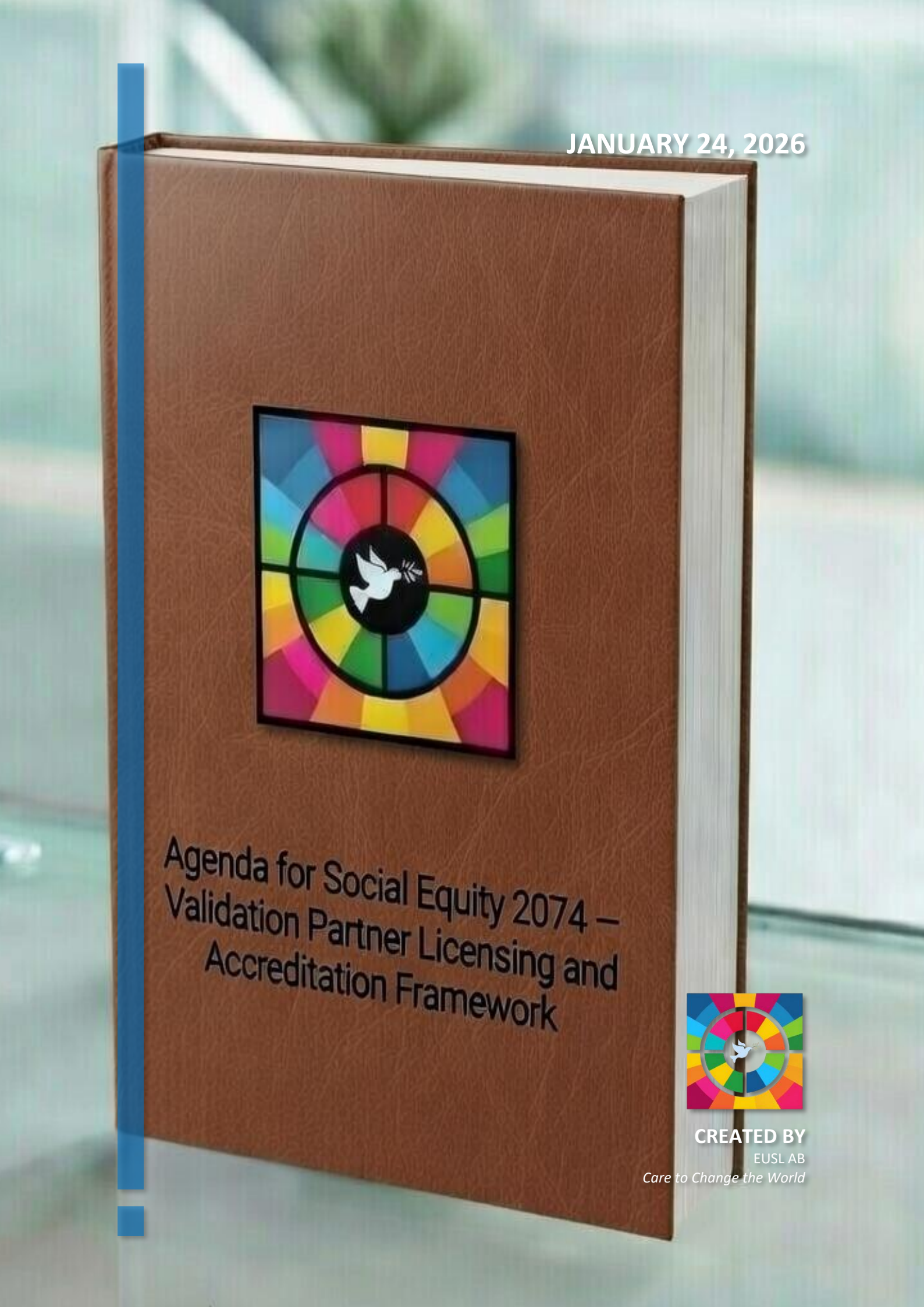

JANUARY 24, 2026

CREATED BY

EUSL AB

Care to Change the World

Table of Contents

Validation Partner Licensing and Accreditation Framework

Introduction

This Validation Partner Licensing and Accreditation Framework forms the second foundational instrument of the Agenda 2074 Social Responsibility Standard (A2074-SRS). It operationalizes the constitutional architecture established in the Foundational Charter by defining who may design and operate validation systems under Agenda 2074, the conditions under which such rights are granted, and the mechanisms for continuous oversight, quality assurance, ethics enforcement, and digital-privacy compliance.

The purpose of this Framework is threefold. First, to ensure that all Validation Partners—whether global, regional, sectoral, or single-goal—operate with demonstrable competence, integrity, and independence, and uphold the non-comparative, proportional, and rights-preserving doctrines codified in Document 1. Second, to guarantee that all methodologies submitted for approval, including hospitality-style star systems, points or maturity indices, sector modules, and deep dives, adhere to the 17 SGG pillars as the normative canon and comply with the patient-level confidentiality regime. Third, to embed robust GSIA oversight across licensing, surveillance, ethics investigations, and remediation, ensuring that the validation ecosystem remains credible, consistent, and safe for enterprises of all sizes.

This Framework is a legally subordinate instrument to the Foundational Charter but carries binding effect on all licensed Partners and their assessors, subcontractors, and affiliates. It incorporates the Digital Integration & Platform Governance Manual for data protocols, the Governance & Oversight Manual for ethics procedures, and the Operating Manual (Open Standard) for methodological specifications. Licensing is a derivative, time-bound, and revocable right. Accreditation is earned, not presumed, and is maintained through continuous compliance, periodic audits, ethics attestations, and demonstrable alignment to canonical updates. Nothing in this Framework authorizes any Partner to claim ISO certification or equivalence, nor to imply comparative ranking of named entities.

The Framework applies globally and accommodates diversity of scale, geography, and sector by introducing tiered authorisations, proportional due diligence, and a structured pathway for Partners to expand scope while maintaining fidelity to the SGG pillars. It ensures that actors such as EUSL—Agenda 2074's flagship Partner in Europe—operate under the same global custodial rules while offering regionally adapted models.

The following Chapters constitute the first two provisions of the Framework.

Chapter 1 — Definitions, Eligibility, and Scope

This Chapter establishes uniform definitions, eligibility criteria, and scope classifications for entities seeking to operate as Validation Partners under the A2074-SRS. All definitions herein shall be interpreted in harmony with the Foundational Charter, with supremacy afforded to canonical interpretations issued by Agenda 2074.

A Validation Partner is an organization licensed by Agenda 2074 to design, operate, and maintain one or more validation models aligned to the 17 SGG pillars and conducted under the proportionality,

non-comparative, and patient-level confidentiality doctrines. Partners may be generalist, regional, sectoral, or single-goal in scope, subject to capacity, due diligence, and continuous oversight.

Eligibility requires that an applicant demonstrate institutional competence, independence, governance maturity, financial integrity, digital-security readiness, and the ability to uphold all structural rights established in the Foundational Charter. Applicants must be legally constituted entities capable of entering enforceable obligations, maintaining auditable records, and cooperating with GSIA in audits, investigations, and corrective actions.

The Framework recognizes four scope classes:

Scope Class	Description	Typical Use Case	Required Competence Level
Generalist Validation Partner	Authorized to operate full multi-pillar models across all sectors and geographies	Cross-sector national or international operator (e.g., EUSL Europe-wide)	Highest; full assessor pool; digital governance; ethics controls
Regional Validation Partner	Authorized within specified geographic boundaries	Single-country or REC-based operator	High; localized competence and language capacity
Sectoral Validation Partner	Authorized for defined industry verticals	Healthcare, hospitality, logistics, education, etc.	High sector-specific competence; technical sampling expertise
Single-Goal Partner	Authorized to conduct deep-dive validation on one SGG pillar	Specialized human-rights NGO, gender equality center, climate analytics institute	Adequate competence in the specific pillar; narrower governance requirements

Minimum baseline competencies for all scopes include: (i) demonstrable understanding of the 17 SGG pillars and canonical interpretations; (ii) ability to design or operate reversible aggregation models; (iii) assessor competence criteria consistent with the Operating Manual; (iv) secure evidence handling and consent ledgering; (v) non-retaliation and de-biasing safeguards; and (vi) organizational independence from advisory, consulting, or lobbying activities that could compromise impartiality.

Applicants may request multiple scopes contemporaneously or sequentially. Each scope is independently reviewed, authorized, monitored, and, where necessary, withdrawn. Expansion to a new scope requires demonstration of capacity, absence of material compliance issues, and successful completion of GSIA ethics review for any high-risk domain (e.g., human rights, minors, sensitive data processing, public-sector integrity).

Chapter 2 — Accreditation Tiers and Authorisations

This Chapter establishes the tiered accreditation architecture under which Validation Partners are authorized and supervised. Accreditation tiers reflect competence, risk, geographic/systemic impact, and oversight requirements. Tier allocation is made by Agenda 2074 in consultation with GSIA and is subject to periodic re-evaluation.

Accreditation tiers do not establish hierarchy or prestige. They define operational boundaries, obligations, and intensity of oversight required to preserve integrity, confidentiality, and proportionality. No Partner may operate beyond the tier and scope expressly authorized in its license.

The Framework recognizes three principal accreditation tiers:

Tier	Description	Permitted Activities	Oversight Intensity
Tier I — Full Multi-Pillar Accreditation	Highest-level authorization for full-scope multi-pillar models	Operate generalist, regional, sectoral, and deep-dive models; propose new methodologies; train assessors	Highest: annual GSIA ethics review; digital audits; meta-audits every 24–36 months
Tier II — Restricted Multi-Pillar Accreditation	Authorization limited by geography or sector	Operate multi-pillar validations within defined domains; adopt but not originate methodologies	Moderate-high: biennial GSIA review; targeted audits; model-implementation monitoring
Tier III — Single-Goal or Module Accreditation	Authorization limited to one SGG pillar or a defined module	Conduct deep-dive validations; issue scoped attestations	Moderate: GSIA review every 3 years; simplified digital audit; focused ethics checks

Tier assignment determines required governance, staffing, digital security, evidence controls, training obligations, and the frequency of GSIA reviews. All Tiers must maintain assessor competence, uphold confidentiality and consent rules, and ensure reversible aggregation of results. Tier I Partners may originate methodologies subject to Agenda 2074 approval (Chapter 4). Tier II Partners may adapt but not originate methodologies. Tier III Partners are confined to deep-dive or module scopes.

Additional authorisation classes apply irrespective of Tier:

Authorisation Class	Applicability	Notes
AI-Assisted Processing Authorisation	Required for Partners using machine-assisted scoring or sampling	Subject to stringent human-in-the-loop, explainability, and safety controls
Public-Sector Authorisation	Required to validate public bodies or sensitive institutions	Includes enhanced conflict-of-interest rules, whistleblower protections
High-Risk Pillar Authorisation	Required for SGG pillars dealing with human rights, minors, safety	Includes GSIA ethics review and mandatory annual reporting
Cross-Border Authorisation	Required for multi-jurisdictional data processing	Includes additional privacy, security, and conflict-of-laws obligations

Accreditation may be upgraded, downgraded, or consolidated through periodic review or pursuant to GSIA findings. Upgrades require evidence of sustained performance, mature governance, and absence

of material compliance issues. Downgrades may follow repeated quality, ethics, or privacy failures. Suspension or withdrawal is addressed in Chapter 12.

Tiering ensures proportional oversight, preserves system integrity, and creates predictable pathways for growth while maintaining rights protection and methodological fidelity across all Partner engagements.

Chapter 3 — Application Requirements and Due Diligence

This Chapter establishes the mandatory application dossier, the stages of review, and the due-diligence standards that govern the admission of Validation Partners under the A2074-SRS. It shall be read in harmony with the Foundational Charter, the Governance & Oversight Manual, the Operating Manual (Open Standard), and the Digital Integration & Platform Governance Manual. Its purpose is to ensure that licensed entities possess the governance maturity, technical capability, independence, and ethics controls necessary to uphold the 17 SGG pillars, proportionality, non-comparative evaluation, and patient-level confidentiality.

An application shall be complete, accurate, and independently verifiable. It shall demonstrate that the applicant is a legally constituted entity with capacity to enter enforceable obligations, to maintain auditable records, to cooperate with GSIA in audits and investigations, and to implement corrective actions where ordered. The applicant shall identify its requested scope class or classes (generalist, regional, sectoral, single-goal) and the accreditation tier sought, acknowledging that scope and tier are independently determined and may be conditioned, limited, or denied on risk grounds.

The application dossier shall, at minimum, contain the following components, each of which is reviewed for sufficiency, credibility, and risk:

Dossier Component	**Minimum Content**	**Review Standard**	**Potential Conditions**
Legal Identity and Governance	Articles of incorporation; beneficial ownership; board composition; governance policies; conflict-of-interest rules	Independence from advisory lines likely to compromise impartiality; disclosure completeness	Board composition adjustments; firewall enhancements
Capability and Staffing	Organizational structure; assessor profiles; competence criteria; recruitment and training plans	Adequacy of assessor pool; competence mapping to requested scope	Competence uplift plans; supervised start-up period
Methodological Readiness	Draft or adopted model(s); SGG mapping; reversible aggregation; sampling logic; evidence classes	Canonical fidelity; proportionality; non-comparative structure	Restricted scope; pilot phase under supervision
Digital and AI Governance	Data architecture; consent ledger; access control;	Privacy-by-design; explainability; auditability	Additional controls; third-party testing; AI use moratoria

	encryption; AI use cases; human-in-the-loop		
Ethics Management System	Ethics policy; complaints channels; whistleblower protection; retaliation safeguards	Accessibility; independence; protection effectiveness	Independent ethics officer; reporting line to GSIA
Financial Integrity	Fee schedules; hardship tiers; funding sources; anti-corruption safeguards	Transparency; non-coercive pricing; ring-fencing	Fee remediation schemes; donor non-interference covenants
Communications and UI/UX	Draft client notices; consent flows; disclosure summaries; ISO disclaimers	Clarity; non-manipulative language; scope/expiry statements	Content corrections; pre-clearance for initial period
Risk and Jurisdiction	Jurisdictional footprint; cross-border data flows; regulatory interfaces	Conflict-of-laws risks; public-sector handling	Cross-border authorisation; enhanced COI rules

The due-diligence process proceeds through staged review, designed to preserve procedural fairness while providing early detection of disqualifying risks and proportional mitigation of remediable issues.

Stage	**Conduct**	**Decision Points**	**Timeline (Indicative)**
Preliminary Completeness Check	Administrative verification of dossier completeness and eligibility	Proceed to substantive review or return for cure of defects	10 business days
Substantive Review — Secretariat/Agency	Review of governance, capability, methodology readiness, digital controls, communications	Admission to GSIA ethics screen; request for clarifications; conditional progression	30–45 business days
GSIA Ethics Screen (Risk-Based)	Assessment of retaliation safeguards, consent governance, COI, whistleblower protections, high-risk domains	Approve ethics posture; impose conditions; require redesign or deny	20–30 business days; expedited for high risk
Technical Interview and Demonstration	Presentation of model logic, sampling, reversible aggregation, and UI/UX by applicant team	Confirm technical feasibility; flag issues for remediation	Scheduled within review window

Site or Virtual Verification (Risk-Based)	Inspection of secure environments, assessor training facilities, and systems	Confirm operational readiness; identify gaps	As needed; Tier I generally required
Decision and Licensing	Grant tier and scope with conditions; deny with reasons; or defer pending remediation	Final licensing terms and obligations; surveillance calendar	Within 10 business days of final review

High-risk scopes—public-sector validations, high-risk pillars (e.g., human rights, minors, safety), AI-assisted scoring, and cross-border processing—require mandatory GSIA involvement. GSIA may prescribe additional safeguards, including independent ethics officers with direct reporting to GSIA, enhanced whistleblower protections, assessor rotation rules, and pre-clearance of consent language for a defined initial period. Failure to satisfy ethics prerequisites results in denial without prejudice to re-application upon remediation.

Risk grading determines the intensity of surveillance and the initial operating limitations:

Risk Grade	**Determinants (Illustrative)**	**Oversight Implications**	**Operating Limitations (Illustrative)**
Low	Narrow scope; mature controls; no AI; single-jurisdiction; robust ethics posture	Standard surveillance cadence	None beyond general conditions
Moderate	Multi-pillar in one jurisdiction; limited AI assistance; mixed client archetypes	Enhanced early-life monitoring; targeted ethics checks	Pre-clearance of communications in first year
High	Cross-border; AI scoring; public-sector; high-risk pillars; complex ownership	Annual ethics audits; digital meta-audits; independent monitor	Staged rollout; limited caseload caps; pilot period
Elevated (Conditional)	Prior compliance issues or structural remediation underway	Close GSIA supervision; frequent reporting	Restrictive conditions; upgrade only upon verified remediation

All applicants must attest that they will refrain from comparative public rankings of named entities, coercive disclosure practices, and any implication of ISO 26000 certification or equivalence. Any material misstatement or omission in the application constitutes grounds for denial or, if discovered post-licensing, for suspension or withdrawal under Chapter 12.

Chapter 4 — Methodology Review and Approval

This Chapter prescribes the standards and procedures for reviewing and approving partner methodologies, ensuring fidelity to the 17 SGG pillars, proportionality, non-comparative evaluation, and patient-level confidentiality. Methodologies encompass hospitality-style star systems, points or maturity indices, sector modules, and single-goal deep dives. Approval is a necessary but not sufficient condition for licensing; it is specific to the method version, the declared scope, and the accreditation tier of the Partner.

The methodology submission package shall disclose, with sufficient specificity to permit independent review, the following elements:

Methodology Element	Required Content	Review Focus
Canonical Mapping	Explicit mapping of controls, metrics, and outputs to SGG1–SGG17	Completeness; avoidance of deletion or substitution; intelligibility
Scoring and Aggregation	Scoring logic; weighting rationale; reversible aggregation; display rules	Preservation of pillar-level review; proportionality; non-comparative design
Sampling and Evidence	Sampling strategy by archetype; evidence classes (policy, process, outcome, grievance/feedback)	Proportional burden; sufficiency; chain-of-custody feasibility
Remediation and Improvement	Triggers for corrective actions; improvement horizon by archetype	Fair timelines; non-coercive remediation; transparency to subject
Confidentiality and Consent	Consent flows; ledger integration; revocation handling; expiry logic	Private-by-default; explicit, informed, revocable consent; UI clarity
AI Use and Human Oversight	AI models used; decision points; explainability; human-in-the-loop	Contestability; no automation of adverse actions without review
Communications and UI/UX	Badge designs; scope statements; expiry; ISO disclaimers	Non-misleading; no implied comprehensiveness; channel specificity
Change Control and Versioning	Semantic versioning; materiality thresholds; rollout plan	Predictable updates; stakeholder notices; auditability

Methodologies are evaluated against a normative rubric. Approval may be unconditional, conditional with mandated modifications, pilot-limited, or denied with reasons.

Criterion	Approval Standard	Typical Conditions (if Conditional)
Canonical Fidelity	All 17 pillars preserved and intelligible; canonical definitions used	Rewording corrections; explicit pillar traceability in UI
Proportionality	Burden calibrated by archetype and risk	Sampling recalibration; evidence simplification for microenterprises

Non-Comparative Design	No public league tables; within-entity benchmarking only	Removal of comparative outputs; anonymization requirements
Reversible Aggregation	Composite displays reversible to pillar-level detail	Back-end linkage proofs; audit trail enhancements
Consent Governance	Explicit, informed, revocable; scope, channel, audience, duration	Consent language pre-clearance; ledger interface changes
Digital Security & AI Guardrails	Privacy-by-design; secure handling; human oversight of AI	Model card publication (internal); explainability tests
Communications Integrity	Clear scope and expiry; ISO 26000 disclaimer; no coercion	Badge redesign; standardized registry text
Remediation Logic	Fair timelines; non-retaliatory; protective where harm	Time-bound improvement plans; ethics escalation triggers

Hospitality-style star systems shall define each star threshold with explicit, measurable control objectives and minimum evidence expectations per pillar. Points or maturity indices shall publish, within the subject interface and GSIA audit interface, the mapping between pillar-level controls and the composite score, with documentation of any sectoral weights and the justification for each. Sector modules may elaborate controls and metrics particular to industry risk, provided that canonical language is preserved and cross-walks to the standard evidence classes remain intact. Single-goal deep dives shall publish a scope and limitations statement, maintain canonical fidelity for the covered pillar, and avoid any implication that the attestation is comprehensive.

For hospitality-style star systems, the following schematic illustrates minimum normative structure:

Star Level	**Minimum Pillar-Aligned Control Objective (Illustrative)**	**Evidence Class Expectation**
★	Foundational controls across all pillars established, documented, and communicated; grievance channel operational	Policy artefacts; basic process evidence; narrative attestations
★★	Controls implemented across core processes; risk-based sampling demonstrates operation; initial outcomes tracking	Process evidence; sampling records; initial outcome indicators
★★★	Controls integrated; continuous improvement cycle active; stakeholder feedback systematically used	Outcome evidence; grievance resolution records; improvement plans
★★★★	Advanced controls with sectoral elaborations; robust data integrity; independent internal assurance	Comprehensive evidence; internal audit interfaces; de-identified benchmarks

★★★★★	Exemplary performance with verifiable outcomes; systemic contributions to anonymized learning; leadership in non-retaliation	High-confidence outcome evidence; participation in anonymized case digests; ethics excellence attestations

Approval is coupled with a change-control regime. Material changes—alterations to pillar mapping, scoring logic, aggregation reversibility, consent flows, or AI decision points—require resubmission and approval prior to deployment. Minor changes—clarifications that do not affect structural rights—may proceed with post-hoc notification as specified in the approval notice. Emergency advisories issued by Agenda 2074 for integrity or safety concerns shall be implemented immediately, with interim measures confirmed in writing. All approved methodologies carry a semantic version identifier; Partners shall ensure that client engagements specify the version in force and that any public disclosures state the version, scope, and expiry.

Pilot approvals may be granted where novel approaches present potential merit but require observed operation under supervision. Pilot conditions may include caseload caps, enhanced GSIA reporting, mandatory client consent notices highlighting pilot status, and pre-clearance of public communications. Conversion from pilot to full approval is contingent on satisfactory performance, absence of material incidents, and closure of identified action items.

No methodology may employ comparative public rankings of named entities, implied ISO certification, or coercive disclosure incentives. Violations constitute material breaches and are subject to GSIA adjudication, corrective orders, and licensing action under Chapter 12.

Chapter 5 — Training, Competency, and Continuing Professional Development

This Chapter mandates structured qualifications, method-specific certifications, and continuing professional development (CPD) obligations for all personnel engaged in design, delivery, supervision, quality assurance, and ethics oversight of validations under the A2074-SRS. It is designed to ensure that assessor competence, methodological literacy, and ethics fluency are demonstrably maintained over time, and that Partners possess the instructional governance required to sustain performance across geographies, sectors, and languages.

Validation Partners shall establish and maintain a formal Competency Management System (CMS) that documents role profiles, competency matrices mapped to the 17 SGG pillars and canonical interpretations, learning paths, examinations, CPD calendars, and re-certification intervals. The CMS shall be auditable and interoperable with the Operating Manual (Open Standard), the Multi-Model Validation Framework, and the Governance & Oversight Manual. Competency obligations apply to staff, contractors, and any third parties performing validation-adjacent activities under a Partner's control.

At minimum, Partners shall maintain differentiated role standards, ensuring that no person undertakes responsibilities beyond their certified competence and that supervisory chains are staffed with personnel qualified to review the models they oversee.

Role Category	**Core Competencies (Minimum)**	**Certification and CPD Requirements**	**Supervision and Limits**

Assessor (Generalist)	Canonical literacy across SGG1–SGG17; proportional sampling; non-comparative evaluation; consent governance	Initial certification on A2074 Open Standard; 24 CPD hours/yr; re-certification every 3 years	Supervised for first 5 engagements; caseload caps in first year
Assessor (Sectoral)	All generalist competencies plus sector risk lenses and metrics; grievance/feedback channel evaluation	Sector module certification; 30 CPD hours/yr with 12 sector-specific	May lead sectoral engagements after 10 supervised assignments
Lead Assessor / Engagement Manager	Model integration; reversible aggregation verification; remediation planning; client communications integrity	Lead credential; 36 CPD hours/yr; annual ethics refresher	Final sign-off authority; responsible for consent posture accuracy
Methodologist	Pillar mapping; scoring/weighting logic; change control; UI/UX disclosures	Methodology design certification; 24 CPD hours/yr; AI/analytics modules where used	May propose changes subject to Chapter 4 approvals
Quality Assurance (QA) Reviewer	Meta-audit techniques; sampling verification; evidence integrity; defect taxonomy	QA/meta-audit certification; 24 CPD hours/yr; independence training	Cannot QA engagements they staffed or supervised
Ethics Officer (Partner-level)	Patient-level confidentiality; retaliation prevention; complaints handling; GSIA interface	Ethics management certification; 24 CPD hours/yr; whistleblower protection	Reports directly to Partner leadership and GSIA (dual line)
Digital & AI Governance Lead	Privacy-by-design; secure evidence handling; consent ledgering; AI guardrails	Digital governance certification; AI human-oversight module; 24 CPD hours/yr	Approves any AI change control affecting determinations

Competency acquisition and maintenance shall be evidenced by examinations, observed practice, calibrated scoring exercises, and case-based ethics simulations. CPD content must include annual updates on canonical interpretations, ethics advisories issued by GSIA, and any changes to digital security, consent ledgering, or AI guardrails. Language and accessibility accommodations shall be provided to ensure comprehension without diluting examination standards. Records of training, examinations, supervision, and CPD completion must be retained in audit-ready form and produced to GSIA upon request.

The CMS shall embed safeguards against bias, conflicts, and drift. Assessor rotation policies must prevent familiarity bias with recurring clients. Independence training shall clarify prohibited relationships, including advisory or lobbying roles that could impair impartiality. Where staff perform

both advisory and validation roles within the same legal group, firewalls described in Chapter 7 shall govern; however, personnel assigned to validation may not concurrently perform related advisory services for the same subject entity or its immediate affiliates within the same validation cycle.

Partners shall implement a structured remediation pathway for competency gaps detected during QA or GSIA reviews, including targeted training, supervised re-performance, or temporary restriction of roles. Repeated deficiencies in ethics or confidentiality competence trigger mandatory re-certification and may lead to license conditions under Chapter 12.

Where AI-assisted tools are used in sampling or analysis, all affected roles must complete method-specific AI modules covering explainability, limitations, bias detection, and human-in-the-loop decision duties. No AI deployment may proceed without certifying at least one methodologist and one digital governance lead on the specific model and its change-control protocol.

The Partner's training program is subject to periodic review as part of the accreditation surveillance cycle. GSIA may issue training and competence orders if systemic gaps are identified, including the requirement to appoint independent trainers or to adopt common curricula published under the A2074 Open Standard. Costs of remedial training are borne by the Partner.

Chapter 6 — Quality Assurance and Meta Audit

This Chapter institutes a multi-layer Quality Assurance (QA) and Meta Audit regime to ensure methodological integrity, consistency of determinations, and continuous improvement without compromising patient-level confidentiality. QA is the Partner's internal responsibility to verify that engagements conform to approved methodologies and structural rights. Meta audits are higher-order reviews—conducted by the Partner's independent QA function and, periodically, by GSIA—to assess whether methodologies are applied consistently, proportionately, and in harmony with canonical interpretations.

Partners shall establish a QA Program approved by their leadership and aligned to accreditation tier and scope. The program must be independent of engagement delivery, report functionally to the Partner's Ethics Officer on confidentiality-relevant defects, and have unfettered access to validation records, consent ledgers, and method documentation. QA reviewers must meet the competency standards in Chapter 5 and be free of conflicts regarding the sampled engagements.

The QA Program shall implement the following minimum cycle and artifacts:

QA Component	Minimum Standard	Frequency / Coverage	Evidentiary Output
Engagement File Reviews	Verification of pillar mapping, sampling sufficiency, reversible aggregation, consent scope compliance	Risk-based sampling; minimum 10% of closed files per quarter; higher for high-risk scopes	QA review memo; defect log; remediation orders
Scoring Calibration Sessions	Cross-assessor calibration using anonymized case fragments and canonical test packs	Quarterly; mandatory for all assessors; documented outcomes	Calibration records; variance analysis; retraining plans

Method Adherence Checks	Audit of adherence to approved version; change-control compliance	Each release; pre-deployment and post-deployment spot-checks	Version control report; deployment attestation
Communications & UI Review	Verification of consent language, scope/expiry, ISO disclaimers, and non-comparative design	Biannual; pre-clearance for material changes	Sign-off records; redline archive
Data Integrity and Security Tests	Access control, encryption, logging, consent ledger immutability	Quarterly for Tier I; biannual for Tier II; annual for Tier III	Security test reports; remediation tickets; closure confirmations
Corrective Action Tracking	End-to-end tracking of defects from detection to closure; trend analysis	Continuous; quarterly roll-ups	CAPA register; trend dashboards; management review minutes

Meta audits operate at the systems level to detect structural drift, bias, or disproportionality and to validate that QA is effective. GSIA may conduct independent meta audits at intervals corresponding to the Partner's accreditation tier and risk grade. Meta audits prioritize rights-critical domains, including consent governance, retaliation prevention, reversible aggregation, and avoidance of comparative outputs.

Meta Audit Focus Area	Review Questions	Typical Evidence	Potential Outcomes
Proportionality in Practice	Are burdens calibrated by archetype? Are microenterprises protected from undue demands?	Stratified file samples; time-on-task; sampling rationales	Redesign of sampling; burden caps; targeted guidance
Confidentiality & Consent	Are disclosures strictly per scope, channel, audience, duration? Are revocations honored?	Consent ledger traces; takedown logs; UI screenshots	Injunctive corrections; consent workflow redesign
Non-Comparative Integrity	Any emergence of league-table effects or implied ranking?	Marketing materials; registry displays; partner portals	Public corrections; marketing controls; license conditions
Reversible Aggregation	Can composites be traced back to pillar-level results reliably?	System demonstrations; audit trail replays	Technical refactoring; mandatory back-end link proofs

AI Guardrails	Is human review effective? Are model changes controlled and explainable?	Model cards; change logs; adjudication records	AI moratoria; third-party testing; enhanced oversight
Ethics Response Effectiveness	Are complaints resolved promptly with protective measures?	Case lifecycle records; timelines; outcomes	Process redesign; training orders; independent monitor

Partners shall maintain a Corrective and Preventive Action (CAPA) system that assigns ownership, deadlines, and verification steps for all defects and improvement opportunities arising from QA and meta audits. CAPA closure requires verification by QA and, where rights-critical, concurrence by the Ethics Officer. Repeated or material QA failures trigger escalation to GSIA, which may impose conditions, mandate independent monitors, or recommend suspension or withdrawal pursuant to Chapter 12.

Performance and consistency metrics shall be monitored by Partner leadership, at minimum: defect rates by type and severity; rework percentages; average time to consent revocation takedown; AI override rates and justifications; sampling burden by archetype; and compliance with CPD requirements. Trends indicating systemic disproportionality or confidentiality risk must be addressed with documented action plans.

Meta audit and QA outputs are confidential by default. Aggregated and anonymized findings may be shared in public-interest reports to promote learning, provided that no subject entity or individual assessor can be identified and that no individual validation result is disclosed absent consent. Any public-interest sharing must be coordinated with GSIA to ensure consistency with the Foundational Charter.

Nothing in this Chapter authorizes comparative public rankings of named entities, nor any compromise of patient-level confidentiality. Where conflicts arise between QA transparency and subject privacy, privacy prevails. Partners must design QA and meta-audit procedures with privacy-preserving techniques, including redaction, controlled environments, and need-to-know access.

Chapter 7 — Independence, Conflicts, and Firewalls

This Chapter mandates structural independence, conflict-of-interest (COI) controls, and operational firewalls to preserve impartiality in validation activities under the A2074-SRS. It shall be construed in concert with the Foundational Charter, the Governance & Oversight Manual, and Chapters 3, 5, and 6 of this Framework. Its objective is to ensure that commercial incentives, advisory relationships, or organizational affiliations do not compromise proportionality, non-comparative evaluation, or patient-level confidentiality.

Validation Partners shall operate validation as a functionally independent line of service with distinct governance, reporting, and financial controls. Where validation is offered within a corporate group that also provides advisory, consulting, lobbying, technology integration, or implementation services, the Partner must implement robust firewalls. At minimum, such firewalls include separate leadership accountability; segregated profit and loss (P&L); independent performance metrics; restricted data access; mandatory COI screening prior to engagement acceptance; and prohibitions on the use of confidential validation information for any non-validation purpose. Personnel assigned to validation

shall not provide advisory services to the same subject entity, its immediate parents, subsidiaries, or controlled affiliates during the same validation cycle.

Conflicts of interest are to be identified, disclosed, assessed, and mitigated before engagement acceptance and continuously thereafter. Disqualifying conflicts include financial interests in the subject entity that could materially affect impartiality; contingent fee arrangements; compensation linked to disclosure or “star” outcomes; and advisory engagements that would require evaluating one’s own work. Mitigable conflicts include prior limited advisory unrelated to the scope under review, distant affiliate relationships without operational control, or non-controlling equity interests subject to blind trust arrangements. All conflicts and mitigation plans must be documented and available for GSIA audit.

Partners shall maintain an Independence and Conflicts Register, overseen by the Partner’s Ethics Officer, with direct visibility to GSIA upon request. The Ethics Officer shall have authority to block engagements, mandate personnel recusals, order rotation of assessors, and require external peer review where appropriate. Repeated or unmitigated conflicts constitute grounds for license conditioning, suspension, or withdrawal under Chapter 12.

The following table codifies mandatory controls:

Control Domain	Minimum Requirement	Prohibited Conduct	Evidence of Compliance
Organizational Independence	Stand-alone validation governance; separate P&L; independent leadership KPIs	Cross-subsidy tied to disclosure outcomes; leadership incentives linked to client publicity	Org charts; P&L statements; KPI frameworks
Engagement Acceptance	Pre-acceptance COI screening; ethics sign-off for high-risk or public-sector scopes	Acceptance where prior advisory creates self-review threat	COI checklists; ethics approvals
Personnel Assignment & Rotation	Recusal of conflicted staff; rotation to avoid familiarity bias; cooling-off periods	Staff assigned simultaneously to advisory and validation for same subject	Staffing records; rotation logs
Information Barriers (Firewalls)	Logical/physical segregation; need-to-know data access; separate IT systems where feasible	Sharing validation data with advisory units; marketing use without consent	Access control lists; audit logs
Compensation & Fees	No outcome-contingent or disclosure-contingent fees; transparent tiered pricing	“Pay-for-stars”; discounts conditioned on publicity	Fee policies; engagement letters
Third-Party Affiliates	COI due diligence on subcontractors; pass-through of independence obligations	Use of sales affiliates paid on disclosure conversions	Subcontractor attestations; affiliate contracts

Board/Ownership Interests	Beneficial ownership disclosure; blind trust or divestiture for material interests	Undisclosed controlling stakes in subjects	Ownership registry; trustee agreements

In circumstances where the Partner is uniquely qualified but faces a mitigable conflict, the Partner may seek a GSIA waiver subject to stringent conditions, including independent QA co-sign, enhanced sampling transparency, and explicit client consent acknowledging the mitigated conflict. Waivers are exceptional, time-bound, and published in anonymized form by GSIA for systemic learning. No waiver is available for outcome-contingent compensation, coerced disclosure incentives, or self-review conflicts.

Breach of independence or COI controls triggers prompt remedial action: cessation or reassignment of the affected engagement, notification to the subject entity, file-level re-validation as needed, and reporting to GSIA. Where breach results in public disclosure contrary to consent or structural rights, immediate injunctive measures shall be implemented pursuant to GSIA direction. The Partner bears the cost of remediation.

Nothing in this Chapter authorizes derogation from patient-level confidentiality. Where conflict mitigation requires external peer review or additional oversight, all reviewers are bound by equal or higher confidentiality obligations, consent constraints, and data security controls.

Chapter 8 — Ethics Assurance System and GSIA Interface

This Chapter requires each Validation Partner to establish, maintain, and continually improve an Ethics Assurance System (EAS) that aligns with the structural rights and doctrines of the A2074-SRS and interfaces directly with GSIA. The EAS is the internal system of policies, procedures, roles, controls, and monitoring practices that ensures ethics compliance, protects autonomy and non-retaliation, and supports effective remedies when risks or violations are detected.

The EAS shall be led by a Partner-level Ethics Officer with operational independence, direct reporting lines to the Partner's governing body, and an established liaison channel to GSIA. The Ethics Officer's mandate includes policy stewardship; oversight of complaint intake and whistleblower protections; review and sign-off of consent language and disclosure artifacts; participation in QA and meta-audit prioritization; escalation of rights-critical incidents to GSIA; and certification of quarterly ethics attestation reports.

Minimum components of the EAS include:

EAS Component	Purpose	Minimum Features	GSIA Interface
Ethics Policy & Code	Codify patient-level confidentiality, non-retaliation, proportionality, non-comparative evaluation	Plain-language commitments; enforcement provisions; disciplinary matrix	Filed with GSIA; updates notified within 10 business days

Complaints & Whistleblower Channels	Enable safe reporting by subjects, staff, and third parties	Anonymous and named channels; anti-retaliation guarantees; multi-language access	GSIA-linked referral pathway; quarterly case statistics
Consent Governance Controls	Ensure explicit, informed, revocable consent with scope, channel, audience, duration	Standardized templates; ledger integration; UI/UX pre-clearance	Pre-clearance for high-risk scopes; audit of revocation performance
Ethics Risk Assessment	Identify and prioritize rights-critical risks	Risk register; heat-map; scenarios (coercion, misuse, re-identification)	Shared summaries; joint reviews for high-risk areas
Incident Response & Remedies	Contain, correct, and prevent recurrence of ethics incidents	Playbooks; injunctive steps; communications rectification; CAPA	Immediate notice for severe incidents; closure verification
Training & Certification	Build and maintain ethics competence	Mandatory onboarding and annual refreshers; case simulations	GSIA advisories integrated into training; audit of completion
Monitoring & Attestation	Provide assurance on ethics performance	Quarterly attestations; KPIs (e.g., takedown times, complaint resolution)	Attestations submitted to GSIA; risk-based follow-ups

Quarterly ethics attestations signed by the Ethics Officer shall confirm: adherence to patient-level confidentiality; absence of coercive disclosure practices; timely handling of revocations (including median takedown times by channel); accuracy of ISO 26000 disclaimers; and disposition of complaints, including protective measures where retaliation risk was alleged. Attestations shall also disclose any material incidents, corrective actions taken, and open CAPA items with target closure dates.

Partners must establish a direct, secure reporting line to GSIA for early warning and escalation. The following categories require prompt (within 5 business days) notification to GSIA: unauthorized disclosure or consent-scope breach; retaliation allegations with credible risk of harm; discovery of irreversible aggregation defects that impede pillar-level review; AI malfunctions leading to adverse determinations without human confirmation; and discovery of comparative outputs or implied ranking in public materials. For each notification, the Partner shall provide a containment status, planned corrective measures, and a timetable for full remediation.

GSIA may, at its discretion, require enhanced ethics supervision for Partners operating in high-risk domains, including appointment of an independent ethics monitor, increased frequency of attestations, pre-clearance of communications, or pilot limitations for new methodologies. Failure to cooperate with GSIA, to provide timely and complete information, or to implement ordered remedies constitutes material non-compliance and may result in license conditions, suspension, or withdrawal under Chapter 12.

To support learning without compromising confidentiality, Partners shall contribute anonymized case digests to GSIA's systemic advisories. Each digest must exclude identifying details, preserve de-identification integrity, and focus on failure modes, corrective actions, and prevention strategies. Participation in anonymized learning is a condition of licensing for Tier I and Tier II Partners and is strongly encouraged for Tier III Partners.

Nothing in this Chapter authorizes GSIA or the Partner to disclose a subject entity's validation results without consent. The EAS must ensure that any transparency measures are aggregate, anonymized, and rights-preserving, and that any subject-opted disclosures are recorded, time-bound, and revocable via the consent ledger consistent with the Foundational Charter and the Digital Integration & Platform Governance Manual.

Chapter 9 — Data Protocols, Security, and Privacy

This Chapter establishes binding data governance obligations for all Validation Partners, ensuring full alignment with the patient-level confidentiality doctrine of the Foundational Charter and the technical specifications of the Digital Integration & Platform Governance Manual. It applies to all data classes, whether originating from subject entities, generated by assessors, created through model-assisted tools, or produced during quality assurance and meta-audit activities. Its purpose is to ensure that all processing is lawful, proportionate, auditable, and rights-preserving, and that no data handling practice compromises confidentiality, autonomy, or non-retaliation.

Validation Partners shall operate under a privacy-by-design and security-by-default paradigm. This requires embedding protective controls at every stage of the processing lifecycle: collection, transmission, storage, analysis, disclosure, retention, and deletion. No processing may occur without a valid legal basis consistent with the purposes of A2074-SRS validation. Secondary use is strictly prohibited unless explicitly, affirmatively, and revocably consented to by the subject entity.

All Partners shall maintain a Data Governance Framework (DGF) incorporating policies, procedures, and technical controls governing evidence handling, privacy notices, consent ledgering, access management, cryptographic protections, audit trails, AI controls, and breach response. The DGF shall be reviewed at least annually, and updated promptly upon issuance of interpretive circulars, GSIA ethics advisories, or relevant digital governance amendments.

Minimum data governance expectations are codified in the following matrix:

Data Governance Domain	**Minimum Standard**	**Obligations**	**Prohibited Conduct**
Collection & Minimisation	Evidence limited to declared scope	Notices must specify purpose, retention, rights	Collection for unrelated commercial purposes
Storage	Encryption at rest; client-segmented repositories	HSM-backed key management; MFA access	Shared storage with advisory units; plaintext repositories

Transmission	End-to-end encrypted channels	Logging of transfer events; integrity hashing	Emailing raw artefacts; unencrypted transfer
Access Control	Strict need-to-know permissions	RBAC/ABAC; periodic access reviews	Broad administrator access; shared accounts
Consent Governance	Immutable ledger; revocation-enabled	Scope, audience, duration recorded	Implied consent; altered consent records
AI Use	Human-in-the-loop; explainability	Model cards; audit logs; change control	Fully automated adverse outcomes
Retention & Deletion	Minimal retention; deletion certificates	Proof of deletion; anonymization where retained	Indefinite storage; undeclared data lakes
Breach Response	Containment, notification, remediation	GSIA notice within 5 business days	Concealment or delayed reporting

Cross-border and third-party data processing require explicit evaluation of jurisdictional risks, contractual protections, and technical safeguards. Subprocessors must be contractually bound to standards equal or higher than those required by this Framework and must support GSIA audit rights.

No data—raw, derived, or metadata—may be used for training, tuning, or validating AI systems unless: (i) it has been irreversibly anonymised; (ii) re-identification risk is negligible; and (iii) such use has been consented to or expressly authorized in the Digital Integration & Platform Governance Manual. Shadow processing without safeguards is prohibited.

Breach incidents—unauthorized access, consent-scope violations, data loss, tampering, AI malfunctions, or accidental disclosure—must be subject to immediate containment, root-cause analysis, documentation, subject notification (unless prohibited by law), and GSIA reporting. GSIA may order remedial measures, require independent testing, or impose license conditions.

Nothing in this Chapter permits comparative public ranking, coercive disclosure, or inference of commercial advantage for consenting to disclosure. Privacy and security obligations supersede operational convenience and commercial interests.

Chapter 10 — Licensing Terms, IP Use, and Branding

This Chapter governs the derivative rights granted to Validation Partners, the permitted and prohibited uses of Agenda 2074 intellectual property, and the rules for co-branding, iconography, and external communications. Its objective is to ensure that public representations of A2074-SRS remain accurate, rights-preserving, non-misleading, and consistent with the custodial role of Agenda 2074.

Licensing is a time-bound, non-exclusive, non-transferable, and revocable right to operate one or more approved validation methodologies under the A2074-SRS. No Partner obtains ownership of the standard, the canonical interpretations, the SGG pillars, the Open Standard specifications, or any iconography associated with Agenda 2074.

10.1 Licensing Terms

Partners may use Agenda 2074 materials strictly within the scope and tier specified in their license. Licenses may include obligations concerning reporting frequency, digital integration adherence, consent governance, fee policies, and ethics liaison duties. Territory and sector restrictions remain binding; Partners shall not imply global authority where authorization is regional or sectoral.

Licenses incorporate:

Licensing Element	Obligation	Note
Scope	Use limited to approved model(s), pillars, and geography	Expansion requires re-application
Term	Valid for defined period with continuous compliance	No automatic renewal
Conditions	Ethics controls, QA, CPD, digital governance	Breach triggers remediation or suspension
Revocability	Revocable for material non-compliance	GSIA may recommend revocation
Reporting	Surveillance metrics, ethics attestations	Frequency based on tier and risk grade

10.2 Intellectual Property (IP) Use

Agenda 2074 retains full ownership of all standard texts, canonical interpretations, visual marks, badges, star icons, and associated registries. Partners receive limited reproduction rights for operational and disclosure purposes.

Permitted uses include:

- Display of Agenda 2074 star icons, badges, or attestations only where the subject entity has provided explicit, informed, and revocable consent.
- Use of textual descriptions of the model (e.g., “Validated under the A2074-SRS Open Standard”).
- Internal copies of frameworks for staff training.

Prohibited uses include:

- Altering official icons, badges, or textual identifiers.
- Using A2074 marks in promotional materials in a manner implying exclusivity, ownership, or custodial authority.
- Representing A2074 validation as an ISO certification or equivalent.
- Using badges or icons in marketing targeted at third parties without subject consent.

10.3 Branding and Co-Branding Rules

Brand integrity requires consistent global presentation. Partners must:

- Use only approved iconography from the Agenda 2074 Brand Asset Catalogue.
- Display badges with scope, duration, and version identifiers.
- Ensure that subject-opted disclosures reflect the precise model and pillar mapping.

Co-branding—use of both Partner and Agenda 2074 branding—is permitted only for:

1. Approved validation results disclosed with consent;
2. Partner webpages that explain the licensed model;
3. Registry listings under Agenda 2074 governance.

Co-branding is prohibited for advertising unrelated services (e.g., consulting, lobbying, software sales).

10.4 Public Communications
All public communications must comply with the Communication & Public Disclosure Protocol. In particular:

- No implication that disclosure is expected, preferred, or advantageous.
- No suggestion that consent is permanent or irrevocable.
- No league tables, comparative rankings, or “top performer” narratives.
- No claims that validation constitutes certification, rating, or guarantee by Agenda 2074.

Partners must maintain an accessible branding compliance log documenting the use of Agenda 2074 assets, templates, and messages.

Violations—including unauthorized use of marks, misleading narratives, coercive messaging, or ISO equivalence claims—constitute material breaches and may result in immediate injunctive correction, public clarification, license conditions, suspension, or withdrawal.

Nothing in this Chapter authorizes disclosure without consent or any diminution of patient-level confidentiality.

Chapter 11 — Commercial Terms, Fees, and Reporting

This Chapter establishes mandatory commercial principles, fee governance rules, and financial reporting obligations for all Validation Partners operating under the A2074-SRS. It ensures that all commercial arrangements uphold the structural rights codified in the Foundational Charter—particularly non-retaliation, proportionality, and patient-level confidentiality—and prevent the emergence of coercive or distortionary economic incentives.

All Partners shall operate on a **cost-recovery and reasonable-margin** basis appropriate to their scope and tier. Fee structures must be transparent, predictable, non-coercive, and accessible to microenterprises, SMEs, public bodies, civil-society organizations, and cross-border entities, respecting proportionality and contextual capacity. No fee arrangement may create incentives that undermine impartiality, influence outcomes, or pressure subjects into disclosure.

11.1 Fee Principles
Partners shall implement a fee model consistent with the following principles:

Fee Principle	Required Standard	Prohibited Conduct
Transparency	Publish fee schedules, tiering, and hardship provisions	Hidden fees; undisclosed surcharges
Proportionality	Fees calibrated to archetype and scope; microenterprise access required	Excessive burdens; uniform pricing regardless of size
Non-Retaliation	Non-disclosure must not increase fees or restrict access	Upcharging for private results; discounted “public” fees
Non-Contingency	No outcome-based fees; no “pay-for-stars”	Any compensation linked to results or disclosure
Accessibility	Hardship schemes for civil society and resource-constrained public entities	Denial of service based on financial capacity (absent risk-justified grounds)
Compliance Alignment	Fees must support CPC obligations (competence, privacy, consent governance)	Subsidy conditional on publicity or marketing participation

Partners may apply reasonable indexation or regional adjustments but must disclose rationale and remain within the bounds of fairness and accessibility.

11.2 Engagement Contracts
Engagement contracts must:

1. Entrench patient-level confidentiality as a binding contractual right.
2. Specify that disclosure is voluntary, explicit, informed, and revocable.
3. Include ISO 26000 non-equivalence disclaimers.
4. Outline scope, method version, retention logic, and expected timelines.
5. Include non-retaliation clauses and accessible complaint routes.
6. Reflect approved fee schedules without hidden charges.

Any contract term inconsistent with superior A2074 instruments is void and remediable under GSIA jurisdiction.

11.3 Revenue-Sharing and Registry Fees
Revenue-sharing arrangements, where permitted by Agenda 2074, shall apply only to:

- Registry maintenance costs,
- Brand stewardship,
- Methodological research and development,
- Affordability funds administered by GSDA.

Revenue-sharing may not create preferential treatment, referral incentives, or dependency relationships between Partners that risk impairing independence.

11.4 Financial Reporting Duties
To preserve transparency and systemic trust, Partners must submit periodic financial reports to Agenda 2074 and GSIA. Reporting frequency corresponds to accreditation tier and risk grade.

Reporting Item	Tier I	Tier II	Tier III
Annual financial statement (non-public)	Required	Required	Required
Mid-year revenue/fee update	Required	Required	Optional
Breakdown of subsidized engagements	Required	Required	Required (if subsidies used)
COI-triggering financial relationships	Required	Required	Required
Internal audit report on fee compliance	Annual	Biennial	As requested
GSIA-requested special review	Mandatory	Mandatory	Mandatory

Financial statements need not be public, but Agenda 2074 may publish aggregated, anonymized financial summaries to support transparency without identifying Partners or subjects.

11.5 Commercial Practices and Marketing
All commercial messaging must adhere to the Communication & Public Disclosure Protocol. Partners must not imply:

- Guaranteed outcomes,
- Preferential scoring,
- ISO certification or equivalence,
- Comparative ranking or performance tiering,
- That public disclosure is commercially advantageous or expected.

Violation of these rules constitutes material non-compliance remediable under Chapter 12.

Chapter 12 — Non-Compliance, Suspension, and Withdrawal

This Chapter establishes the remedial and enforcement framework for addressing non-compliance by Validation Partners. It is grounded in the supremacy of patient-level confidentiality, proportionality, and ethics enforcement under GSIA. Non-compliance may be technical, procedural, ethical, digital-security related, or structural. The severity of the response is calibrated to the risk presented, the nature of the violation, and the Partner’s remediation record.

12.1 Categories of Non-Compliance

Non-compliance is categorized as follows:

Category	Description	Examples
Technical Non-Compliance	Failure to adhere to methodological or procedural standards	Incorrect sampling; outdated method version; defective aggregation
Ethics Non-Compliance	Violations of confidentiality, non-retaliation, or consent governance	Coerced disclosure; unauthorized public listing; retaliation
Digital-Security Non-Compliance	Breaches of data handling rules or AI oversight duties	Unencrypted storage; AI adverse decision without human review
Independence/COI Non-Compliance	Breaches of independence or conflict-of-interest controls	Undisclosed advisory relationship; outcome-contingent fees
Financial Non-Compliance	Violations of fee rules or improper financial incentives	“Pay-for-stars”; disclosure-linked discounts
Structural Non-Compliance	Persistent failures undermining integrity of the Partner’s function	Chronic QA failures; governance collapse; refusal to cooperate

12.2 GSIA-Ordered Remediation

GSIA may order corrective actions tailored to the severity and nature of the breach. Remedies include:

Remedy Type	Description	Typical Triggers
Corrective Actions	File-level rework; consent correction; sampling recalibration	Technical errors; incorrect disclosures
Protective Measures	Injunctive relief; consent takedown; non-retaliation orders	Unauthorized publication; threat of retaliation
Process Redesign	Re-engineering of consent workflows, QA processes, AI guardrails	Systemic flaws; repeated process defects
Personnel Actions	Recusals; retraining; reassignment; disciplinary measures	Assessor misconduct; COI breach
Independent Monitoring	Appointment of an external monitor for defined period	Recurring ethics violations; high-risk remediation
Financial Remediation	Fee refunds; hardship adjustments; economic correction	Coercive pricing; prohibited discounts

Temporary Conditions	Restrictions on scope, caseload, or method variety	Early-stage Partners; post-incident stabilization

GSIA shall determine the proportionality of remedies based on severity, recurrence, cooperation level, and impact on subjects.

12.3 Suspension
Suspension is a temporary but serious measure, invoked where non-compliance presents active risk to subjects, public interest, or system integrity. During suspension:

- No new engagements may be opened.
- All public disclosures must be frozen or withdrawn (subject to consent).
- Existing engagements may continue only under strict GSIA supervision.
- The Partner must submit a corrective action plan within the timeframe specified.

Suspension normally precedes revocation unless the breach is so egregious that immediate withdrawal is required.

12.4 Withdrawal (Revocation)
Withdrawal terminates the Partner's license and authorisations. Grounds include:

- Egregious ethics violations (e.g., intentional unauthorized disclosure),
- Persistent non-cooperation,
- Structural collapse of governance or QA,
- Material misrepresentation during application,
- Continued operation while suspended,
- Use of A2074 marks in fraudulent or misleading ways.

Upon withdrawal:

- All A2074 marks, badges, icons, and references must be removed immediately.
- Subjects must be notified, including rights to request record transfers or deletion.
- Agenda 2074 may appoint an interim Partner or provide transition guidance to ensure continuity of service for affected subjects.
- Re-application is barred for a minimum period defined in the decision notice (typically two to five years), subject to GSIA concurrence.

12.5 Public Statements
Agenda 2074 may issue anonymized public statements concerning systemic issues revealed through Partner non-compliance. Named disclosures about a specific Partner are issued only when necessary to:

1. Prevent ongoing harm,
2. Correct materially misleading public information, or

3. Comply with applicable law.

No subject entity's validation results may be disclosed in such statements without consent.

12.6 Interaction with Appeals
Suspension or withdrawal may be appealed under Chapter 13. Appeals do not automatically stay enforcement unless GSIA determines that a limited stay does not pose a risk to subjects or public interest.

Chapter 13 — Appeals, Reinstatement, and Due Process

This Chapter establishes the procedural guarantees available to Validation Partners subject to adverse actions under this Framework, including corrective orders, license conditions, suspension, or withdrawal. It preserves the supremacy of patient-level confidentiality, non-retaliation, and ethical integrity while ensuring that Partners receive fair notice, meaningful opportunity to be heard, and proportionate review mechanisms. The procedures herein apply to all licensing decisions, GSIA determinations, and Agenda 2074 actions that materially affect a Partner's rights or obligations.

All adverse actions begin with the issuance of a written notice specifying: (i) the factual basis of the alleged non-compliance; (ii) the provisions of the Charter or this Framework implicated; (iii) the rights of the Partner to respond; and (iv) any interim protective measures imposed to safeguard subjects or system integrity. Notices shall be sufficiently detailed to permit an informed response, without disclosing confidential subject results beyond what is strictly necessary for the adjudicative process. Where confidentiality constraints prevent disclosure of specifics, GSIA may provide summaries or anonymised patterns that preserve due process without compromising privacy.

Partners shall have a meaningful opportunity to respond, including submission of explanations, documentary evidence, remedial plans, and, where appropriate, sworn declarations from responsible officers. GSIA may convene a hearing—virtual or in person—where complex factual disputes, ethical concerns, or systemic implications are present. Hearings are non-public, with records maintained under strict confidentiality. The Partner may be represented by counsel or authorised officers, may call witnesses with GSIA approval, and may request reasonable accommodations where necessary to preserve fairness.

Following review, GSIA shall issue a reasoned determination addressing each material issue, including factual findings, legal and ethical reasoning, and the remedies imposed. Determinations shall respect proportionality and shall demonstrate how patient-level rights, non-retaliation, and public-interest safeguards were considered. Where GSIA imposes conditions, suspension, or withdrawal, the determination shall specify remedial pathways, timelines for compliance, and whether limited or supervised operation may continue during the remedy period. Determinations shall be issued in writing and form part of the Partner's confidential ethics record.

Appeals may be filed to the Agenda 2074 Appeals Panel within the time specified in the determination notice. The Panel reviews for procedural fairness, proportionality, sufficiency of evidence, alignment with canonical interpretations, and adherence to GSIA's mandated independence. The Panel may affirm, reverse, modify, or remand the determination with instructions. Remand may include requirements for supplemental fact-finding, enhanced confidentiality protections, or adjusted remedy timelines. Appeals do not automatically stay enforcement; however, the Panel may grant a limited stay where necessary to prevent irreparable harm and where such stay does not endanger subjects or public interest.

Reinstatement of a suspended or withdrawn Partner requires demonstration of full remediation of all identified issues, establishment of durable controls to prevent recurrence, completion of any required training or governance reforms, and, where applicable, successful completion of a supervised pilot period. For withdrawals, reinstatement is contingent upon expiry of the minimum ineligibility period specified in the withdrawal notice and affirmative GSIA concurrence that reinstatement poses no foreseeable risk to confidentiality, ethics, or integrity. Reinstatement may be conditional, requiring enhanced reporting, independent monitoring, periodic ethics attestations, pre-clearance of communications, or reduced scope and tier until sustained compliance is demonstrated.

Nothing in this Chapter authorizes disclosure of subject-level validation results during appeal or reinstatement proceedings. All proceedings shall preserve confidentiality and autonomy, and shall not give rise to negative inference concerning subjects or participating enterprises. Records of appeals or reinstatement decisions may be used for anonymised systemic learning, but not for public identification of the Partner absent legal necessity or explicit consent.

The due-process regime established here ensures that enforcement actions are not arbitrary, that Partners retain meaningful recourse, and that system integrity is preserved without compromising the structural rights embedded in the A2074-SRS.

Final Word

This Licensing and Accreditation Framework constitutes the authoritative regulatory architecture for determining who may operate validation systems under the Agenda 2074 Social Responsibility Standard, how those systems must be designed, and the safeguards required to protect subjects, uphold ethical integrity, and maintain global consistency. Together with the Foundational Charter, it establishes a disciplined and rights-preserving model in which methodological innovation is encouraged, provided canonical fidelity is maintained and patient-level confidentiality remains inviolable.

The Framework ensures that Validation Partners operate with competence, independence, proportionality, and transparency; that methodologies are rigorously reviewed and continuously improved; that ethics oversight by GSIA is structurally protected; and that the economic and digital architectures supporting validation activities remain free of coercive incentives, comparative distortions, and undue influence. It preserves a global custodial standard that is adaptable to local context yet anchored in a universal canon of 17 Social Global Goals.

As the A2074-SRS expands across regions, sectors, and institutional families, this Framework ensures that the trust placed in validation remains justified, that every participant—microenterprise, public body, cooperative, or multinational—is treated fairly and proportionately, and that the standard retains its legitimacy as a public-interest instrument. It affirms the core principle that meaningful social responsibility cannot be compelled by coercion or comparison, but is strengthened through autonomy, confidentiality, ethical governance, and structured improvement.

Document 2 stands as one of the pillars of the Agenda 2074 system. It is issued to guide those entrusted with the operation of validation models and to guarantee that the standard remains credible, accessible, and aligned with the overarching doctrine that under Agenda 2074, everyone can do something.