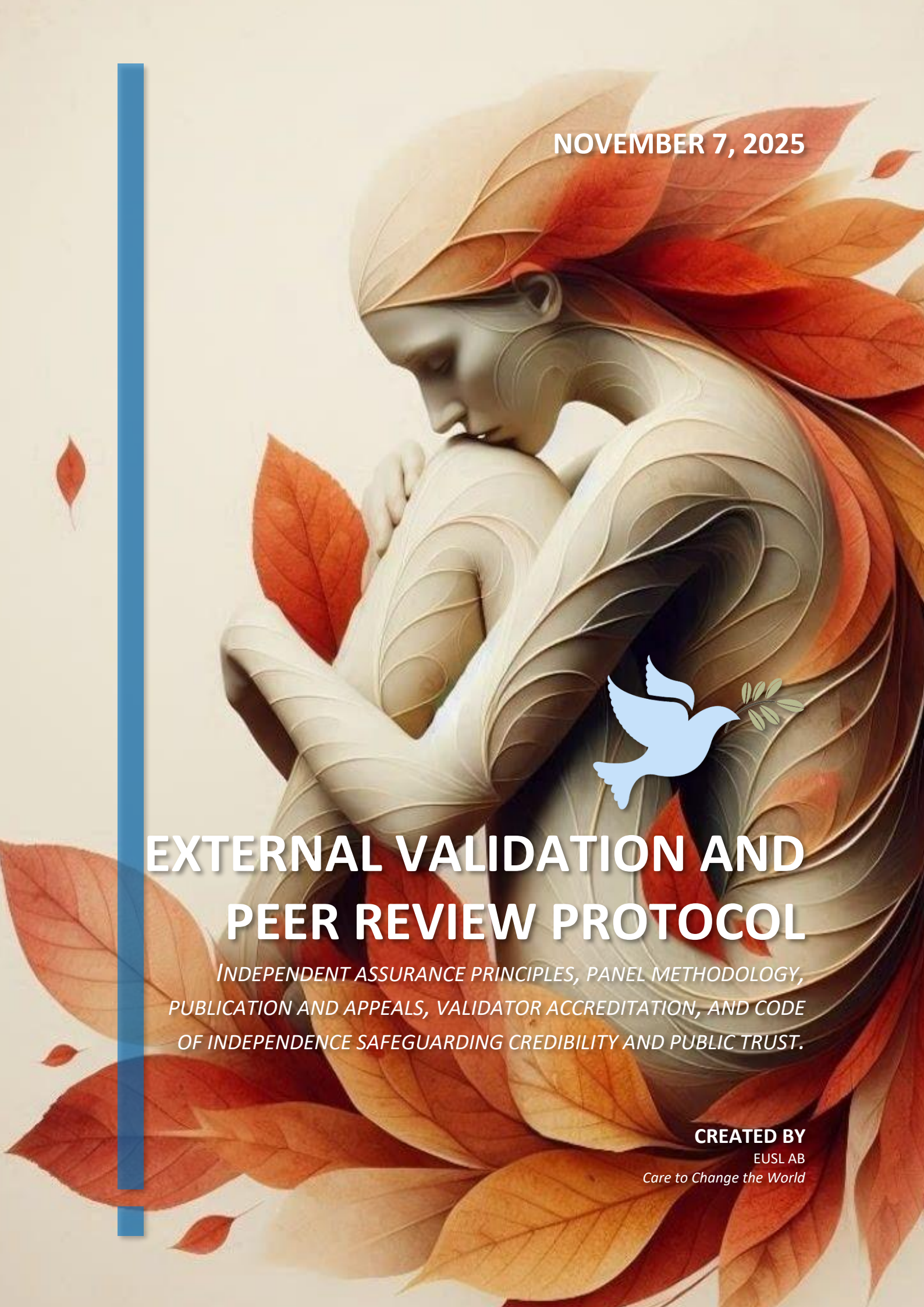

NOVEMBER 7, 2025

EXTERNAL VALIDATION AND PEER REVIEW PROTOCOL

INDEPENDENT ASSURANCE PRINCIPLES, PANEL METHODOLOGY, PUBLICATION AND APPEALS, VALIDATOR ACCREDITATION, AND CODE OF INDEPENDENCE SAFEGUARDING CREDIBILITY AND PUBLIC TRUST.

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

Chapter 1 — Independent Assurance Principles 2

Chapter 2 — Peer Review Panels and Methodology 3

Chapter 3 — Publication and Transparency Rules 4

Chapter 4 — Rectification and Appeals Process 5

Chapter 5 — Accreditation of Validators 6

Chapter 6 — Code of Independence and Professional Conduct 7

External Validation and Peer Review Protocol

Preamble

This Protocol constitutes the binding standard for independent external validation and peer review of programmes implemented through SLUC and its Components (DESA, PCPP, PCGG), as well as associated academic and research outputs governed by UCE/UACE. It operationalises the separation-of-functions doctrine under Agenda 2074 by locating assurance outside implementation chains while preserving lawful access to information and stakeholder participation. The Protocol is harmonised with internationally recognised norms for responsible conduct and safeguards—namely the OECD Guidelines for Multinational Enterprises (2023 Update, the UN Guiding Principles on Business & Human Rights, the World Bank Environmental and Social Framework, and the IFC Performance Standards. Evaluation quality and disclosure align with the OECD DAC Evaluation Criteriaand the World Bank Access to Information Policy. Assurance practice draws from ISAE 3000 (Revised) for non-financial assurance engagements with audit conduct informed by ISO 19011 and competence/independence principles reflected in ISO/IEC 17029. Where personal data are processed, the Protocol requires compliance with GDPR; for scholarly peer review, it references COPE guidance and, in higher-education QA contexts, the ESG – Standards and Guidelines for Quality Assurance in the EHEA.

This instrument applies to all validations commissioned by GSEA or SLUC and to peer reviews convened for research and academic outputs. It shall be incorporated by reference into procurement packages, grant conditions, and membership covenants that foresee external assurance.

Chapter 1 — Independent Assurance Principles

1.1 Purpose and Scope.

External validation provides independent, evidence-based assurance over (i) MEL indicators and results claims; (ii) compliance with environmental, social, and gender/inclusion safeguards; (iii) fiduciary controls and procurement integrity; and (iv) the effectiveness of grievance-redress mechanisms, as cross-referenced in Document 06 and Document 08. The scope shall be proportionate to risk and materiality, informed by **OECD DAC** criteria on relevance, effectiveness, efficiency, sustainability, and equity and calibrated to ESF/IFC comparators for safeguards equivalency.

1.2 Independence and Impartiality.

Assurance providers must meet organisational and financial independence standards equivalent to ISAE 3000 (Revised) and ISO/IEC 17029, including the absence of advisory roles in the subject engagement within the prior twenty-four months, and prohibition on contingent-fee arrangements. Individuals shall disclose all actual or perceived conflicts, with enforced recusals and cooling-off rules. Independence is further protected through appointment by GSEA (or its delegated panel secretariat), not by the delivery unit under review.

1.3 Competence and Due Professional Care.

Panels shall collectively demonstrate expertise in MEL, safeguards (ESF/IFC), fiduciary controls, sectoral domains (e.g., digitalisation, TVET, agriculture), and local legal/cultural contexts. Due care requires sufficient, appropriate evidence and documentation consistent with ISO 19011 and the assurance standards cited.

1.4 Proportionality, Materiality, and Levels of Assurance.
Work programmes shall be risk-based, with clear materiality thresholds. Levels of assurance are defined as limited or reasonable per ISAE 3000 (Revised), declared explicitly in the assurance statement together with scope limitations.

1.5 Rights to be Heard and Procedural Fairness.
Auditees are afforded a documented factual-accuracy check on draft findings; affected stakeholders must have safe opportunities to contribute evidence consistent with ESF ESS10 and IFC PS1 engagement principles. The Protocol adopts non-retaliation and remedy expectations under the UNGPs.

1.6 Confidentiality, Data Protection, and Ethics.
Evidence handling complies with GDPR and minimisation principles; sensitive testimonies (e.g., GBV/SEAH) are processed under enhanced protections. All panel members sign confidentiality and data-processing undertakings. For scholarly peer review, ethical conduct follows COPE standards.

1.7 Transparency and Public Interest.
Assurance statements, management responses, and time-bound corrective-action plans shall be published through SLUC's transparency portal, observing legitimate confidentiality and safety constraints, and aligned to the World Bank Access to Information Policy spirit. Summaries must state scope, methods, limitations, level of assurance, and key findings.

1.8 Remedies, Sanctions, and Follow-Up.
Material non-conformities trigger corrective actions and, where warranted, sanctions as set out in Document 06. Validation follow-up verifies closure of actions and feeds into Agenda 2074 public reporting. Persistent deficiencies may trigger re-validation or thematic audit.

Chapter 2 — Peer Review Panels and Methodology

2.1 Panel Constitution and Governance.
Peer review is conducted by a Panel constituted for each assignment with: a Chair (process integrity and timeliness), a Rapporteur (methods and documentation), and domain experts covering MEL, safeguards, fiduciary, and sector specialisms. Where academic outputs are reviewed, a scholarly editor and an ethics advisor join the Panel. Diversity of gender, geography, and discipline is required to reduce bias, consistent with OECD Guidelines (2023) expectations on inclusive governance.

2.2 Eligibility, Rotation, and Cooling-Off.
Members must meet competence criteria and independence rules (no involvement in design, financing, or delivery of the subject within the prior twenty-four months). Rotation applies after two consecutive assignments in the same geography or programme stream. These safeguards mirror independence tenets in ISAE 3000 (Revised) and conformity guidance in ISO/IEC 17029.

2.3 Methodological Framework.
Panels prepare a Validation and Review Plan setting objectives, evidence tests, sampling frames, and analytical methods. Mixed-methods and triangulation are mandatory: document review, key-informant interviews, focus groups, site verification, data re-performance/recalculation, and control testing. Stakeholder engagement follows ESF ESS10/IFC PS1; safeguards testing maps directly to ESS/PS requirements (e.g., ESS2/PS2 labour, ESS4/PS4 community health and safety.

2.4 Sampling and Evidence Sufficiency.
Sampling is risk-based and documented, with minimum coverage thresholds for high-risk activities. Evidence sufficiency/appropriateness is assessed in line with ISAE 3000 (Revised) criteria; limitations and sampling risk are disclosed.

2.5 Thematic Protocols.
For fiduciary reviews, Panels test segregation of duties, reconciliations, procurement integrity, and anomaly detection against control designs described in Document 06, and benchmark liquidity/FX practices to Basel references as relevant. For digitalisation, privacy/security controls are assessed against GDPR and ISO/IEC 27001/27701. For AI-enabled components, Panels test governance against the OECD AI Principles. For academic outputs, peer-review ethics and editorial standards follow COPE; where higher-education QA is implicated, Panels reference ESG.

2.6 Findings, Ratings, and Evidence Records.
Findings are graded (Compliant; Minor Non-Conformity; Major Non-Conformity; Not Applicable) with explicit evidence citations and risk implications. Evidence records (workpapers) are retained per GDPR-compliant schedules. Draft reports undergo factual-accuracy checks by auditees and a limited right-of-reply by affected stakeholders through safe channels consistent with UNGPs non-retaliation.

2.7 Deliverables and Publication.
The Panel issues (i) a full Validation/Peer Review Report; (ii) a Public Assurance Statement specifying level of assurance; and (iii) a Management Letter with corrective-action recommendations and timeframes. Publication follows the transparency provisions referenced in the Preamble and the World Bank Access to Information comparators.

2.8 Interface with Component-Level MEL.
Each Component (DESA, PCPP, PCGG) maintains its own MEL; Panels verify interoperability with the Unified MEL Framework (Document 08), comparability of indicators, and the fidelity of aggregation into Agenda 2074 reporting.

Chapter 3 — Publication and Transparency Rules

3.1 Normative Basis and Public-Interest Imperative.
Publication of validation and peer review outputs is a mandatory transparency obligation under Agenda 2074 and shall be executed in alignment with the principles of World Bank Access to Information Policy ( ), the disclosure expectations of OECD Guidelines for Multinational Enterprises (2023) ( ), and the participatory flow provisions codified in Agenda 2074 Chapters 5–6.

3.2 Scope of Disclosure.
The following documents shall be disclosed through SLUC's transparency portal:

- **Public Assurance Statement:** Summarising scope, methodology, level of assurance (limited or reasonable), and key findings.
- **Management Response and Corrective Action Plan:** Including timelines and responsible entities.
- **Validation Report Summary:** A non-technical digest accessible to stakeholders, translated into relevant local languages.

Full technical reports may be disclosed subject to confidentiality and safety constraints, with sensitive data (e.g., GBV/SEAH cases, proprietary technology) redacted.

3.3 Format and Accessibility.
All disclosures shall be:

- Machine-readable and compliant with open-data principles (FAIR and CARE frameworks).

- Accessible to persons with disabilities and available in multilingual formats.
- Indexed with persistent identifiers (e.g., DOI) for scholarly outputs, consistent with open-science norms.

3.4 Timing and Frequency.

- **Initial Publication:** Within 30 days of validation report approval.
- **Follow-Up Updates:** Quarterly status reports on corrective actions until closure.
- **Annual Consolidated Disclosure:** Aggregated summaries of all validations conducted during the reporting year.

3.5 Confidentiality and Legitimate Exceptions.
Exceptions to disclosure shall be narrowly construed and documented, limited to:

- Personal data protected under **GDPR**.
- Security-sensitive information (e.g., critical infrastructure vulnerabilities).
- Proprietary or trade-secret content where disclosure would cause material harm.

Justifications for non-disclosure must be recorded and subject to independent review.

3.6 Public Engagement and Feedback.
Stakeholders shall have the right to submit comments on published summaries through SLUC's digital platform. Feedback loops are integrated into adaptive management processes under Document 08.

Chapter 4 — Rectification and Appeals Process

4.1 Purpose and Procedural Fairness.
The rectification and appeals process ensures that auditees and affected stakeholders have a structured, impartial mechanism to contest findings or seek review of corrective-action requirements. This process reflects the fairness principles embedded in UNGPs and the grievance-effectiveness criteria under ESF ESS10.

4.2 Eligibility and Standing.
The following parties may initiate rectification or appeal:

- Auditees subject to validation or peer review.
- Stakeholders directly affected by findings or corrective actions.
- Component-level MEL units where interoperability or indicator integrity is contested.

4.3 Submission Protocols.
Appeals must be lodged within 30 calendar days of publication of the assurance statement or corrective-action plan. Submissions shall include:

- Identification of contested findings.
- Evidence supporting the appeal.
- Proposed remedy or alternative interpretation.

Appeals are filed through SLUC's secure portal, with acknowledgment issued within five business days.

4.4 Review Panels and Independence.
Appeals are adjudicated by an Independent Review Panel constituted under GSEA authority, separate from the original validation team. Panel composition mirrors independence and competence standards in Chapter 2, with mandatory inclusion of a legal advisor and an ethics officer.

4.5 Decision Timelines and Outcomes.

- **Preliminary Assessment:** Within 15 days of receipt.
- **Final Determination:** Within 45 days, unless extended for complexity.
  Outcomes include:
- Upholding original findings.
- Amending findings or corrective actions.
- Ordering a re-validation or thematic audit.

Decisions are documented and disclosed publicly, subject to confidentiality constraints.

4.6 Escalation and Finality.
Where disputes remain unresolved, escalation to the Agenda 2074 Oversight Council is permitted. Decisions of the Council are final and binding within the Creativa governance system.

4.7 Learning and Systemic Improvement.
Appeals data are analysed annually to identify systemic issues and inform revisions to MEL, safeguards, and assurance protocols. Lessons learned are disseminated through SLUC's Knowledge Repository.

Chapter 5 — Accreditation of Validators

5.1 Purpose and governance.
Accreditation assures that external validators and peer-review panellists engaged by GSEA/SLUC possess the competence, independence, and ethical posture required to render reliable assurance. Accreditation is administered by a GSEA Accreditation Council with a permanent secretariat. The system is benchmarked to internationally recognised conformity-assessment norms for accreditation bodies (ISO/IEC 17011) and for assurance engagements (ISAE 3000 (Revised); AA1000AS v3), with audit practice guided by ISO 19011 and competence/independence principles reflected in ISO/IEC 17029.

5.2 Scope of accreditation and grades.
Scopes are defined by thematic modules and roles to ensure proportional competence: (i) MEL and results verification; (ii) environmental and social safeguards equivalency (ESF/IFC); (iii) fiduciary controls and procurement integrity; (iv) digital governance, privacy and security; and, where relevant, (v) academic peer review. Grades comprise Associate Validator, Validator, Lead Validator, and Panel Chair; progression requires demonstrated competence, positive performance history, and independence records free of material breaches.

5.3 Entry requirements and assessment pathway.
Applicants submit a dossier evidencing education, professional certifications, sectoral experience, recent assurance workpapers, and continuing-professional-development (CPD) records. Independence and conflict-of-interest declarations are mandatory. Assessment comprises document review, a competence-matrix scoring, a witnessed assignment (or equivalent simulation), and a structured

interview. Due professional care and ethical fitness are appraised against ISAE 3000 (Revised) and AA1000AS v3 criteria; audit technique follows ISO 19011.

5.4 Validity, surveillance, and renewal.
Accreditation is granted for three years, subject to annual surveillance reviews covering: engagement volume and quality, independence breaches (none material), complaint management, and CPD (minimum 40 hours/year across MEL, safeguards, fiduciary, digital-privacy). Renewal requires an on-site or virtual reassessment and positive stakeholder references; adverse findings trigger probation or non-renewal consistent with the sanctions regime in Chapter 6.

5.5 Public registry and transparency.
A live public registry lists accredited persons and firms, scopes, grades, validity dates, and any sanctions. Publication adheres to the disclosure ethos of Agenda 2074 and the accessibility principles reflected in the World Bank Access to Information Policy.

5.6 Cross-recognition.
GSEA may recognise accreditations issued by accreditation bodies that are signatories to the IAF Multilateral Recognition Arrangement (MLA) or the ILAC MRA, subject to an Agenda 2074 equivalency module (ethics, independence, safeguards integration, MEL interoperability).

5.7 Funding and fee safeguards.
To preserve independence, validator compensation is drawn from a ring-fenced GSEA Assurance Fund; contingent-fee arrangements and success-fees are prohibited, mirroring independence expectations under ISAE 3000 (Revised) and the IESBA International Code of Ethics (Independence Standards).

5.8 Insurance and liability.
Accredited validators maintain appropriate professional indemnity and data-breach insurance, proportionate to engagement risk, complementing fiduciary risk controls described in Document 06.

5.9 Complaints, investigations, and sanctions.
Complaints against validators are receivable by the Accreditation Council and handled under due-process rules. Confirmed breaches may result in reprimand, suspension, scope reduction, or revocation; decisions and rationales are published, respecting **GDPR** constraints. Appeals follow Chapter 4 procedures.

Chapter 6 — Code of Independence and Professional Conduct

6.1 Normative alignment and binding effect.
This Code is binding on all accredited validators and panellists. It synthesises independence and ethics principles from the UN Guiding Principles on Business & Human Rights (UNGPs), the OECD Guidelines for Multinational Enterprises (2023), the IESBA International Code of Ethics, and assurance standards

6.2 Independence threats and safeguards.
Validators shall identify and mitigate self-interest, self-review, advocacy, familiarity, and intimidation threats. Prohibited relationships include financial interests in auditees, recent employment (prior twenty-four months), provision of non-assurance services related to the subject matter (prior twenty-four months and for twelve months post-engagement), and fee-dependence beyond prudent thresholds. Safeguards comprise team rotation, engagement quality review by an independent reviewer, additional supervision, and transparency of relevant relationships.

6.3 Conflicts-of-interest and disclosure.
Before acceptance and throughout the engagement, validators complete independence questionnaires and update conflict registers upon any change of circumstances. Known conflicts trigger recusal or disengagement. Disclosure of permitted immaterial relationships is included in the assurance statement to preserve public trust, consonant with the OECD Guidelines (2023) expectation of truthful communication.

6.4 Integrity, objectivity, and professional competence.
Validators act with honesty, fairness, and due care, avoiding misrepresentation and selective disclosure ("impact-washing"). Competence is maintained through CPD and supervision consistent with ISO 19011 guidance on auditor competence.

6.5 Confidentiality, data protection, and information security.
Evidence handling complies with GDPR and privacy-by-design principles, with secure storage, role-based access, encryption, and breach-notification procedures; digital workpapers follow tamper-evident logging. Where AI-enabled tools are used, validators document data lineage and human oversight consistent with the OECD AI Principles.

6.6 Stakeholder engagement and non-retaliation.
Interactions with affected people, including whistleblowers and GBV/SEAH survivors, follow survivor-centred, non-retaliatory protocols aligned with **UNGPs** and **ESF ESS10**. Coercion, intimidation, or inducements to influence testimony are prohibited.

6.7 Gifts, hospitality, and inducements.
Gifts or hospitality that could reasonably influence judgement are prohibited; modest, customary courtesies are permitted only where lawful and recorded in a public gift register, echoing anti-bribery expectations under **ISO 37001**.

6.8 Engagement quality review and documentation.
High-risk or high-materiality validations require a pre-issuance Engagement Quality Review by an independent, accredited reviewer. Documentation must support conclusions with sufficient, appropriate evidence and be retained per GDPR-compliant schedules; alterations post-issuance are logged with full audit trails, in line with ISAE 3000 (Revised) discipline.

6.9 Enforcement and disciplinary measures.
Breaches of this Code are investigated by the Accreditation Council. Proven breaches may lead to reprimand, mandated training, scope limitation, suspension, or revocation; egregious cases are referred to competent authorities. Outcomes and rationales are published, respecting privacy and safety constraints, and are appealable under Chapter 4.

6.10 Interface with Component-level MEL and scholarly peer review.
Validators operating within DESA, PCPP, PCGG, and UCE/UACE contexts adhere to this Code while respecting methodological specifics under Document 08 (Unified MEL) and editorial ethics under COPE and ESG (EHEA) where academic QA is implicated.