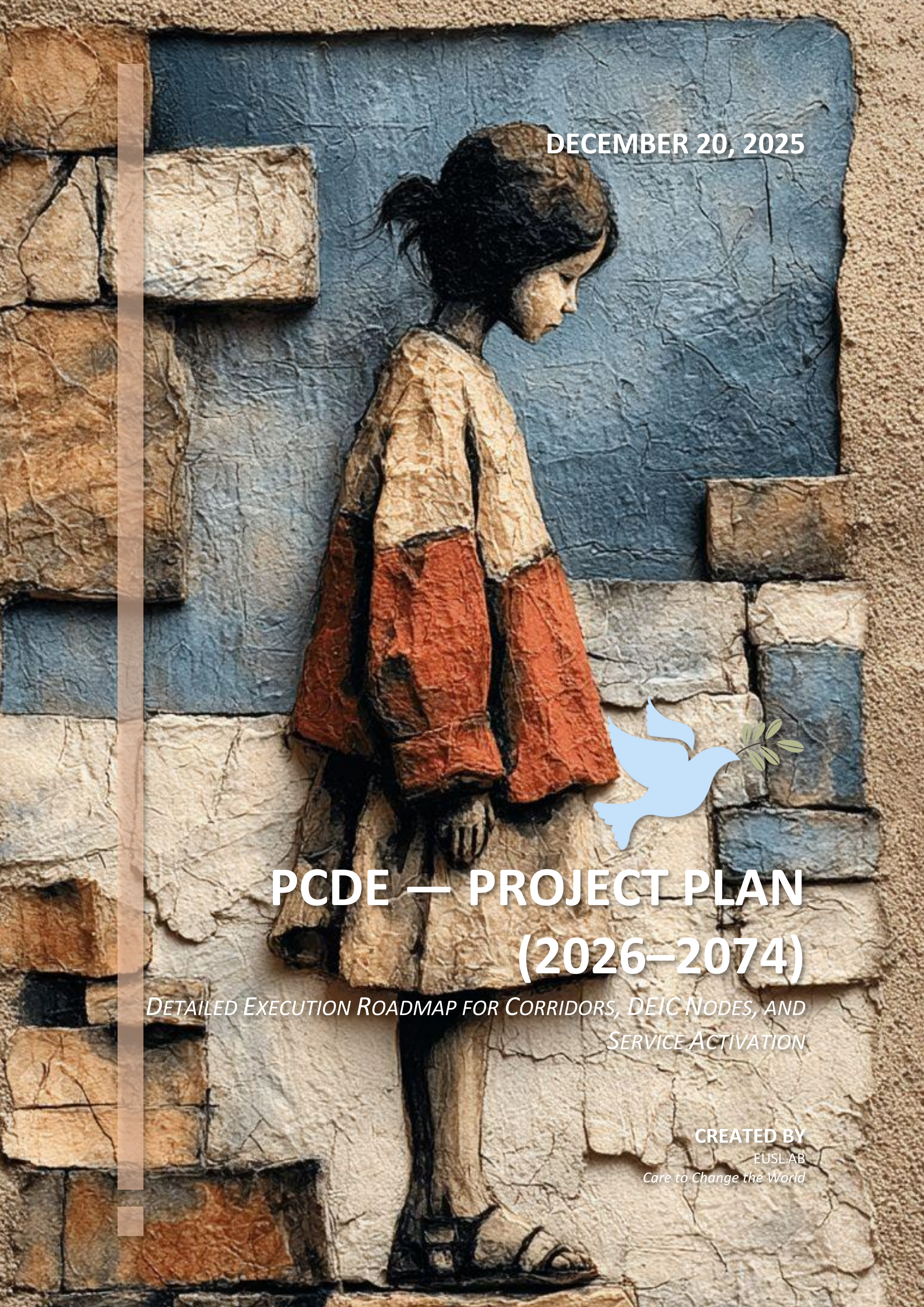

DECEMBER 20, 2025

PCDE — PROJECT PLAN (2026–2074)

Detailed Execution Roadmap for Corridors, DEIC Nodes, and Service Activation

CREATED BY

EUSL AB

Care to Change the World

Table of Contents

PCDE Project Plan 2026-2074

Introduction

This Project Plan translates the Business Plan’s strategic intent into a sequenced, standards-anchored execution blueprint across Africa (mirroring the REC architecture—COMESA, SADC, EAC), the Americas (Pan-Americas), and Asia (pan-regional), with Europe excluded from scope at this stage. It interlocks with ongoing regional programmes and policy frameworks—COMESA’s Inclusive Digitalisation of Eastern & Southern Africa (IDEA), SADC’s Digital Transformation Strategy, EAC’s regional ICT and digital-integration tracks, and analogous payment and digital-market initiatives in the Americas and Asia—while enforcing the safeguards, transparency, and cybersecurity canon (AfDB ISS; World Bank ESF; OCDS; IATI; ISO/IEC 27001; NIST SP 800-207; ISO/IEC 27701).

Chapter One — Purpose, Scope, Outcomes

Purpose

The Project Plan defines how PCDE will be implemented—what assets will be built, which services will be activated, and how compliance and disclosures will be maintained—across priority regions. In Africa, phasing mirrors the three principal Regional Economic Communities (RECs): COMESA, SADC, and EAC, aligning corridor selection, node deployment, and trust-service activation with IDEA’s harmonisation platform, SADC-DTS interventions, and EAC’s digital-integration initiatives.

In the Americas, execution exploits the Inter-American Development Bank’s platforms that enable MSME market entry and payment interoperability—ConnectAmericas for trade connectivity and procurement signalling, and the newly launched IDB Pay initiative for fast, interoperable retail payment systems—together with public-private dialogues under PAGA on digital payments.

In Asia, delivery leverages ASEAN’s regional payment-connectivity momentum and policy guidance toward interoperable, local-currency cross-border payments, de-fragmentation, and secure data flows—framed by ASEAN Leaders’ declarations and technical workstreams documented by ERIA, AMRO, and regional fora.

Scope

The Plan covers:
(i) corridor-grade fiber and neutral IXPs; (ii) DEIC nodes and workforce localisation; (iii) applied AI service onboarding for public and market use cases; (iv) trust-service rails (digital identity, signatures/seals, secure payments, compliance dashboards); (v) safeguards instruments and stakeholder engagement; (vi) quality assurance and acceptance; (vii) MEL integration and open data disclosures (OCDS/IATI); and (viii) close-out and handover. All activities are governed by AfDB’s updated Integrated Safeguards System (effective 31 May 2024) and, where co-financed or relevant, the World Bank ESF (effective for IPF projects since 1 Oct 2018).

Outcomes

Outcomes are framed in three families—access/adoption, governance/integrity, and market activation—reported through machine-readable datasets:

- Access and adoption: corridor latency and uptime improvements; IXPs traffic offload; DEIC throughput; MSME onboarding to payments and marketplaces (IDEA, SDBA/DRPP/REPSS interlocks).

- Governance and integrity: IPSAS-aligned accrual reporting (finance), OCDS publication end-to-end for contracting, IATI activity/results files for development-finance disclosures.
- Market activation: interoperable payments (IDB Pay in LAC; ASEAN RPC in Asia; SDBA pilots in COMESA), inclusive e-commerce enablement, and cross-border transaction-friction reduction.

Operational resilience and lawful data processing are ensured under an ISO/IEC 27001 ISMS, Zero-Trust enforcement per NIST SP 800-207, and privacy management under ISO/IEC 27701 where personal data are processed.

Chapter Two — Work Breakdown Structure (WBS) and Deliverables

WBS Overview

The WBS organises execution across four levels—Programme → Region → Country → Workstream—so that build, activation, safeguards, and disclosures proceed coherently with REC or regional-platform schedules.

Level 1 — Programme (Pan-Regional Portfolio)

- **P-1 Governance & Compliance Backbone.** Maintain standards canon (ISS/ESF; OCDS/IATI; ISMS/ZTA/PIMS) and a central registry for policies, models, contract templates, and disclosure identifiers.
- **P-2 MEL & Public Dashboards.** Publish portfolio-wide access/adoption/activation indicators (IATI results codelists; OCDS implementation releases) and quarterly compliance notes.

Level 2 — Region (REC/Regional Platform Alignment)

- **R-COMESA (IDEA/SDBA Interlock).** Regional planning, least-cost corridor modelling, capacity building; e-payment/e-commerce harmonisation pilots under SDBA and DRPP/REPSS references. Deliverables: regional planning dossiers; standards-alignment statements; pilot corridor/payment interoperability reports.
- **R-SADC (SADC-DTS).** Conform corridor and digital-skills work to SADC-DTS goals and 2030 targets; produce legal/regulatory harmonisation briefs and observatory inputs. Deliverables: DTS alignment matrix; regional skills and regulatory memoranda; observatory data packs.
- **R-EAC (ICT/EARDIP).** Coordinate with EAC ICT and EA-RDIP tracks, including ONA, e-commerce strategy and CERT roadmap; align cross-border fibre routes and digital-market facilitation. Deliverables: EAC integration note; corridor–policy concordance; CERT/data-protection harmonisation outline.
- **R-Pan-Americas (IDB Ecosystem).** Interface to ConnectAmericas for MSME sourcing/trade and to IDB Pay/PAGA for payment interoperability. Deliverables: Americas market-entry packets; MSME onboarding cohorts; FRPS interoperability assessments.
- **R-Asia (ASEAN RPC/Policy).** Align trust-service rails and payment activation with ASEAN RPC initiatives and ERIA guidance; produce local-currency transaction roadmaps. Deliverables: ASEAN RPC alignment dossier; QR standards conformance; cross-border payment case studies.

Level 3 — Country (SPVs/CDUs)

- **C-1 Corridor & IXP Delivery.** Feasibility, permitting/ROW, EPC awards, build and light-up; acceptance tests with latency, uptime, packet-loss thresholds; OCDS releases at planning, tender, award, contract, and implementation stages. Deliverables: feasibility & safeguards screening; ROW/permit package; tender & award dossiers; acceptance test reports; OCDS datasets.

- **C-2 DEIC Node Operations.** Site selection, fit-out, cohort scheduling, curricula (fiber/Cyber/AI/Trust); local-content and gender/youth participation targets; stakeholder engagement plans and grievance mechanisms (ISS/ESF). Deliverables: DEIC fit-out acceptance; cohort rosters; SEPs and grievance logs; IATI activity & results files.

- **C-3 Trust-Service Activation.** eID, e-signature/seal, timestamping, certificate lifecycle; secure payments integration (regional platform interlocks). Deliverables: policy packs; PKI/identity operations manual; payment interoperability test reports; privacy DPIAs (ISO/IEC 27701).

- **C-4 Applied AI Service Onboarding.** Health triage, education/TVET adaptive learning, trade inspection risk scoring, multilingual assistance; model cards and evaluation summaries; ZTA enforcement evidence. Deliverables: model cards/evaluation; service SLAs; ZTA artefacts; incident-response playbooks.

- **C-5 Safeguards & Stakeholder Engagement.** ESIA/ESMP/RAP/SEP drafting and disclosure; community health and safety, labour protections; portfolio-level ISS/ESF compliance reports. Deliverables: ES instruments; disclosure registry entries; verification mission notes.

- **C-6 Quality Assurance & Acceptance.** Corridor acceptance (network telemetry, SLA conformance); DEIC facility acceptance; trust-service compliance and audit trails; AI service acceptance run-books. Deliverables: acceptance certificates; QA audit trails; corrective-action logs.

- **C-7 MEL & Public Dashboards.** Publish financials (IPSAS accruals), contracting (OCDS), activity/results (IATI); quarterly public summaries. Deliverables: IPSAS statements; OCDS & IATI updates; dashboard releases.

Level 4 — Workstreams (Cross-cutting)

Workstream	**Primary Deliverables**	**Standards & Platforms**
Corridors/IXPs	Feasibility & route studies; permits & ROW; EPC award; build; acceptance tests	OCDS releases; ISS/ESF instruments; regional planning notes (IDEA/SADC/EAC)
DEIC & Workforce	Fit-out acceptance; cohort schedules; curricula packs; SEPs & grievance	ISS/ESF; regional skills frameworks; IATI activity/results
Trust Services	PKI & eID policy; certificate ops; payment interoperability tests	ISO/IEC 27701; regional payment initiatives (SDBA/DRPP; IDB Pay; ASEAN RPC)

Workstream	Primary Deliverables	Standards & Platforms
Applied AI	Model cards & evaluation; ZTA artefacts; service SLAs	NIST SP 800-207; ISMS controls (ISO/IEC 27001)
Safeguards	ESIA/ESMP/RAP/SEP; verification & portfolio reports	AfDB ISS; World Bank ESF
Disclosures	OCDS end-to-end; IATI organisation/activity; IPSAS statements	OCDS; IATI; IPSAS guidance

References

- **COMESA — IDEA Programme.** Programme documents and PCU. [comesa.int]
- **World Bank — IDEA Aide-Mémoire (Apr 2025; COMESA).** Project launch & implementation support mission. [documents....ldbank.org]
- **COMESA — IDEA launch and regional targets.** News release. [comesa.int]
- **SADC — Digital Transformation Strategy (DTS) draft.** SADC-DTS (Oct 2022). [sadc.int]
- **EAC — ICT sector page and EA-RDIP.** ICT sector; EA-RDIP. [eac.int], [eac.int]
- **EAC — Model ICT Policy (EACO, 2017).** Policy framework. [eaco.int]
- **IDB — ConnectAmericas.** About; Launch note. [connectamericas.com], [iadb.org]
- **IDB — IDB Pay (2025).** Press release. [iadb.org]
- **IDB Lab & WEF — PAGA.** Accelerating digital payments in LAC (2022). [publicatio...s.iadb.org]
- **ASEAN/ERIA/AMRO — Regional Payment Connectivity.** ERIA policy brief (Jan 2025); AMRO blog (Apr 2025); East Asia Forum op-ed (Mar 2025). [eria.org], [amro-asia.org], [eastasiaforum.org]
- **AfDB — Updated ISS effective 31 May 2024.** Press release. [afdb.org]
- **World Bank — ESF overview.** ESF portal. [worldbank.org]
- **Open Data Standards.** OCDS documentation; IATI Standard portal; IATI Reference (2.03). [standard.o...acting.org], [iatistandard.org], [reference....oriati.org]
- **Cybersecurity & Privacy Baselines.** NIST SP 800-207 Zero Trust Architecture; ISO/IEC 27001:2022; ISO/IEC 27701:2025. [nvlpubs.nist.gov], [iso.org], [aftld.org]

Chapter Three — Corridor and Node Selection Methodology

Purpose and Alignment

This methodology establishes how PCDE selects cross-border fiber corridors, neutral Internet Exchange Points (IXPs), and DEIC node locations across Africa, the Pan-Americas, and Asia. Selection is anchored to regional policy platforms and REC/state initiatives to ensure harmonisation, reduce fragmentation, and maximise co-financing readiness. In Africa, corridor and node choices are explicitly aligned with

COMESA's Inclusive Digitalisation of Eastern & Southern Africa (IDEA) programme and its regional harmonisation and planning platform, SADC's Digital Transformation Strategy (DTS) goals to 2030, and EAC's ICT and regional digital integration workstreams (including EA-RDIP). In the Americas, site selection leverages ConnectAmericas for market signalling and MSME participation and the IDB Pay/PAGA agenda for interoperable fast retail payments. In Asia, corridor and trust-service choices reflect ASEAN Regional Payment Connectivity (RPC) and associated guidance from ERIA and AMRO on interoperability, local-currency transactions, and QR standardisation.

Selection Principles

PCDE applies six normative principles to corridor and node selection:

1. **Regional Policy Concordance.** Corridors must intersect geographies prioritised by REC/regional platforms to exploit least-cost modelling, regulatory harmonisation, and capacity-building. For COMESA, corridor selection references IDEA's regional platform and work plan; for SADC, selections support DTS targets (universal affordable access, harmonised legal frameworks, digital skills); for EAC, routes that complement EA-RDIP and One Network Area reforms.
2. **Demand Density and Latency Impact.** Preferred corridors reduce round-trip latency and introduce route diversity between population and industrial centres, including cross-border metropolitan clusters where IXPs can achieve significant traffic offload. This is consistent with REC targets to close the **coverage–usage gap** documented in IDEA launch notes.
3. **Interoperable Payments and Digital Market Readiness.** Node locations are prioritised where e-payments/e-commerce interoperability is being harmonised: COMESA's SDBA/DRPP pilots, IDB Pay in LAC, and ASEAN's RPC efforts, because transaction frictions materially affect adoption of digital services.
4. **Safeguards Feasibility and Community Licence.** Site choices must pass pre-screening under AfDB's updated **Integrated Safeguards System (ISS)** (effective 31 May 2024) and, where co-financed, the World Bank **ESF** (effective 1 Oct 2018), to ensure manageable E&S risks, viable land/ROW arrangements, stakeholder engagement, and grievance mechanisms.
5. **Last-Mile Economics and DEIC Throughput.** Nodes are preferred when local last-mile economics (municipal permits, power availability, shared civil works) and DEIC intake capacity (gender/youth ratios, TVET partners) yield faster adoption and workforce localisation consistent with REC skills objectives.
6. **Disclosure Readiness and Co-financier Compatibility.** Selections must be documentable end-to-end in **OCDS** for procurement and **IATI** for activities/results to maintain transparency, comparability, and MDB-grade assurance.

Methodological Steps (per corridor / node)

1. **Regional Screening and Concordance Check.**
   The Secretariat issues a screening memo benchmarking candidate routes/nodes against REC or regional platform priorities (IDEA, SADC-DTS, EAC EA-RDIP; IDB Pay/PAGA; ASEAN RPC). The memo identifies expected policy continuity, legal/regulatory feasibility, and payment/e-commerce interlocks.

2. **Technical and Economic Feasibility (TEF).**
   TEF studies model traffic forecasts, latency reductions, capex/opex, route diversity, IXP placement potential, and DEIC demand absorption. For COMESA and EAC, TEF consults regional least-cost modelling and planning guidance.

3. **Safeguards Pre-Screening.**
   Apply ISS/ESF risk classification; pre-scope ESIA/ESMP/RAP/SEP requirements; verify community health and safety, labour protections, and climate-risk screening obligations.

4. **Payments/Trust-Rails Readiness Assessment.**
   Confirm presence or timeline of interoperable retail payments/e-commerce pilots or frameworks (SDBA in COMESA; IDB Pay/PAGA in LAC; ASEAN RPC/QR standardisation in Asia). Map trust-service rails (eID/e-signature/seal) to payment corridors.

5. **Stakeholder and MSME Market Signalling.**
   Issue market signals through appropriate platforms (e.g., **ConnectAmericas** for LAC) to gauge MSME interest, supplier capacity, and local partnership options for DEIC operations and service onboarding.

6. **Decision Dossier and Disclosure Plan.**
   Compile TEF, safeguards pre-screen, payments readiness, and stakeholder inputs into a decision dossier; record planned OCDS releases

Regional Application Examples (illustrative)

- **COMESA:** A corridor linking Lusaka–Lilongwe with neutral IXP upgrades and SDBA/DRPP payments pilots; decision dossier references IDEA's harmonisation platform and the 2025 launch targets (180 million access; 100 million services) to maximise adoption.

- **SADC:** A metropolitan extension prioritising DTS objectives (universal affordable access, harmonised frameworks, skills); DEIC nodes co-located with TVET partners and municipal permitting efficiencies.

- **EAC:** Cross-border fibre reinforcing EA-RDIP and ONA reforms; DEIC nodes near border trade hubs, with CERT/data-protection harmonisation in view.

- **Pan-Americas:** Southern Cone "Pampas" node cluster where ConnectAmericas sourcing pipelines and IDB Pay/PAGA case studies indicate strong MSME and payments readiness; trust-service rails mapped to FRPS design.

- **Asia (ASEAN):** Corridor tied to RPC and local-currency transaction pilots, with QR standards conformance and DEIC programmes in logistics/commerce; trust-services aligned to regional payment frameworks.

Chapter Four — Schedules and Gate Criteria

Purpose

This chapter codifies an integrated schedule model and gate criteria for corridors, IXPs, DEIC nodes, trust-service rails, and applied AI services. Gate artefacts are designed for publication under OCDS and IATI, allowing external verification and MDB life-cycle assurance. Safeguards gates reference AfDB ISS and World Bank ESF instruments; cyber/privacy gates reference ISO/IEC 27001, NIST SP 800-207, and ISO/IEC 27701.

Schedule Horizons

- **Foundation (2026–2030):** Priority cross-border corridors and capital IXPs per REC/platform; initial DEIC cohorts; baseline trust-service activation (eID/e-sign/seal) and two to three AI use-cases per sector; establish disclosure cadence (OCDS/IATI). Aligns to AU/SADC 2030 targets and IDEA first-phase workplans.
- **Expansion (2031–2040):** Corridor densification, metropolitan extensions, secondary city DEIC networks; broaden AI catalogues; scale payment interoperability (SDBA, IDB Pay, ASEAN RPC); blended financing consolidation.
- **Maturity (2041–2074):** Capacity upgrades (400G/800G), cryptographic agility for trust-rails, continuous AI model governance, route diversity, renewal checkpoints integrated with dividend logic and sustainability strategy. (Cross-references Document 3 Chapters 7–9.)

Integrated Stage-Gate Model

Gate	Timing (indicative)	Minimum Artefacts	Publication/Standards
G1 — Regional Concordance	T-12 to T-9 months	REC/platform alignment memo (IDEA/SADC-DTS/EAC EA-RDIP; LAC IDB Pay/PAGA; ASEAN RPC); initial route/node shortlist	Attach memo to OCDS planning release; register IATI activity skeleton
G2 — Feasibility & Safeguards Screening	T-9 to T-6	TEF report; ISS/ESF risk classification; pre-scope ESIA/ESMP/RAP/SEP	ESF/ISS screening notes; publish OCDS planning notice; update IATI activity
G3 — Procurement Launch & Award	T-6 to T-3	Tender docs; evaluation report; award decision; draft EPC/managed-service contracts	Full OCDS tender/award/contract releases; beneficial ownership (where lawful)
G4 — Build/Fit-out & Safeguards Instruments	T-3 to T0	EPC progress; DEIC fit-out acceptance; final ESIA/ESMP/RAP/SEP; HSE logs	ISS/ESF instruments; IATI transactions; OCDS implementation updates
G5 — Trust-Rails & AI Go-Live	T0 to T+6	eID/e-signature/seal ops manuals; payment interoperability test reports (SDBA/IDB Pay/ASEAN RPC); model cards & ZTA artefacts; DPIAs	NIST SP 800-207/ISO/IEC 27001; ISO/IEC 27701 DPIA; publish public summaries
G6 — Acceptance & MEL	T+6 onward	Corridor acceptance telemetry (latency/uptime/packet-loss); DEIC cohort outcomes; dividend logic KPIs; grievance logs	IATI results; OCDS implementation and amendments; safeguards portfolio reports

Regional Calendaring and Critical Path

- **COMESA (IDEA/SDBA):** Align corridor awards to IDEA PCU annual workplan cycles (as per 2025 Aide-Mémoire) and SDBA scoping/pilot windows; payments tests (DRPP/REPSS) scheduled pre-DEIC entrepreneurship cohorts.
- **SADC (DTS):** Anchor milestones to DTS monitoring observatory and 2030 goal checks; synchronise procurement with national regulatory updates supporting harmonised legal frameworks.
- **EAC (EA-RDIP/ICT):** Corridor permits and ONA/e-commerce strategy consistency checks done prior to award; CERT/data-protection harmonisation sessions calendared with EAC and national authorities.
- **Pan-Americas (ConnectAmericas/IDB Pay/PAGA):** Market signalling via ConnectAmericas precedes node fit-outs; FRPS interoperability testing scheduled with IDB Pay/PAGA partners; MSME onboarding waves follow payments go-live.
- **Asia (ASEAN RPC):** Payment connectivity and QR standardisation tests occur prior to trust-rails activation; DEIC logistics/commerce bootcamps align with local-currency transaction corridors.

Gate Assurance and Independence
All gates are subject to independent assurance: financial statements audited under IPSAS; procurement publication integrity under OCDS; development-finance disclosure under IATI; safeguards implementation under ISS/ESF; cyber/privacy posture under ISO/IEC 27001, NIST SP 800-207, and ISO/IEC 27701. Gate artefacts and management responses are disclosed in public summaries, except where legitimately classified.

References

- **COMESA — IDEA Programme.** Programme documents and PCU; Aide-Mémoire (Apr 2025). [au.int], [d4daccess.eu]
- **COMESA — Launch targets and harmonisation.** News release. [iso.org]
- **SADC — Digital Transformation Strategy.** SADC-DTS (Oct 2022). [ipsasb.org]
- **EAC — ICT / EA-RDIP.** ICT sector page; EA-RDIP. [iso.org], [transparency.org]
- **LAC — ConnectAmericas; IDB Pay; PAGA.** ConnectAmericas; IDB Pay; PAGA (IDB Lab/WEF).
- **ASEAN — RPC/Local-currency & interoperability.** ERIA policy brief (Jan 2025); AMRO blog (Apr 2025).
- **Safeguards frameworks.** AfDB Updated ISS (effective 31 May 2024); World Bank ESF main page. [webstore.ansi.org], [afdb.org]
- **Open-data standards.** OCDS documentation; IATI Standard portal. [unctad.org], [intosaipas.org]
- **Cybersecurity & Privacy baselines.** ISO/IEC 27001:2022; NIST SP 800-207; ISO/IEC 27701

Chapter Five — Resource Planning and Procurement Lots

Purpose and Operating Premise

This Chapter establishes the resourcing model and a lot-based procurement architecture that enables PCDE to deliver corridor-grade fiber and IXPs, DEIC nodes, trust-service rails, and applied AI services across Africa (COMESA, SADC, EAC), the Pan-Americas, and Asia. The model is designed to preserve fiduciary integrity and MDB-grade transparency—publishing contracts end-to-end under the Open Contracting Data Standard (OCDS) and financial/activity data under the International Aid Transparency Initiative (IATI)—and to remain interoperable with regional platforms (COMESA IDEA; EU–COMESA SDBA), REC strategies (SADC DTS), and digital-integration tracks (EAC EA-RDIP; ASEAN RPC; IDB ConnectAmericas and IDB Pay/PAGA).

Resourcing Structure

PCDE resources are organised at three operational layers with clear segregation of duties:

1. **Programme Centre (Secretariat).** Custodian of standards and compliance (ISS/ESF; OCDS/IATI; ISO/IEC 27001, NIST SP 800-207, ISO/IEC 27701), portfolio MEL and dashboards, central vendor prequalification, model contracts, and disclosure governance (identifiers, release schedules).

2. **Regional Operating Units (ROUs).** REC/platform alignment (e.g., COMESA–IDEA planning, SADC-DTS observatory milestones, EAC EA-RDIP and ONA), corridor and IXP coordination, DEIC siting policy, payment/e-commerce interoperability scheduling (SDBA, IDB Pay, ASEAN RPC), and regional capacity building.

3. **Country Delivery Units (CDUs)/SPVs.** Permits and rights-of-way, EPC management, DEIC fit-out, trust-service operations, AI service onboarding, stakeholder engagement and grievance mechanisms, acceptance testing, and publication of all contracting stages in OCDS together with IATI activity/results updates.

Workforce Localisation and Skills

DEIC nodes anchor workforce localisation through accredited curricula tied to build schedules. Core skills include fiber deployment and NOC operations, SOC/incident response and GRC/privacy (ISMS/PIMS), applied AI operations/model governance, PKI/identity administration and payment interoperability. Local-content and gender/youth participation targets are aligned with REC strategies and safeguards, and are monitored through IATI results fields and safeguards portfolio reports.

Procurement Strategy and Lot Architecture

Procurement is conducted through **open, competitive procedures** with end-to-end OCDS publication (planning, tender, award, contract, implementation). Lots are structured to balance competition, specialisation, and accountability, and to facilitate REC/platform interlocks:

- **Lot A — Corridor EPC & IXP Integration.** Design-and-build for cross-border fiber segments, metro extensions, ducting/civil works, and neutral IXP upgrades. Contracts include SLA-backed acceptance criteria (latency, uptime, packet-loss) and route diversity commitments; OCDS releases document planning, tender, award, and implementation telemetry.

- **Lot B — DEIC Fit-Out & Operations.** Supply, installation, and commissioning of DEIC facilities (learning labs, coworking, security/privacy sandboxes), followed by an operations service with targets for cohort throughput, placement, MSME onboarding, and inclusion (gender/youth/rural). Safeguards instruments and stakeholder plans are mandatory deliverables.

- **Lot C — Trust-Service Rails.** Establish and operate PKI/identity (eID, e-signature/seal, time-stamping), certificate lifecycle management, secure document exchange, and payment interoperability testing coordinated with regional initiatives (SDBA/DRPP; IDB Pay; ASEAN RPC). Privacy DPIAs, PIMS documentation, and cryptographic-agility plans are required.
- **Lot D — Applied AI Managed Services.** Deploy and operate sector AI use-cases (health triage, adaptive learning, risk-based inspection, multilingual assistance), with published model cards and evaluation summaries, Zero-Trust enforcement artefacts, and incident-response playbooks.
- **Lot E — Programme-Wide Assurance & MEL.** Independent audits (IPSAS financials; OCDS publication integrity; IATI completeness/timeliness), safeguards verification (ISS/ESF), cyber/privacy assessments (ISO/IEC 27001; ISO/IEC 27701; ZTA), and public dashboard curation.

Contract Forms and Award Criteria

Contract forms cover EPC, managed services, and framework agreements. Award criteria balance technical quality (route diversity, IXPs design, ISMS/ZTA/PIMS controls), value-for-money, inclusion outcomes (DEIC targets), and integrity and compliance. Beneficial-ownership disclosures for awarded suppliers and SPV shareholders are required where lawful; anti-bribery and AML/CFT controls follow **ISO 37001** practice and **FATF** Recommendations.

Publication and Disclosure

Each lot is published in OCDS from planning to implementation; amendments, payment milestones, performance telemetry, and sanctions (if any) are recorded and linked. Financial/activity/result data are published in IATI with organisation and activity identifiers to maintain comparability and external reuse.

Regional Procurement Interlocks

In COMESA, lot calendars are aligned with IDEA PCU workplans and SDBA scoping/pilot windows; in SADC, procurement synchronises with DTS legal/regulatory harmonisation; in EAC, awards consider EA-RDIP, ONA, and regional e-commerce strategy; in the Pan-Americas, market signalling uses ConnectAmericas and payments go-live sequences under IDB Pay/PAGA; in Asia, trust-service operations and payments testing are scheduled to match ASEAN RPC/QR standardisation.

Chapter Six — Safeguards and Stakeholder Engagement

Framework and Obligations

Safeguards and stakeholder engagement are governed by the African Development Bank's updated Integrated Safeguards System (ISS)—effective 31 May 2024—and, where co-financed or applicable, the World Bank Environmental and Social Framework (ESF)—effective for IPF projects since 1 October 2018. These frameworks require risk-based assessments, robust labour and community protections, resource efficiency and pollution prevention measures, inclusive stakeholder engagement, grievance mechanisms, and disclosure throughout the project life cycle.

Instrument Suite and Life-Cycle Application

For each corridor and node, PCDE will prepare, disclose, and implement instruments commensurate with risk:

- **Screening and Scoping.** Risk classification under ISS/ESF; scoping notes for ESIA/ESMP/RAP/SEP; identification of vulnerable groups and contextual risks (including SEA/SH).
- **Assessment and Planning.** ESIA (environmental and social impact assessment), ESMP (management plan), RAP (resettlement action plan) where applicable, SEP (stakeholder engagement plan) with meaningful consultations and accessible formats.
- **Implementation and Monitoring.** Community health and safety, labour and working conditions, resource efficiency, biodiversity and cultural heritage protections; periodic safeguards monitoring with portfolio-level reporting.
- **Grievance Mechanisms and Remedies.** Accessible grievance mechanisms for workers and affected communities; disclosure of recourse mechanisms including AfDB's Independent Recourse Mechanism where applicable; remediation tracking and public summaries.

Stakeholder Engagement Protocol

Engagement follows ESF ESS10 and ISS Operational Safeguard guidance, ensuring inclusive participation, timely information disclosure, and responsiveness to concerns. Special measures protect vulnerable groups and address SEA/SH risks, consistent with updated ISS emphasis and ESF good-practice notes; engagement records are maintained and summarised publicly, safeguarding personal data.

Data Protection, Cybersecurity, and Incident Response

Where personal data are processed, PCDE operates a Privacy Information Management System (PIMS) conformant with ISO/IEC 27701, with privacy notices, data-subject rights, DPIAs for high-risk processing, and cross-border transfer controls. In African jurisdictions, interpretation is cognisant of the AU Malabo Convention baseline; for EU data subjects, GDPR obligations apply. Information security is governed by an ISMS conformant with ISO/IEC 27001 and enforced through Zero-Trust Architecture per NIST SP 800-207, with published posture summaries and incident-response procedures, including lawful breach notifications.

REC/Regional Consistency

Safeguards and engagement will be tailored to regional contexts while preserving the core obligations above. In COMESA, engagement will coordinate with IDEA's capacity-building platform and SDBA pilots to mitigate digital-market frictions; in SADC, measures will support DTS goals for universal access, harmonised frameworks, and digital skills; in EAC, stakeholder engagement will align with EA-RDIP and ONA/e-commerce reforms; in ASEAN, data-protection and payments security will consider RPC and QR standardisation guidance; in the Pan-Americas, MSME-centric engagement will leverage ConnectAmericas signalling and IDB Pay/PAGA payment-interoperability milestones to reduce transaction-cost barriers.

Disclosure and Assurance

All safeguards instruments, non-confidential engagement records, and grievance-mechanism summaries will be disclosed via PCDE's public registry and linked to OCDS/IATI identifiers to preserve traceability and external verification. Assurance will be provided through independent audits and verification missions—testing ISS/ESF implementation, OCDS/IATI completeness, and cyber/privacy controls—with management responses disclosed in annual public summaries.

References

- **Open data standards.**
  OCDS — Open Contracting Data Standard. *Documentation (latest)*: <https://standard.open-contracting.org/latest/en/>.
  IATI — International Aid Transparency Initiative. *Standard and governance*: <https://iatistandard.org/>. [unctad.org] [intosaipas.org]

- **Safeguards frameworks.**
  AfDB — Updated Integrated Safeguards System (ISS). *Effective 31 May 2024; press release*: <https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-groups-updated-integrated-safeguards-system-iss-becomes-effective-71539>.
  World Bank — Environmental and Social Framework (ESF). *Overview*: <https://www.worldbank.org/en/projects-operations/environmental-and-social-framework>. [webstore.ansi.org] [afdb.org]

- **Africa regional anchors.**
  COMESA — IDEA Programme. *Programme documents & PCU*: <https://www.comesa.int/inclusive-digitalisation-of-eastern-and-southern-africa-idea-program-documents/>; *Launch & targets*: <https://www.comesa.int/comesa-world-bank-launch-2-5-billion-programme-on-accelerating-digital-access/>.
  EU–COMESA — SDBA. *Scoping/workshop note*: <https://www.comesa.int/wp-content/uploads/2025/03/e-Comesa-Newsletter-Issue-No.-748.pdf>; *programme concept* (D4D Hub): <https://expertise-france.gestmax.fr/12619/1/comesa-sdba-expert-e-epayment-and-ecommerce-eastern-and-southern-africa-h-f>.
  SADC — Digital Transformation Strategy (DTS). *Draft, Oct 2022*: <https://www.sadc.int/sites/default/files/2025-08/EN%20-%205.2.3B%20-%20CM--SADC-ICT-INFO-MINISTERS-2023-4.8D%20-%20Draft%20SADC%20DTS_1.pdf>.
  EAC — ICT sector & EA-RDIP. *ICT*: <https://www.eac.int/268-sector/information-and-communications-technology-ict>; *EA-RDIP*: <https://www.eac.int/infrastructure/eardip>. [au.int], [iso.org] [academic.oup.com], [au.int] [ipsasb.org] [iso.org], [transparency.org]

- **Pan-Americas anchors.**
  ConnectAmericas — About/platform. <https://connectamericas.com/content/about-connectamericas>.
  IDB — IDB Pay. *Press release (Nov 2025)*: <https://www.iadb.org/en/news/idb-pay-expand-digital-payment-systems-latin-america-and-caribbean>.
  IDB Lab/WEF — PAGA (payments initiative). *Report (May 2022)*: <https://publications.iadb.org/en/accelerating-digital-payments-latin-america-and-caribbean>.

- **Asia anchors.**
  ASEAN — Regional Payment Connectivity (RPC). *ERIA policy brief (Jan 2025)*: <https://www.eria.org/uploads/Integrating-Digital-Payments-in-ASEAN.pdf>; *AMRO blog (Apr 2025)*: <https://amro-asia.org/enhancing-regional-payment-connectivity-across-asean3-economies>.

- **Cybersecurity & privacy baselines.**
  ISO/IEC 27001:2022 (ISMS): <https://www.iso.org/standard/27001>.

NIST SP 800-207 (Zero Trust Architecture): <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>.
ISO/IEC 27701:2025 (PIMS): <https://www.iso.org/standard/27701>.
AU — Malabo Convention (Cybersecurity & Personal Data Protection): <https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf>.
GDPR (EUR-Lex legal text): <https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04/eng>.
[afdb.org] [szi.gov.zm] [gdpr-info.eu] [iadb.org] [soma.larc.nasa.gov]

- **Integrity & AML/CFT.**
  ISO 37001:2025 (Anti-Bribery Management Systems): <https://www.iso.org/standard/37001>.
  FATF Recommendations (as amended Oct 2025): <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

Chapter Seven — Quality Assurance and Acceptance Tests

Purpose and Assurance Philosophy

Quality assurance (QA) and acceptance form the legal and technical basis upon which PCDE assets and services are certified fit-for-purpose, disclosed to the public, and handed over to operations. The regime couples measurable performance tests with compliance verification under the safeguards and transparency canon. Acceptance artefacts and their evidentiary trails are published in machine-readable form through the Open Contracting Data Standard (OCDS) for procurement and contract implementation, and through the International Aid Transparency Initiative (IATI) for activity and results disclosures, enabling independent scrutiny and cross-donor comparability.

Scope of QA and Acceptance

QA covers corridor-grade fiber and neutral IXPs, DEIC facilities and service operations, trust-service rails (identity, signatures/seals, certificates, secure payments), and applied AI services. Acceptance integrates performance telemetry with safeguards and cyber/privacy compliance checks anchored to the AfDB Updated Integrated Safeguards System (ISS), the World Bank Environmental and Social Framework (ESF), and security/privacy baselines (ISO/IEC 27001, NIST SP 800-207, ISO/IEC 27701).

A. Corridors and IXPs — Technical Acceptance Criteria

Corridor and IXP acceptance is based on demonstrable improvements to transport reliability and interconnection quality:

1. **Latency, Jitter, Availability.** Round-trip latency reduction against baseline on activated routes; jitter within agreed bounds; availability ≥99.95% across a rolling 30-day window. Test evidence is generated by calibrated measurements during agreed acceptance periods, then published as part of OCDS implementation updates.

2. **Path Diversity and Resilience.** Physical and logical path diversity verified against design; failover simulations demonstrating continuity under single-failure scenarios. Acceptance reports are appended to contract records with public summaries through OCDS.

3. **IXP Functional Tests.** Cross-connect validation, peering session stability, route propagation integrity, and minimum offload targets to local peering. Acceptance logs and summaries are

disclosed together with safeguards instrument status (ESIA/ESMP/RAP/SEP) in IATI activity documents.

All corridor/IXP acceptance must demonstrate that the underlying civil works and operational practices conform to applicable E&S instruments under ISS/ESF, including stakeholder engagement closure notes and grievance-mechanism summaries.

B. DEIC Nodes — Facilities and Service Acceptance

DEIC acceptance combines facility commissioning with service-level outcomes:

1. **Facility Commissioning.** Fit-out completion certificates; power, cooling, connectivity readiness; safety checks; accessibility provisions consistent with stakeholder plans and community health and safety requirements under safeguards.
2. **Programme Throughput and Inclusion.** Verified cohort intake and completion, local-content participation, gender and youth ratios consistent with REC targets (e.g., SADC DTS goals on universal access and skills). Outcome evidence is published via IATI results fields with supporting documentation.
3. **Service SLAs.** Time-to-onboarding for MSMEs, ticket resolution SLAs, and integration metrics for logistics, payments, and marketplace tools; amendments to contracts are posted through OCDS release packages to preserve traceability.

C. Trust-Service Rails — Identity, Signature/Seal, Certificates, Payments

Trust-service acceptance validates the legal-technical substrate for digital transactions:

1. **PKI/Identity Operations.** Root and issuing CA setup; certificate lifecycle (issuance, renewal, revocation); audit logs; cryptographic-agility plans for algorithm lifecycle. Privacy DPIAs and PIMS records are produced in conformance with ISO/IEC 27701 and, where applicable, GDPR/Malabo baselines.
2. **Electronic Signatures/Seals.** Conformance testing for signature/seal creation, validation, and time-stamping; non-repudiation evidence; acceptance reports appended to contract records and summarised publicly.
3. **Payment Interoperability Tests.** End-to-end tests for fast retail payments and e-commerce flows aligned with regional initiatives—COMESA SDBA/DRPP pilots, IDB Pay in the Americas, and ASEAN RPC local-currency/QR standardisation in Asia—with documented results and remediation notes.

D. Applied AI Services — Safety, Efficacy, and Security

AI acceptance combines model-performance verification with operational controls:

1. **Model Cards and Evaluation Summaries.** Published documentation for each use-case (e.g., health triage, adaptive learning, risk-based inspection), including scope, data, metrics, error bounds, and known limitations; public summaries linked in IATI activity documents.
2. **Zero-Trust Enforcement Artefacts.** Authentication/authorisation flows, device posture, micro-segmentation, and least-privilege evidence consistent with NIST SP 800-207, with ISMS governance under ISO/IEC 27001.

3. **Incident-Response Playbooks.** Run-books for detection, containment, eradication, recovery, evidence preservation, and lawful notifications (e.g., GDPR breach notification pathways where relevant); post-incident public summaries without exposing exploit vectors.

E. Publication and External Assurance

Acceptance artefacts (telemetry, reports, certificates, logs) are referenced by their OCDS release identifiers and IATI activity IDs to maintain the machine-readable end-to-end audit trail. Independent assurance engagements test IPSAS financial statements, OCDS publication integrity, IATI completeness/timeliness, ISS/ESF instrument implementation, and ISMS/PIMS/ZTA controls; summaries and management responses are disclosed annually.

Chapter Eight — MEL Integration and Public Dashboards

Purpose and MEL Architecture

Monitoring, Evaluation, and Learning (MEL) converts acceptance evidence and operational data into publicly verifiable outcomes. PCDE's MEL integrates IATI activity and results publishing with OCDS contract lifecycle data, creating dashboards that stakeholders and co-financiers can independently interrogate. The MEL architecture supports safeguards oversight (ISS/ESF), financing windows, and regional policy targets, while respecting data protection under ISO/IEC 27701 and security under ISO/IEC 27001/NIST SP 800-207.

Outcome Families and Indicator Logic

MEL indicators are grouped into three outcome families, each tied to underlying artefacts and disclosures:

1. **Access and Performance.** Corridor latency/jitter/availability; IXP offload ratios; DEIC facility readiness; trust-rail availability (identity/signature/seal); AI service uptime. Indicators draw from acceptance telemetry and contract SLAs and are published in periodic IATI results updates.

2. **Adoption and Inclusion.** DEIC cohort intake/completion; gender/youth/rural participation; MSME onboarding to payments and marketplaces; reduction in transaction-friction (time/cost). Indicators are aligned to REC targets (e.g., SADC DTS skills and universal access) and regional payment frameworks (SDBA, IDB Pay, ASEAN RPC).

3. **Governance and Integrity.** OCDS publication completeness, timeliness and amendment traceability; IPSAS budget-to-actual variance; safeguards instrument status and grievance-mechanism resolution rates; ISMS/PIMS posture summaries. Public dashboards surface these metrics using OCDS/IATI references.

Data Sources and Publication Cadence

- **OCDS:** Planning notices at feasibility; tender and award packages; contracts and implementation releases with acceptance telemetry and amendments; quarterly publication integrity checks.

- **IATI:** Organisation file (publisher-wide), activity files for each corridor/node/service, quarterly transaction and results updates, annual portfolio roll-ups. Reference pages and codelists are used to standardise reporting and ensure comparability.

Evaluation Design and Learning Loops

MEL embeds evaluation cycles that incorporate independent validation (where co-financed) and programme-level learning:

- **Verification Missions.** Safeguards verification against ISS/ESF; performance audits of disclosure integrity (OCDS/IATI); cyber/privacy posture assessments; results sampling in DEIC cohorts and payment-interoperability pilots; public summaries with corrective-action plans.
- **Regional Learning.** COMESA IDEA workshops and SDBA technical fora consolidating cross-country lessons; SADC DTS observatory inputs; EAC EA-RDIP coordination on cross-border digital integration; ASEAN RPC case-study exchanges; Americas MSME insights via ConnectAmericas and IDB Pay/PAGA community outputs.

Data Governance and Privacy

Public dashboards employ aggregation and minimisation to avoid exposure of personal data, applying **ISO/IEC 27701** controls and, where applicable, GDPR/Malabo transfer and breach-notification rules. Telemetry used for performance indicators is de-identified or summarised; any necessary personal-data processing is supported by DPIAs and data-subject rights mechanisms.

Risk-Responsive MEL

MEL incorporates early-warning thresholds and triggers—e.g., performance dips below acceptance levels, adoption shortfalls, grievance escalation, disclosure delays—initiating remedial workflows and, if needed, public notices appended to OCDS/IATI entries. This maintains stakeholder trust and aligns with ISS/ESF expectations for adaptive risk management and stakeholder engagement.

Public Transparency and Accountability

All dashboards and MEL documents reference their **OCDS release identifiers** and **IATI activity IDs**, ensuring end-to-end traceability from planning to acceptance and results. The approach operationalises PCDE's governance commitments and supports donor comparability, as demonstrated by IATI's reference model and widespread publishers; it also standardises procurement data for analysis and reuse per OCDS guidance.

References

- **Open-data standards and guidance.**
  Open Contracting Data Standard (OCDS): *Documentation (latest)* — <https://standard.open-contracting.org/latest/en/>.
  IATI — International Aid Transparency Initiative: *Standard and governance* — <https://iatistandard.org/>; *Reference/codelists (2.03)* — <https://reference.codeforiati.org/>. [unctad.org] [intosaipas.org], [idev.afdb.org]
- **Safeguards frameworks.**
  AfDB — Updated Integrated Safeguards System (ISS): *Effective 31 May 2024* — <https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-groups-updated-integrated-safeguards-system-iss-becomes-effective-71539>.
  World Bank — Environmental and Social Framework (ESF): *Overview* — <https://www.worldbank.org/en/projects-operations/environmental-and-social-framework>. [webstore.ansi.org] [afdb.org]
- **Regional anchors (illustrative acceptance/MEL interlocks).**
  COMESA — IDEA Programme: *PCU & programme documents* —

<https://www.comesa.int/inclusive-digitalisation-of-eastern-and-southern-africa-idea-program-documents/>; *Launch & targets* — <https://www.comesa.int/comesa-world-bank-launch-2-5-billion-programme-on-accelerating-digital-access/>.
EU–COMESA — SDBA: *Scoping workshop* — <https://www.comesa.int/wp-content/uploads/2025/03/e-Comesa-Newsletter-Issue-No.-748.pdf>.
SADC — Digital Transformation Strategy (DTS): <https://www.sadc.int/sites/default/files/2025-08/EN%20-%205.2.3B%20-%20CM--SADC-ICT-INFO-MINISTERS-2023-4.8D%20-%20Draft%20SADC%20DTS_1.pdf>.
EAC — ICT Sector / EA-RDIP: <https://www.eac.int/268-sector/information-and-communications-technology-ict>; <https://www.eac.int/infrastructure/eardip>.
Pan-Americas — ConnectAmericas; IDB Pay; PAGA: <https://connectamericas.com/content/about-connectamericas>; <https://www.iadb.org/en/news/idb-pay-expand-digital-payment-systems-latin-america-and-caribbean>; <https://publications.iadb.org/en/accelerating-digital-payments-latin-america-and-caribbean>.
Asia — ASEAN RPC: *Policy brief (ERIA)* — <https://www.eria.org/uploads/Integrating-Digital-Payments-in-ASEAN.pdf>; *AMRO blog* — <https://amro-asia.org/enhancing-regional-payment-connectivity-across-asean3-economies>. [au.int], [iso.org] [academic.oup.com] [ipsasb.org] [iso.org], [transparency.org]

- **Cybersecurity & privacy baselines.**
  ISO/IEC 27001:2022 (ISMS): <https://www.iso.org/standard/27001>.
  NIST SP 800-207 (Zero Trust Architecture): <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>.
  ISO/IEC 27701:2025 (PIMS): <https://www.iso.org/standard/27701>.
  GDPR (legal text): <https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04/eng>.
  AU — Malabo Convention (Cybersecurity & Personal Data Protection): <https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf>.

Chapter Nine — Close-Out and Handover

Purpose and Legal Effect

This Chapter codifies the procedures by which PCDE transitions completed assets and services from project delivery to steady-state operations, and how it preserves survival obligations for safeguards, transparency, cybersecurity, privacy, and integrity. Close-out is a formal legal act with evidentiary artefacts published under the Open Contracting Data Standard (OCDS) and the International Aid Transparency Initiative (IATI), and with compliance attested against the AfDB Updated Integrated Safeguards System (ISS) and, where applicable, the World Bank Environmental and Social Framework (ESF).

1. Close-Out Triggers and Preconditions

Close-out may be initiated only when all of the following preconditions are satisfied and evidenced:

1. **Technical Acceptance Achieved.** Corridors and IXPs have met acceptance thresholds (latency, availability, path diversity; peering offload), DEIC facilities and service SLAs are commissioned, trust-service rails (eID/e-signature/seal, time-stamping) are operational with completed payment-interoperability tests, and applied AI services have published model cards and

evaluation summaries. Acceptance artefacts must be linked to the contract record via OCDS implementation releases and to activities via IATI results.

2. **Safeguards Instruments Completed.** ESIA/ESMP/RAP/SEP instruments are finalised; stakeholder engagement records indicate meaningful consultations; grievance-mechanism cases are resolved or formally handed to operations with agreed remediation plans, all consistent with **ISS** and **ESF** requirements.
3. **Cybersecurity and Privacy Baselines in Place.** ISMS controls (ISO/IEC 27001) and Zero-Trust enforcement artefacts (NIST SP 800-207) are verified; PIMS documentation (ISO/IEC 27701) and DPIAs (as needed) are completed, with lawful breach-notification pathways (e.g., GDPR/Malabo) embedded in incident plans.
4. **Disclosure Integrity Validated.** Contract lifecycle data (planning, tender, award, contract, implementation, amendments) are complete in OCDS; activity/transaction/results are complete and timely in IATI; annual IPSAS accrual financial statements and audit opinions have been disclosed.

2. Handover Package — Contents and Format

The Secretariat shall assemble a **Handover Package** per asset/service, comprising:

- **Technical Dossier.** As-built documentation, acceptance test reports, telemetry summaries, configuration baselines, spares lists, and O&M manuals.
- **Safeguards Dossier.** Final ESIA/ESMP/RAP/SEP, grievance-mechanism closure report, and lessons-learned note consistent with **ISS/ESF** guidance.
- **Security & Privacy Dossier.** ISMS policies and control registers (ISO/IEC 27001), Zero-Trust architecture artefacts (NIST SP 800-207), PIMS artefacts (ISO/IEC 27701), DPIAs, data-retention schedules, and cross-border transfer log.
- **Operations Dossier.** Run-books for routine operations and incident response; vendor warranties and support SLAs; contact matrices for escalation.
- **Disclosure Index.** Table of **OCDS release identifiers** and **IATI activity IDs** covering the full life cycle, ensuring machine-readable traceability.

The Handover Package is deposited in the public registry with non-confidential artefacts accessible via OCDS/IATI links; protected artefacts (e.g., key material, personal data) are controlled under PIMS/ISMS policies.

3. Operations Transfer Protocol

3.1 Transfer Meeting and Sign-Off.

A formal **Operations Transfer Meeting** is convened with the receiving operator (SPV/NOC/DEIC operator/trust-service authority). The minutes annex the Handover Package index and confirm:

- custody of critical infrastructure and credentials;
- activation of O&M SLAs and warranty obligations;
- continuity of safeguards monitoring and grievance mechanisms;
- subscription to the publication cadence (OCDS/IATI) for operational updates.

Sign-off is recorded in both the contract OCDS implementation release and the IATI activity narrative.

3.2 Shadow-Ops Window.
For complex assets, a defined shadow-operations window (typically 90–180 days) allows joint operation, knowledge transfer, and KPI verification. Deviations trigger corrective-action plans and, if material, public notes appended to OCDS/IATI records.

4. Survival Obligations
The following obligations survive close-out and bind the operator and PCDE entities:

- **Transparency & Finance.** IPSAS accrual reporting; continued publication of contract amendments and performance under OCDS; periodic IATI updates of activity transactions and results.
- **Safeguards.** Ongoing monitoring and reporting under ISS/ESF; maintenance of stakeholder engagement and grievance mechanisms until commitments are fully discharged.
- **Cybersecurity & Privacy.** ISMS and Zero-Trust operations; breach-notification procedures pursuant to GDPR/Malabo (where applicable); PIMS maintenance and lawful data-retention/deletion.
- **Integrity & AML/CFT.** Anti-bribery controls (ISO 37001) and AML/CFT measures aligned to **FATF Recommendations**, including beneficial-ownership transparency where lawful.

5. Residual Risk Registers and Remediation
Prior to close-out, CDUs/SPVs shall update Residual Risk Registers covering:

- technical debt (e.g., deferred diversity segments or facility upgrades);
- E&S follow-ups (e.g., livelihood restoration milestones under RAPs);
- security/privacy risks (e.g., legacy components pending cryptographic agility);
- payment interoperability caveats (e.g., phased adoption in regional pilots).

Each residual item is assigned an owner, timeline, and verification pathway; status is summarised in the public registry and referenced to OCDS/IATI identifiers.

6. Archival, Registry, and Knowledge Management
6.1 Digital Archival.
All non-confidential artefacts are archived with persistent URIs linked to OCDS and IATI entries; schema and codelists follow the standards' reference documentation to ensure future re-use and analytics.

6.2 Lessons-Learned and Regional Sharing.
Lessons-learned summaries are fed into REC/platform fora (COMESA IDEA, SDBA technical workshops; SADC DTS observatory; EAC EA-RDIP coordination; ASEAN RPC case-studies; Americas ConnectAmericas/IDB Pay/PAGA communities) to support harmonisation and interoperability.

7. Post-Handover Audit and Public Confirmation
Within six months of close-out, the Secretariat commissions an independent post-handover audit to test:

- accuracy and completeness of OCDS and IATI publications;

- continued safeguards implementation (ISS/ESF);
- ISMS/PIMS/ZTA operational effectiveness (ISO/IEC 27001; ISO/IEC 27701; NIST SP 800-207).

Audit summaries and management responses are disclosed publicly and linked to the relevant OCDS/IATI identifiers.

8. Exceptional Termination or Suspension During Close-Out

If exceptional termination or suspension is required (e.g., legal impossibility, material integrity breaches), operators shall follow the escalation ladder defined in the Business Plan and Charter, preserving survival obligations for transparency, safeguards, and data protection. Public notices explaining the decision and remediation roadmaps must be appended to the OCDS and IATI records