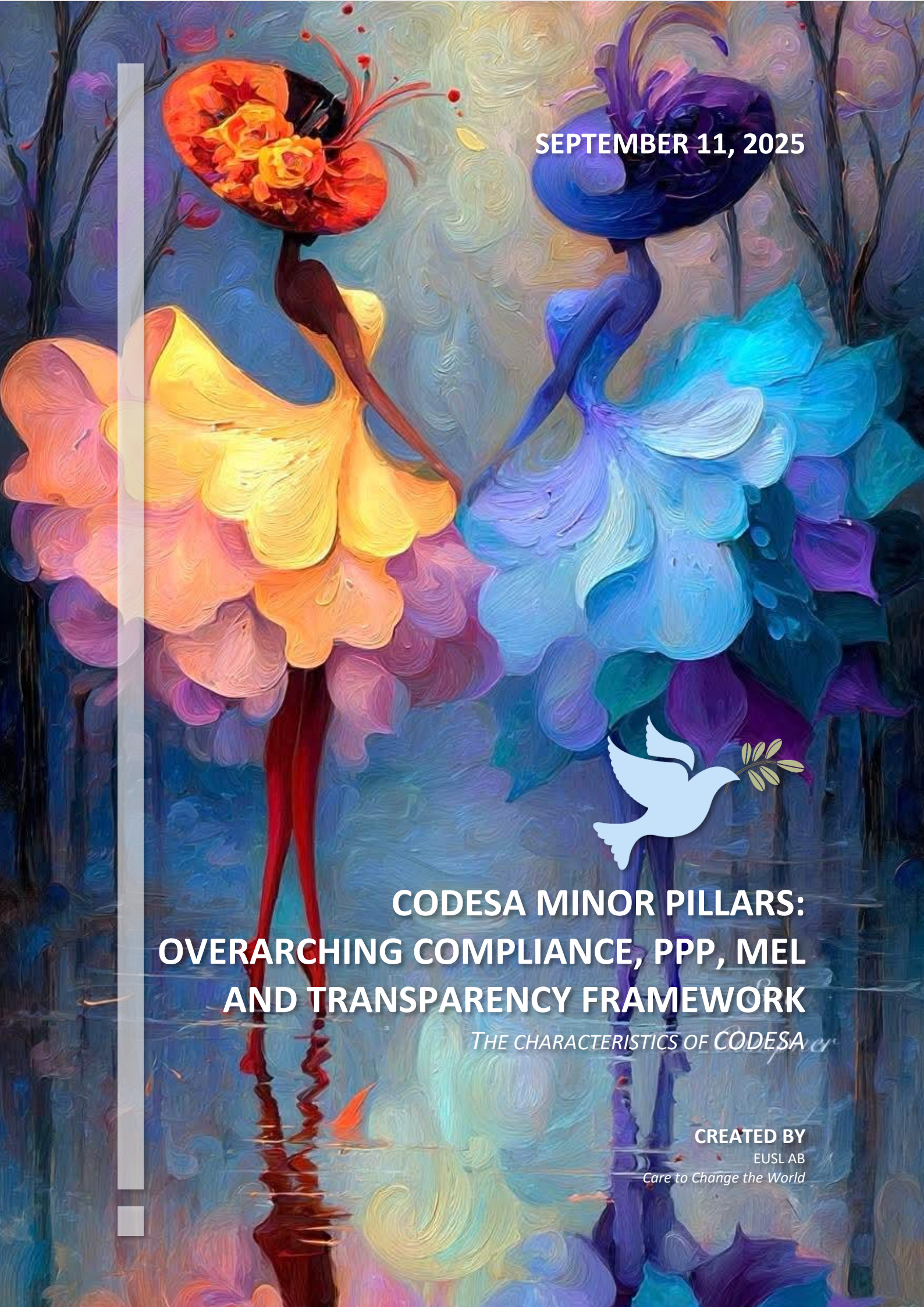


An impressionistic painting featuring two stylized flowers. On the left, a flower with a dark red stem and a large, vibrant yellow and orange bloom. On the right, a flower with a dark blue stem and a large, light blue and purple bloom. A white dove is depicted in flight, carrying a small olive branch in its beak. The background is a mix of soft, blended colors like blue, green, and yellow, with visible brushstrokes. The overall mood is peaceful and artistic.

SEPTEMBER 11, 2025

CODESA MINOR PILLARS: OVERARCHING COMPLIANCE, PPP, MEL AND TRANSPARENCY FRAMEWORK

THE CHARACTERISTICS OF CODESA

CREATED BY

EUSL AB

Care to Change the World

Table of Contents

Executive Abstract	2
Institutional Context, Scope, and Rationale	2
3. Legal Basis and Governance under GSIA Membership	4
4. PPP Governance Rules	6
5. Procurement Integrity and Market Transparency (OCDS)	8
6. Fiduciary Management, IPSAS/ISA, and Internal Control	9
7. Environmental and Social Safeguards (ISS 2024)	11
8. Stakeholder Engagement, Grievance and Accountability	11
9. Data Protection, Cybersecurity and Digital Rights	12
10. Risk and Incident Management	13
11. Ethical Posture and “No War” Principle	13
12. Communications and Proactive Disclosure	14
13. Implementation Roadmap and Gate Reviews	15

CODESA Minor Pillars – Overarching Compliance, PPP, MEL and Transparency Framework

Executive Abstract

This document consolidates the Minor Pillars—cross-cutting policy and control instruments that apply uniformly across all Major Pillars and program streams (including Power Play, SDEP/SFPSEI, Digitalisation/DPI, and the Digital & Social Innovation Academy). The Minor Pillars translate the GSIA – Flowhub Trio Plus compliance architecture into enforceable program rules for: public–private partnership governance; procurement integrity and market transparency; fiduciary controls and audit; environmental and social safeguards (including SEA/SH); data protection, cyber-security, and digital rights; stakeholder engagement and grievance; MEL and result verification; risk and incident management; beneficial ownership and sanctions screening; and strategic communications and disclosure. Each pillar is implemented as a membership obligation under GSIA, enforced by Flowhub’s non-bypassable process gates, audit-ready evidence chains, and default Open Contracting Data Standard (OCDS) publication across the full contracting cycle. Flowhub integrates a sovereign, federated platform stack (Municipio + Microsoft Purview + Zero Trust + Nextcloud) so that no payment is released without a digitally verified link to an approved procurement action, a certified deliverable, and the required public disclosures. [\[GSIA - Flo...Trio Plus\]](#), [\[Open Contr...a Standard\]](#), [\[Microsoft...soft Learn\]](#), [\[SP 800-53...ystems ...\]](#)

The Minor Pillars are expressly aligned with the African Development Bank (AfDB) policy framework that governs regional operations, procurement, and safeguards, including the Updated Integrated Safeguards System (ISS) which became effective on 31 May 2024 and strengthens requirements for community health and safety, SEA/SH prevention and response, stakeholder engagement and value-chain oversight. They also embed the AfDB’s risk-based, value-for-money procurement doctrine (2015 Procurement Policy) and adopt IPSAS/ISA for financial reporting and external audit. Collectively, they deliver a compliance-by-design regime that reconciles sovereign country-window financing with uniform, independently operated controls across participating states. [\[African De...System ...\]](#), [\[PROCUREMENT...OPERATIONS\]](#), [\[GSIA - Flo...Trio Plus\]](#)

The document is intended for COMESA policy organs, ACTESA, participating RMCs, AfDB departments and co-financiers. It should be read as the overarching instrument under which program-specific manuals and operating procedures are harmonized and disclosed through the Flowhub portal and OCDS feeds, ensuring comparability, portability, and public accountability across the portfolio. [\[GSIA - Flo...Trio Plus\]](#)

Institutional Context, Scope, and Rationale

Context and anchoring. The Minor Pillars sit above the Major Pillars as a single, Community-level compliance and PPP framework operated by GSIA and instrumented through Flowhub Trio Plus. GSIA’s model is a dual component: a Membership Framework (membership covenant + Country Fiduciary Compacts) and a digital control environment (Flowhub) that enforces obligations through role-based workflows, immutable audit trails, and machine-readable disclosure. The arrangement preserves sovereign country-window financing while standardising fiduciary, procurement, E&S and data-governance practice across jurisdictions in line with AfDB’s regional-operations architecture. [\[GSIA - Flo...Trio Plus\]](#)



Scope and coverage. The Minor Pillars establish the following cross-cutting regimes, each defined in subsequent chapters and parameterised for program-specific application in Flowhub:

1. **PPP Governance and Control** (composition, decision rights, prior/post review, conflict-of-interest, disclosure).
2. **Procurement Integrity and Market Transparency** (open competition default; standstill and debriefing; beneficial ownership; sanctions and cross-debarment screening; **OCDS** planning–tender–award–contract–implementation publication). [\[PROCUREMENT...OPERATIONS\]](#), [\[Open Contr...a Standard\]](#)
3. **Fiduciary Management, IPSAS/ISA and Internal Control** (ring-fenced designated accounts; direct-payment default; quarterly IFRs; annual ISA audits; COSO-consistent controls). [\[GSIA - Flo...Trio Plus\]](#)
4. **Environmental and Social Safeguards** (ISS 2024 baseline; ESIA/ESMP/LMP/SEP registers; high-risk third-party review; 48-hour incident escalation; SEA/SH survivor-centred protocols). [\[African De...System ...\]](#), [\[GSIA - Flo...Trio Plus\]](#)
5. **Stakeholder Engagement, Grievance and Accountability** (SEP plans, safe channels, non-retaliation, community disclosure). [\[GSIA - Flo...Trio Plus\]](#)
6. **Data Protection, Digital Rights, and Cybersecurity** (COMESA privacy policy integration; **Zero Trust** identity/device/data controls; **Microsoft Purview** assessments and evidence; sovereign **Nextcloud** storage with GDPR-style resilience). [\[Microsoft...soft Learn\]](#), [\[SP 800-53...ystems ...\]](#), [\[GSIA - Flo...Trio Plus\]](#)
7. **MEL and Results Verification** (indicator baselines and disaggregation; quarterly/annual reporting; independent mid-term and final evaluations; Flowhub dashboards). [\[GSIA - Flo...Trio Plus\]](#)
8. **Risk and Incident Management** (fiduciary/procurement/E&S/SEA-SH/cyber forms; triage; remedies; public outcome notes). [\[GSIA - Flo...Trio Plus\]](#)
9. **Communications and Proactive Disclosure** (OCDS feeds; non-confidential safeguards and financial extracts; crisis communications protocols; portfolio dashboards). [\[Open Contr...a Standard\]](#), [\[GSIA - Flo...Trio Plus\]](#)
10. **Ethical Posture and Conflict-Sensitivity** (codifying values-based commitments—e.g., “No War”—as operational conflict-sensitivity, do-no-harm and exclusion lists, enforceable through procurement and partner due-diligence gates). [\[GSIA - Flo...Trio Plus\]](#)

Why a single, overarching instrument. Fragmented manuals and country-by-country variance increase fiduciary, safeguard, and reputational risk and consume scarce supervision bandwidth. GSIA’s consolidated approach—membership covenant + Flowhub control plane—standardises process gating and disclosure, enables comparative analytics (including red-flagging through OCDS data), and lowers the cost and time to reach first disbursement. It also provides AfDB and co-financiers a uniform, auditable view of procurement, milestones, incidents, and remedial actions across sovereign windows, in line with the Bank’s procurement policy and the ISS update’s emphasis on community health and safety, SEA/SH response and stakeholder engagement. [\[PROCUREMENT...OPERATIONS\]](#), [\[African De...System ...\]](#), [\[Open Contr...a Standard\]](#)



Technology as the compliance spine. The Minor Pillars are not declarative: they are **operationalised** in Flowhub. Role-based workflows, prior/post-review controls, sanctions/beneficial-ownership checks, acceptance and payment gates, privacy-by-design, and **Purview** evidence packs are embedded at each step. A federated design ensures **data sovereignty** at RMC level while preserving regional oversight and disaster-recovery posture; non-bypassable gates enforce that **no payment** occurs without compliant procurement, verified deliverables, and required disclosures. Security and privacy controls are benchmarked to **NIST SP 800-53 Rev. 5** and audited through Purview's control assessments and evidence repositories. [\[GSIA - Flo...Trio Plus\]](#), [\[Microsoft...soft Learn\]](#), [\[SP 800-53...ystems ...\]](#)

Interface with Major Pillars and programs. The Minor Pillars apply **horizontally**. For example, in SDEP/SFPSEI they bind ACTESA value-chain procurements and warehouse-receipt operations to OCDS, ISS, and incident protocols; in Power Play and Digitalisation they bind corridor/DPI packages to open tendering, standstill/debriefing, data-protection, and DPI security conformance; in the Academy they govern provider accreditation, assessment integrity, learner-data privacy, and publication of MEL. The public record across all streams is consolidated via Flowhub portals and OCDS feeds for competition, scrutiny, and learning.

3. Legal Basis and Governance under GSIA Membership

3.1. Nature and effect of the Minor Pillars.

The Minor Pillars constitute a single, Community-level compliance instrument that is binding on all participating sovereign country windows, implementing agencies, and private partners by virtue of accession to the **GSIA Membership Framework** and execution of the relevant **Country Fiduciary Compacts**. By design, they operate as uniform, enforceable programme rules across multi-country operations, and are implemented through the non-bypassable control gates and machine-readable disclosures of **Flowhub Trio Plus**. This construct preserves sovereign financing at country level while standardising fiduciary, procurement, environmental and social safeguards, data-governance, and disclosure practices, consistent with the GSIA architecture described in the *GSIA – Flowhub Trio Plus* white paper. [\[GSIA - Flo...Trio Plus\]](#)

3.2. Source of obligations and hierarchy of instruments.

The following legal sources are incorporated **by reference** and govern in the order stated where applicable law permits: (i) the GSIA Charter and **Membership Agreement**; (ii) the **Country Fiduciary Compact** and its annexes (including the PPP Annex, Disclosure Schedule, Data-Processing Addendum, and Integrity Pact); (iii) the **AfDB Procurement Policy for Bank Group-Funded Operations (2015)** and the Bank's integrity framework (sanctions and cross-debarment); (iv) the **Updated Integrated Safeguards System (ISS)** of the African Development Bank, effective **31 May 2024**; and (v) the **Open Contracting Data Standard (OCDS)** for full-cycle contracting publication. Programme-specific manuals must be harmonised to this hierarchy and are monitored and enforced in Flowhub. [\[GSIA - Flo...Trio Plus\]](#), [\[PUBLICATIO.... - COMESA\]](#), [\[Welcome -...genda 2063\]](#), [\[COMESA fin...- ZBC NEWS\]](#)

3.3. Parties and privity.

The parties to the GSIA regime comprise the Regional Economic Community institutions and specialised agencies performing coordination and technical leadership (including ACTESA), each participating Regional Member Country acting through its designated implementing entity, and private partners admitted to the programme. Rights and obligations are codified in the **Membership Agreement** (including representational rights in the General Assembly) and in the **Country Fiduciary Compact**, which binds national windows to Flowhub's control plane and to open-contracting disclosure as conditions of participation. [\[GSIA - Flo...Trio Plus\]](#)



3.4. Flowhub as the control plane; auditability and evidence.

Flowhub Trio Plus is the compliance operating system that enforces the Minor Pillars through role-based workflows, immutable audit trails, and publication engines. Its federated design provides each country with a sovereign instance while interconnecting all instances to GSIA's compliance hub for portfolio-level oversight. No disbursement is effected unless the contracting, delivery, and payment gates are satisfied and the corresponding OCDS releases are published. Evidence packs, prior- and post-review files, and corrective-action registers are maintained in **Microsoft Purview Compliance Manager** and surfaced to supervision missions as audit-ready dossiers. [\[GSIA - Flo...Trio Plus\]](#), [\[COMESA COM...- ENGLISH\]](#)

3.5. Data-protection and cybersecurity posture.

All learner, bidder, contractor, and project records processed by Flowhub are handled under a documented privacy programme aligned to the Community's policy environment and benchmarked to recognised control catalogues. Identity, device, and data protections follow a **Zero Trust** model; technical and organisational controls are mapped to **NIST SP 800-53 Rev. 5**; and evidentiary artefacts, logs, and registries are retained under immutability and least-privilege access. Sovereign data residency and resilience are achieved through the platform's federated hosting and 3-2-1 backup posture. [\[GSIA - Flo...Trio Plus\]](#), [\[PPP Refere...artnership\]](#)

3.6. Procurement integrity and market transparency.

All programme procurement adheres to the **AfDB Procurement Policy (2015)**, including its value-for-money and risk-based prior/post-review doctrine. The Minor Pillars make **OCDS publication** a default condition of participation, ensuring machine-readable releases at planning, tender, award, contract, and implementation stages; beneficial ownership disclosure and sanctions/cross-debarment screening are mandatory pre-award checks. [\[PUBLICATIO... - COMESA\]](#), [\[COMESA fin...- ZBC NEWS\]](#)

3.7. Safeguards and social licence.

The **ISS (2024)** is adopted as the safeguards baseline, with explicit operationalisation of strengthened requirements for community health and safety, SEA/SH prevention and response, stakeholder engagement, and value-chain oversight; high-risk activities trigger independent review. Flowhub maintains digital registers for ES instruments, incidents, and corrective actions, with time-bound escalation and public release of non-confidential summaries. [\[Welcome -...genda 2063\]](#), [\[GSIA - Flo...Trio Plus\]](#)

3.8. PPP-specific legal coherence and dispute resolution.

For PPPs, the Minor Pillars recognise national PPP statutes and contracting authorities while ensuring coherence with international guidance, notably the **World Bank PPP Reference Guide 3.0** and the **UNCITRAL Legislative Guide and Model Legislative Provisions on PPPs**. Disputes under the Membership Agreement or Country Fiduciary Compact are resolved by **independent dispute resolution under UNCITRAL rules**, without prejudice to project-level dispute boards and lender step-in rights codified in Direct Agreements. [\[PPP Refere...artnership\]](#), [\[UNCITRAL L...rtnerships\]](#), [\[GSIA - Flo...Trio Plus\]](#)

3.9. Governance bodies and decision rights.

Strategic oversight is exercised by GSIA organs as defined in the Charter and Membership Agreement, including a General Assembly and delegated committees. Operationally, roles are defined as follows: the **AfDB** performs prior/post review and supervision; **RMC implementing agencies/PMUs** execute day-to-day activities in Flowhub; **ACTESA** leads technical harmonisation and cross-country synthesis;

and **GSIA** configures and enforces controls, manages OCDS publication, and consolidates reporting for the public portal and co-financiers. [\[GSIA - Flo...Trio Plus\]](#)

3.10. Remedies, termination, and publication duties.

Material non-compliance may result in suspension of disbursements, contract termination, recovery, debarment referral, and public reporting of outcomes. Publication duties follow the Disclosure Schedule, with narrowly tailored redactions grounded in law; failure to publish constitutes a curable breach that can escalate to suspension in the event of persistent default. [\[GSIA - Flo...Trio Plus\]](#)

4. PPP Governance Rules

4.1. Purpose and scope.

These rules establish uniform, enforceable standards for the identification, appraisal, procurement, contracting, and oversight of public–private partnerships implemented under sovereign country windows but supervised through GSIA’s control environment. They complement national PPP laws and regulations and are grounded in internationally recognised guidance on institutional frameworks, value for money, fiscal risk management, and integrity. [\[PPP Refere...artnership\]](#), [\[Public Gov...rtnerships\]](#)

4.2. Institutional framework and authorisations.

PPP proposals must originate from or be endorsed by the competent line ministry and the national PPP unit where established; they must demonstrate consistency with sector strategies and fiscal frameworks and include an assessment of contingent liabilities and guarantees. The **OECD Principles for Public Governance of PPPs** require that a clear, legitimate institutional framework is supported by competent authorities; the PPP Reference Guide details the need for defined policy, processes, institutions, and rules that promote good governance of a PPP programme. These requirements are transposed into Flowhub approvals and checklists, making authorisations auditable and visible. [\[Public Gov...rtnerships\]](#), [\[PPP Refere...artnership\]](#)

4.3. Project preparation and appraisal.

Each PPP must present a structured appraisal that includes options analysis, affordability tests, **value for money (VfM)** assessment, risk allocation matrices, environmental and social due diligence in line with the **ISS (2024)**, and stakeholder-engagement plans proportionate to risk. Flowhub registers these artefacts and blocks market sounding or launch of procurement until required evidence and approvals are complete. [\[PPP Refere...artnership\]](#), [\[Welcome -...genda 2063\]](#)

4.4. Procurement route, integrity, and competition.

Selection methods must comply with the **AfDB Procurement Policy (2015)**, privileging competitive approaches that maximise contestability and VfM; any direct negotiation route requires documented justification, prior review, and publication of reasoning. **OCDS** is mandatory from planning through implementation, enabling market visibility, red-flag analytics, and third-party scrutiny; beneficial ownership declarations and sanctions/cross-debarment screening are compulsory at bid and pre-signature stages. Standstill periods and debriefings are codified and enforceable through Flowhub’s award gate. [\[PUBLICATIO... - COMESA\]](#), [\[COMESA fin...- ZBC NEWS\]](#)

4.5. Contract structure and risk allocation.

PPP contracts must: (i) allocate risks to the party best able to manage them; (ii) codify performance-based payment mechanisms and tariff/availability regimes with transparent indexation and change-in-law clauses; (iii) set inspection, testing, and acceptance regimes, including **environmental and social management plan (ESMP)** obligations as payment pre-conditions; and (iv) include **Direct Agreements** with lenders that provide step-in rights, cure periods, and assignment

mechanics. The **UNCITRAL Legislative Guide and Model Legislative Provisions** provide model formulations for these clauses and institutional responsibilities. [\[UNCITRAL L...rtnerships\]](#)

4.6. Fiscal commitments, government support, and transparency.

Government support instruments (guarantees, comfort letters, availability payments, minimum-revenue undertakings, tax and customs arrangements) must be approved through the national budget process and disclosed; contingent liabilities are to be monitored in Flowhub, and summaries published in accordance with the Disclosure Schedule. The **OECD Principles** emphasise using the budgetary process transparently to minimise fiscal risks; Flowhub captures the approvals and makes them auditable. [\[Public Gov...rtnerships\]](#)

4.7. Safeguards, stakeholder engagement, and grievance.

The **ISS (2024)** is binding on PPPs; ESIA/ESMP/LMP/SEP instruments are prepared, disclosed, and tracked in Flowhub with 48-hour incident escalation. Stakeholder engagement follows documented SEP plans; grievance mechanisms are safe, accessible, and non-retaliatory. High-risk activities trigger independent expert review before financial close and at major variations. [\[Welcome -...genda 2063\]](#)

4.8. Data protection, DPI interfaces, and cybersecurity.

Where PPPs operate or interconnect with **digital public infrastructure**, operators must implement privacy-by-design, conditional access, encryption at rest and in transit, and logging consistent with **NIST SP 800-53 Rev. 5** control families; evidence of control effectiveness is maintained and scored in **Microsoft Purview Compliance Manager** and forms part of periodic compliance statements. [\[PPP Refere...artnership\]](#), [\[COMESA COM...– ENGLISH\]](#)

4.9. MEL, contract management, and performance remedies.

KPIs, baselines, and reporting intervals are contractually defined and mirrored in Flowhub dashboards. Payment is contingent on verified milestones and compliance with ESMP obligations; chronic under-performance triggers liquidated damages, performance security enforcement, step-in, or termination per contract. Mid-term and final evaluations use recognised criteria and are published in non-confidential form on the programme portal. The **PPP Reference Guide 3.0** emphasises disciplined contract management and performance monitoring as a condition for PPP efficacy. [\[PPP Refere...artnership\]](#), [\[GSIA - Flo...Trio Plus\]](#)

4.10. Integrity, conflicts, and “No War” ethic.

Conflicts of interest are prohibited and disclosed through mandatory declarations by officials and bidders; GSIA integrates sanctions and cross-debarment screening and requires public beneficial-ownership disclosures. The programme’s ethical posture—expressed for communication purposes as “No War”—is operationalised through conflict-sensitivity screening, exclusion lists for sanctioned entities, and incident protocols for intimidation or violence affecting sites or stakeholders, all captured and escalated in Flowhub. [\[GSIA - Flo...Trio Plus\]](#)

4.11. Publication and exceptions.

OCDS publication is mandatory at plan, tender, intended award (standstill), signature, amendment, and quarterly implementation status (milestones, payments, variations). Exceptions are strictly limited, time-bound, and recorded with legal bases for redaction. The publication cadence, formats, and quality controls are specified in the Disclosure Schedule and enforced by Flowhub’s release engine. [\[COMESA fin...- ZBC NEWS\]](#), [\[GSIA - Flo...Trio Plus\]](#)



4.12. Dispute resolution and enforcement.

Project-level disputes are addressed first through contractually required dispute boards and expert determination mechanisms, with escalation to arbitration as provided by the PPP contract; membership-level disputes proceed under **UNCITRAL** rules. GSIA may recommend suspension of programme privileges for persistent breaches and will publish non-confidential outcomes to sustain market integrity. [\[UNCITRAL L...rtnerships\]](#), [\[GSIA - Flo...Trio Plus\]](#)

5. Procurement Integrity and Market Transparency (OCDS)

Purpose and applicability. This chapter codifies a uniform, enforceable regime for end-to-end procurement integrity and market transparency across all programme streams and country windows. It incorporates the African Development Bank's Procurement Policy for Bank Group-Funded Operations (2015)—including its value-for-money, fit-for-purpose, and risk-based prior/post-review doctrine—and mandates Open Contracting Data Standard (OCDS) publication for the full contracting cycle. All obligations are implemented through Flowhub Trio Plus gates and are binding via the GSIA Membership Agreement and Country Fiduciary Compacts. [\[AfCFTA – T...ompetition\]](#), [\[Programme...AUDA-NEPAD\]](#), [\[PPP Refere...artnership\]](#)

Operating principles. Open competitive procurement is the default market approach. Restricted or direct selection routes require written justification, prior review where applicable, and timely disclosure of reasons. Evaluation is documented against pre-published criteria; conflicts of interest are declared and recorded; beneficial ownership is disclosed at bid and prior to signature; sanctions and cross-debarment screening is performed before award. These practices derive from the AfDB policy framework and are embedded as non-bypassable Flowhub checks. [\[AfCFTA – T...ompetition\]](#), [\[PPP Refere...artnership\]](#)

OCDS publication regime. The programme treats OCDS publication as a condition of participation. Releases must be issued, at minimum, for: (i) **planning** (including procurement plan and revisions), (ii) **tender** (including addenda), (iii) **intended award** with a standstill period for complaints and debriefing, (iv) **contract/signature** (including securities, KPIs, payment schedules, and ESMP obligations), and (v) **implementation** (milestones, variations, invoices, and payments) on a quarterly cadence. Flowhub's publication engine compiles the structured JSON in compliance with the latest OCDS schema and exposes a public portal for portfolio-level analytics and red-flagging. [\[Programme...AUDA-NEPAD\]](#), [\[PPP Refere...artnership\]](#)

Control gates enforced by Flowhub. Four non-bypassable gates govern each process: the **market-integrity gate (pre-award)** performs sanctions screening and beneficial-ownership checks and locks evaluation minutes; the **contracting gate (award/signature)** seeds the contract record and triggers the OCDS award/contract releases; the **delivery gate (acceptance)** three-way matches PO/GRN/Invoice and verifies safeguards compliance; and the **payment gate (disbursement)** validates banking details, applies dual approvals, posts to ledgers, and publishes implementation updates. No payment is released unless each antecedent gate is satisfied and evidence is filed. [\[PPP Refere...artnership\]](#)

Complaints, standstill, and debriefing. All competitive procedures include a standstill period between notice of intended award and signature. Complaints are logged and triaged in Flowhub; debriefings are recorded; and, where the AfDB prior-review regime applies, the Bank's no-objection is documented before signature. OCDS releases reflect complaint status and outcomes to preserve a public record consistent with best practice. [\[AfCFTA – T...ompetition\]](#), [\[Programme...AUDA-NEPAD\]](#)



Variation control and contract management. Variations must respect the governing procurement framework and be justified, priced, authorised, and **published**. Flowhub maintains a contract-management register that links amendments to their initiating events, updates forecast out-turn costs, and enforces that ESMP-related obligations remain payment pre-conditions. All implementation releases update the OCDS record to enable lifecycle analytics and market scrutiny. [\[AfCFTA – T...ompetition\]](#), [\[Programme...AUDA-NEPAD\]](#)

Exceptions and redactions. Exceptions to publication are narrowly circumscribed. Where confidentiality is lawfully invoked, grounds and duration are recorded; a redacted release is still issued to preserve the contracting timeline and identifiers, consistent with OCDS guidance on partial disclosure. Flowhub blocks disbursement if required releases are missing or unjustifiably delayed. [\[Programme...AUDA-NEPAD\]](#)

Data quality and portfolio analytics. The Academy of red-flags rests on data quality. Flowhub performs automated conformance checks against the OCDS schema; data stewards correct structural or semantic errors; and programme dashboards show on-time publication rates, completeness, and supplier-market concentration to support value-for-money supervision. The World Bank/OCP guidance on OCDS provides the canonical specification for these checks. [\[The Africa...Trade Area\]](#), [\[Programme...AUDA-NEPAD\]](#)

Interoperability with AfDB supervision. Prior/post-review packages are compiled as audit-ready evidence packs in Microsoft Purview, ensuring that supervision teams can retrieve the signed evaluation reports, sanction screens, beneficial-ownership attestations, complaint logs, and OCDS snapshots from a single source of truth. [\[COMESA fin...- ZBC NEWS\]](#)

Remedies and public accountability. Proven misconduct or material breaches trigger suspension, termination, recovery, and sanctions referrals; non-confidential outcomes are summarised on the Flowhub portal to reinforce market integrity. These consequences are aligned to AfDB's integrity framework and the GSIA enforcement remit. [\[AfCFTA – T...ompetition\]](#), [\[PPP Refere...artnership\]](#)

6. Fiduciary Management, IPSAS/ISA, and Internal Control

Purpose and scope. This chapter establishes a uniform fiduciary regime—accounting, internal control, internal and external audit, cash management, disbursement, and public financial disclosure—that is compatible with sovereign systems yet **standardised** programme-wide. It is anchored in **IPSAS** for financial reporting, **ISA** for external audit, and the **COSO Internal Control—Integrated Framework** for internal-control design and evaluation. Flowhub instruments these requirements so that financial flows, approvals, reconciliations, and audit trails are **evidence-ready** at all times. [\[Handling o... - COMESA\]](#), [\[2023-2024...diting ...\]](#), [\[Internal C...ork - CORE\]](#)

Accounting and reporting framework. Implementing entities prepare quarterly interim financial reports and annual project financial statements in accordance with **IPSAS** (accrual, or modified cash with a documented transition plan where approved). Statements include designated-account reconciliations, notes on contingent liabilities arising from PPPs, and a reconciliation of OCDS-reported payments to ledger postings. Flowhub ensures that bank-book and sub-ledger movements are traced to contract records and that **public extracts** are disclosed per the programme's disclosure schedule. [\[Handling o... - COMESA\]](#), [\[Programme...AUDA-NEPAD\]](#)

Disbursement and cash management. Disbursements follow Bank-approved modalities with a **direct-payment default** to suppliers/contractors against verified milestones, reducing idle balances and

leakage. Designated Accounts, where used, are ring-fenced and dual-authorised; reconciliations are monthly; and advance use is capacity-tested and time-bound. Flowhub blocks payment unless three-way match and safeguard checks are satisfied, and posts the corresponding OCDS implementation update. [\[PPP Refere...artnership\]](#)

Internal control architecture. Implementing entities maintain an internal-control system consistent with **COSO**—control environment, risk assessment, control activities, information and communication, and monitoring—supported by the seventeen principles. Flowhub operationalises segregation of duties, maker–checker approval chains, threshold-based additional reviews, device-compliance checks, and automated reconciliations; management attests annually to control effectiveness, with deficiencies tracked to remediation. [\[Internal C...ork - CORE\]](#)

Internal audit function. A professionally independent internal audit function operates under the **Institute of Internal Auditors’ Standards**, reporting to an Audit & Risk Sub-Committee. Its risk-based plan covers procurement cycles, cash management, payroll where relevant, IT general controls (identity, device, and data), and safeguards-incident handling. Reports and management action plans are filed in Flowhub; follow-up is monitored to closure. The transition to the **Global Internal Audit Standards (effective January 2025)** is managed through an adoption note and gap analysis. [\[Internatio...l Auditing\]](#), [\[Introduc...ards - PKF\]](#)

External audit under ISA. Annual project financial statements are audited in accordance with the **IAASB’s International Standards on Auditing**, with full and unrestricted access to records (including Flowhub evidence packs and OCDS data). Audit opinions and management letters are published in non-confidential form on the programme portal; group-audit considerations (e.g., multiple implementing entities) are addressed per **ISA 600 (Revised)**. [\[2023-2024...diting ...\]](#)

Cyber-financial controls and evidentiary integrity. The financial-control layer is coupled with a **Zero Trust** security posture and mapped to **NIST SP 800-53 Rev. 5** families for identification and authentication, access control, audit and accountability, configuration management, and incident response. Purview maintains the obligations register, assigns responsible officials, records tests of operating effectiveness, and computes a risk-based compliance score to support both management oversight and auditor procedures. [\[PUBLICATIO.... - COMESA\]](#), [\[COMESA fin...- ZBC NEWS\]](#)

Fraud risk management and whistleblowing. Fraud risk assessments are performed annually. Whistleblowing channels are confidential and accessible; cases are logged, preserved under legal hold within Flowhub, triaged within 48 hours, and escalated to the integrity function and, where relevant, to AfDB. Outcomes are reflected in contract-management actions and, in non-confidential summary, on the public portal. [\[PPP Refere...artnership\]](#)

Assurance map and escalation. First-line controls are operated by PMUs; the GSIA compliance team constitutes the second line, configuring controls and monitoring conformance; internal audit and the supreme audit institution/external auditor form the third line. Material qualifications, significant control deficiencies, or publication failures are escalated to the GSIA Steering structures with defined remedies, including suspension of disbursements and corrective action plans time-bound to the next gate review. [\[PPP Refere...artnership\]](#)

Public financial disclosure. In addition to OCDS implementation data, the programme publishes: (i) annual audited financial statements; (ii) quarterly financial summaries; and (iii) variance analyses against plan. Redactions are narrowly tailored and justified in writing; the publication cadence is part



of the Disclosure Schedule and is enforced through Flowhub. [\[Programme...AUDA-NEPAD\]](#), [\[PPP Refere...artnership\]](#)

Continuity and exit. Upon closure or transfer, the complete evidentiary chain—ledgers, bank reconciliations, trial balances, audit logs, and OCDS archives—is handed over to the receiving authority. Flowhub’s sovereign instances, based on open and widely adopted components, facilitate orderly transition without prejudice to data sovereignty and retention rules. [\[PPP Refere...artnership\]](#)

7. Environmental and Social Safeguards (ISS 2024)

The environmental and social safeguard framework for CODESA is anchored in the African Development Bank’s Integrated Safeguards System (ISS), effective 31 May 2024, which constitutes the minimum compliance threshold for all programme activities. This includes, but is not limited to, public-private partnerships (PPPs), regional corridor infrastructure, digital public infrastructure (DPI) deployments, and agrifood value-chain interventions. The ISS introduces enhanced provisions on community health and safety, prevention and response to sexual exploitation and abuse/sexual harassment (SEA/SH), stakeholder engagement, and climate resilience, ensuring that all interventions are socially inclusive and environmentally sustainable.

Operationalisation through Flowhub

The Flowhub platform serves as the compliance backbone for safeguards implementation, embedding the following mechanisms:

- **Registers and Templates:** Environmental and Social Impact Assessments (ESIA), Environmental and Social Management Plans (ESMP), Labour Management Procedures (LMP), Stakeholder Engagement Plans (SEP), and Resettlement Action Plans (RAP) are digitised and integrated into Flowhub. Completion and approval of these instruments constitute a pre-condition for procurement initiation.
- **Incident Management:** All SEA/SH and Environmental, Health, and Safety (EHS) incidents must be reported within 48 hours through Flowhub. Survivor-centred protocols are mandatory, with escalation pathways to GSIA and AfDB supervisory bodies.
- **Payment Gating:** Disbursement of milestone payments is contingent upon verified ESMP compliance, recorded and validated within Flowhub.
- **Disclosure and Transparency:** Non-confidential summaries of safeguard instruments and compliance reports are published quarterly on the Open Contracting Data Standard (OCDS) portal to ensure public accountability.
- **Independent Review:** Activities classified as high-risk under ISS trigger mandatory third-party review prior to financial close and at any major contractual variation.

This structure guarantees that environmental and social safeguards are not treated as procedural formalities but as enforceable conditions embedded in the programme’s fiduciary and operational architecture.

8. Stakeholder Engagement, Grievance and Accountability

Stakeholder engagement under CODESA adheres to the principles articulated in AfDB ISS and World Bank Environmental and Social Standard 10 (ESS10), ensuring that engagement is early, inclusive,

proportionate, and continuous. The objective is to institutionalise meaningful consultation and establish robust grievance redress mechanisms that reinforce accountability and trust.

Core Requirements and Flowhub Integration

- **Stakeholder Engagement Plan (SEP):** Each project must maintain a SEP, uploaded and version-controlled in Flowhub, with mandatory updates at key milestones.
- **Grievance Redress Mechanism (GRM):** Accessible, confidential, and non-retaliatory grievance channels are established for communities, workers, and programme beneficiaries. Complaints are logged digitally, assigned unique identifiers, and resolved within time-bound parameters.
- **Public Record and Transparency:** Flowhub publishes anonymised grievance statistics and resolution summaries on a quarterly basis, reinforcing transparency and institutional credibility.
- **Integration with Monitoring, Evaluation, and Learning (MEL):** Engagement performance indicators—such as consultation coverage, grievance closure rates, and stakeholder satisfaction—are systematically captured and integrated into quarterly performance reports and gate reviews.

This approach ensures that stakeholder engagement is not a one-off exercise but a continuous governance function embedded in programme delivery.

9. Data Protection, Cybersecurity and Digital Rights

CODESA's digital governance framework is grounded in the COMESA Data Privacy Policy and benchmarked against General Data Protection Regulation (GDPR) principles, ensuring lawful, fair, and transparent processing of personal data. Flowhub enforces a Zero Trust security posture, mapping its controls to NIST SP 800-53 Rev. 5 families for identity management, access control, auditing, and incident response.

Technical and Organisational Controls

- **Identity and Access Management:** Multi-factor authentication (MFA), conditional access policies, and least-privilege role-based access control (RBAC) are mandatory.
- **Data Protection:** All data is encrypted at rest and in transit, with immutable audit logs and WORM-like retention for evidentiary artefacts.
- **Hosting and Resilience:** A federated architecture is adopted, leveraging sovereign Nextcloud storage with GDPR-style **3-2-1 backup** protocols to ensure resilience and data sovereignty.
- **Compliance Evidence:** Microsoft Purview is deployed to maintain obligations registers, assign control ownership, and store audit-ready evidence packs for supervisory review.

Digital Rights and Transparency

Data-subject rights—including access, rectification, and erasure—are operationalised through Flowhub workflows. Privacy notices, consent records, and data processing disclosures are published on the programme portal, ensuring compliance with both legal and ethical standards.

This framework positions CODESA as a model for responsible digitalisation, balancing innovation with rights-based governance and cybersecurity resilience.

10. Risk and Incident Management

Purpose and scope.

This pillar establishes a uniform, auditable system for identifying, assessing, and mitigating risks across fiduciary, procurement, environmental and social (E&S), cyber/data, and operational domains. It also codifies incident-response protocols for integrity breaches, SEA/SH allegations, EHS events, and cybersecurity incidents. The framework aligns with AfDB's fiduciary and safeguards risk appetite and is enforced through Flowhub's digital workflows.

Risk taxonomy and ownership.

Risks are categorised as:

- **Fiduciary:** misuse of funds, fraud, weak internal controls.
- **Procurement:** collusion, bid rigging, non-compliance with AfDB rules.
- **Safeguards:** ISS non-compliance, SEA/SH, stakeholder engagement failures.
- **Cyber/data:** breaches, ransomware, GDPR non-compliance.
- **Political/governance:** interference in procurement, resistance to disclosure.
- **Operational:** connectivity gaps, skills churn, platform downtime.

Each risk is assigned an owner (PMU, GSIA compliance team, or provider) and tracked in Flowhub's risk register with inherent/residual ratings, mitigation plans, and escalation thresholds.

Incident workflows.

Flowhub provides structured forms for fiduciary, procurement, SEA/SH, EHS, and cyber incidents. Key features:

- **Logging and triage:** All incidents logged within 24–48 hours; severity classification triggers escalation.
- **Escalation:** High-risk cases escalate to GSIA and AfDB supervision; SEA/SH cases follow survivor-centred protocols.
- **Evidence preservation:** Immutable logs and WORM-like retention ensure evidentiary integrity.
- **Remedies:** Suspension of disbursements, contract termination, recovery, sanctions referral.
- **Public accountability:** Non-confidential summaries published quarterly on the Flowhub portal.

Continuous improvement.

Risk registers and incident analytics feed into quarterly reviews and gate decisions; lessons learned inform updates to control frameworks and training modules.

11. Ethical Posture and “No War” Principle

Concept and operationalisation.

The “No War” principle is the programme's shorthand for a broader conflict-sensitivity and do-no-harm ethic. It commits all actors to avoid financing, enabling, or legitimising activities that perpetuate violence, conflict, or systemic human-rights abuses. This principle is not aspirational; it is embedded in enforceable controls.

Implementation mechanisms:

- **Exclusion lists:** Flowhub integrates sanctions and cross-debarment lists and applies conflict-sensitivity screening to suppliers and partners.
- **Beneficial ownership transparency:** Mandatory disclosure at bid and pre-signature stages; refusal or misrepresentation is grounds for exclusion.
- **Human-rights due diligence:** PPP and procurement packages include conflict-risk assessments; high-risk contexts require independent review.
- **Ethics declarations:** Officials and bidders sign integrity and non-collusion pacts; conflicts of interest are declared and logged.
- **Incident escalation:** Allegations of intimidation, violence, or SEA/SH trigger immediate suspension and investigation under documented protocols.

Alignment with global norms:

The principle draws on OECD Guidelines for Multinational Enterprises, AfDB integrity rules, and UNCITRAL PPP guidance on responsible contracting. It is reinforced by Flowhub's transparency posture—OCDS publication and public dashboards deter opaque dealings and enable civil-society oversight.

12. Communications and Proactive Disclosure

Strategic posture.

Communications are treated as a compliance function, not an afterthought. The COMESA Communication Strategy (2022–2025) provides the baseline for audience segmentation, message discipline, and channel governance. The Minor Pillars elevate disclosure to a legal obligation, operationalised through Flowhub's OCDS engine and public dashboards.

Mandatory disclosures:

- **Procurement:** OCDS releases at planning, tender, award, contract, and implementation stages.
- **Financial:** Annual IPSAS-based statements and quarterly summaries.
- **Safeguards:** Non-confidential ESMP/SEP summaries and incident statistics.
- **MEL:** Gate-review findings, mid-term and final evaluation reports.

Engagement and grievance transparency:

Stakeholder Engagement Plans and grievance mechanisms are publicised in accessible formats and languages; Flowhub publishes anonymised grievance data and resolution rates.

Crisis communication:

Pre-cleared protocols govern incident notification, spokesperson designation, and corrective-action disclosure for fiduciary breaches, SEA/SH cases, and cyber events. Timely, accurate communication is mandatory to preserve trust and mitigate reputational risk.

Advocacy and continental alignment:

External messaging positions the programme as a compliance-by-design model aligned with AfDB's ISS (2024), procurement policy, and the AU Digital Transformation Strategy. Advocacy materials emphasise open contracting, fiduciary integrity, and social safeguards as competitive advantages for co-financiers and private partners.

13. Implementation Roadmap and Gate Reviews

Purpose and structure.

The roadmap sequences legal enablement, platform configuration, and operational roll-out to ensure that **first disbursement** and **PPP execution** occur only after the Minor Pillars' control environment is fully operational. Gate reviews provide structured decision points for tranche releases, continuation, and corrective actions.

Phase A — Legal Enablement (Weeks 0–6)

- **Outputs:** GSIA Charter and Membership Agreement executed; Country Fiduciary Compacts signed; PPP Annex and Disclosure Schedule adopted; Flowhub configuration protocols approved.
- **Dependencies:** AfDB no-objection to governance instruments; alignment with national PPP statutes.
- **Gate 0:** Legal effectiveness confirmed; membership obligations enforceable.

Phase B — Platform Configuration and Control Baseline (Weeks 4–12)

- **Outputs:** Flowhub hub and first sovereign instance live; Zero Trust identity/device/data controls enforced; Purview assessments mapped to AfDB procurement and ISS control sets; Nextcloud sovereign storage operational; OCDS publication engine tested.
- **Acceptance criteria:** RBAC workflows active; control matrix validated; public portal online with sample OCDS feed.

Phase C — Pilot PPP and Procurement Launch (Weeks 10–22)

- **Outputs:** Procurement plan approved with prior/post review thresholds; first PPP or major works tender launched; ES instruments uploaded; SEP and grievance channels active; OCDS planning and tender releases published.
- **Gate 1:** AfDB no-objection recorded; Flowhub evidence pack complete; risk register initialised.

Phase D — First Award and Disbursement (Weeks 18–30)

- **Outputs:** Standstill observed; contract record instantiated with KPIs, ESMP obligations, and payment schedule; OCDS award and contract releases published; milestone acceptance verified; direct-payment modality triggered.
- **Gate 2:** Compliance statement issued by GSIA; IPSAS-based IFR submitted; Purview compliance score $\geq$ agreed threshold.

Phase E — Scale-Up and Mid-Term Review (Months 6–18)

- **Outputs:** Additional RMCs onboarded; Flowhub instances federated; PPP portfolio under risk-based prior review; MEL dashboards operational; OCDS completeness $\geq$ 95%.
- **Gate 3 (Mid-Term, Year 3):** Independent evaluation using OECD-DAC criteria; fiduciary and safeguards conformance verified; corrective actions implemented.

Phase F — Consolidation and Continuation (Years 4–10)

- **Outputs:** Steady-state operations; cross-REC comparability achieved; Continuation Dossier prepared for next decennial compact.



- **Gate 4 (End-Term, Year 10):** Renewal decision based on outcome bands (procurement integrity, safeguards compliance, PPP performance, MEL indicators) and IPSAS/OCDS audit record.

Gate Review Logic and Evidence Requirements

Each gate is contingent on:

- **Fiduciary:** IPSAS-compliant IFRs; ISA audit opinions; COSO-aligned internal control attestations.
- **Procurement:** OCDS publication at all stages; sanctions/beneficial-ownership checks; Flowhub evidence packs.
- **Safeguards:** ISS-aligned ES instruments; incident logs; SEA/SH protocols operational.
- **Data governance:** Zero Trust posture; Purview compliance score; privacy incident register.
- **MEL:** Indicator baselines, disaggregation, and adoption metrics verified.

Remedies for non-compliance: Suspension of disbursements, corrective-action plans, or membership sanctions; persistent failure escalates to AfDB and triggers public disclosure of non-confidential findings.

Integration with AfDB supervision and Flowhub analytics

Gate reviews are synchronised with AfDB supervision missions. Flowhub dashboards provide real-time compliance scoring, OCDS completeness metrics, and red-flag analytics for procurement and safeguards. Evidence packs are exportable for ISA audits and AfDB prior/post review, reducing transaction costs and accelerating readiness for subsequent tranches.