SEPTEMBER 11, 2025

CODESA PILLAR II: DIGITALISATION AND CONNECTIVITY

For a connected COMESA Region

CREATED BY

EUSL AB

Care to Change the World

Table of Contents

CODESA PILLAR II: DIGITALISATION AND CONNECTIVITY

Executive Abstract

The Digitalisation and Connectivity pillar under CODESA aims to establish a regional digital public infrastructure that accelerates economic integration, governance modernization, and social inclusion across the COMESA region. Building on lessons from national initiatives such as South Sudan's digital transformation plan, this mission seeks to harmonize ICT policies, deploy broadband connectivity, and enable interoperable e-government services across Member States.

The mandate is to operationalize COMESA's Information & Networking and Infrastructure & Logistics program areas by delivering a ten-year program structured around four workstreams: (i) backbone and last-mile connectivity; (ii) e-government service stack; (iii) cybersecurity and data governance; and (iv) regional interoperability for trade and public services. Furthermore, the mandate is to digitalize the member states according to the Swedish Open Broadband Community standard and open up the market for Internet Service Providers, to increase connectivity speeds and lower the prices for end consumers.

The financing model combines multilateral and bilateral donor support, DFI co-financing, and private sector participation through PPPs and blended finance. Governance will be anchored in COMESA's institutional organs, with CODESA serving as the lead specialized agency under the oversight of the Council of Ministers.

Expected outcomes include:

- Deployment of regional broadband corridors and national last-mile connectivity solutions.
- Establishment of sovereign cloud environments and regional data centers.
- Rollout of digital identity systems and interoperable e-government platforms.
- Adoption of regional cybersecurity and data protection frameworks.
- Integration with the COMESA Digital Free Trade Area and AU Digital Transformation Strategy.

This pillar mitigates risks related to cyber threats, interoperability gaps, and financing volatility through a safeguards framework aligned with COMESA ICT policy, AfDB ISS, and ISO/IEC 27001 standards.

References:

- COMESA Information & Networking Division
- COMESA Infrastructure & Logistics Division
- COMESA ICT Status Report

Context

The COMESA region faces a dual challenge: **low broadband penetration** and **fragmented digital governance frameworks**, which constrain trade facilitation, public service delivery, and regional integration. Current ICT infrastructure is uneven, with significant disparities in backbone connectivity, data center capacity, and cybersecurity readiness. Many Member States rely on consumer-grade platforms for government operations, exposing them to data sovereignty risks and operational inefficiencies.

The urgency of digitalisation is amplified by the African Union's Digital Transformation Strategy (2020–2030) and COMESA's Digital Free Trade Area (DFTA) initiative, which call for harmonized ICT policies, interoperable systems, and secure digital platforms to enable cross-border trade and e-government services.

Lessons from South Sudan's digital transformation plan—anchored in Agenda 2074 and aligned with Agenda 2063—demonstrate that digitalisation is not a technical upgrade but a strategic imperative for governance, economic resilience, and social equity. South Sudan's phased approach (fiber backbone, sovereign cloud, digital ID, and e-services) provides a replicable model for COMESA, adapted to a regional scale.

This mission aligns with:

- **COMESA Treaty objectives** on regional integration and trade facilitation.
- **Agenda 2063** aspirations for inclusive growth and digital innovation.
- **Agenda for Social Equity 2074**, positioning digitalisation as a driver of social justice and economic opportunity.

By embedding digitalisation within COMESA's institutional framework, this pillar will create a **regional digital commons** that supports Member States in achieving sovereignty, interoperability, and resilience in the digital age.

3. Legal Basis

The legal foundation for this pillar is anchored in the **COMESA Treaty**, particularly Articles 3 and 4, which establish the objectives of regional integration, trade facilitation, and cooperation in infrastructure and ICT. The Treaty empowers the COMESA Authority and Council of Ministers to create specialized agencies and programmatic instruments to advance these objectives.

The Digitalisation and Connectivity pillar derives its legitimacy from:

- **COMESA Treaty and Protocols**: Providing the overarching legal mandate for ICT harmonization and digital trade facilitation.
- **COMESA ICT and e-Government Strategies**: Adopted under the Information & Networking Division, these strategies call for regional interoperability, cybersecurity frameworks, and digital public infrastructure (COMESA ICT Status Report).
- **Specialized Agency Precedent**: ACTESA's establishment under Article 182 sets a precedent for CODESA as a specialized agency with a mandate for digitalisation and social development.
- **Continental and Global Commitments**: Alignment with the **African Union Digital Transformation Strategy (2020–2030)**, the **African Continental Free Trade Area (AfCFTA)** digital protocols, and the **UN SDGs**, particularly Goals 9 (Industry, Innovation, and Infrastructure) and 16 (Peace, Justice, and Strong Institutions).

- **Data Governance Instruments**: COMESA's Data Privacy Policy and regional cybersecurity guidelines provide the normative basis for cross-border data flows and digital trust (Data Privacy Policy).

The pillar will operate under a **Council-endorsed mandate**, with CODESA serving as the implementing agency, subject to COMESA financial regulations, procurement rules, and safeguards frameworks.

4. Mandate, Objectives, and Theory of Change

Mandate

The Digitalisation and Connectivity pillar is mandated to:

- Deploy **regional broadband corridors** and last-mile connectivity solutions to bridge the digital divide.
- Establish **sovereign cloud environments** and regional data centers to ensure data sovereignty and resilience.
- Roll out **digital identity systems** and interoperable e-government platforms across Member States.
- Harmonize **cybersecurity, data protection, and ICT policies** to enable secure and trusted digital ecosystems.
- Integrate COMESA Member States into the **Digital Free Trade Area** and continental digital frameworks.

Strategic Objectives

1. **Infrastructure Development**: Expand regional fiber optic backbones and cross-border connectivity aligned with COMESA corridor strategies.
2. **Government Digitalisation**: Transition Member States from fragmented systems to secure, interoperable platforms for governance and service delivery.
3. **Digital Identity and Inclusion**: Implement regional standards for digital ID systems to enable access to services and trade.
4. **Cybersecurity and Data Governance**: Establish a regional cybersecurity operations center and harmonized data protection frameworks.
5. **Capacity Building**: Develop a Digital and Social Innovation Academy to train officials, SMEs, and civil society in digital governance and cybersecurity.

Theory of Change

The pillar is premised on the principle that **regional economic integration and governance modernization require a secure, inclusive, and interoperable digital ecosystem**. By addressing infrastructure gaps, policy fragmentation, and capacity deficits, the program will create enabling conditions for trade facilitation, efficient public services, and inclusive growth.

Causal Pathway:

- **Inputs**: Financial resources, technical expertise, ICT infrastructure, and policy instruments.

- **Activities**: Deployment of broadband corridors, establishment of data centers, rollout of digital ID systems, and harmonization of ICT policies.
- **Outputs**: Operational regional connectivity, functional e-government platforms, and standardized cybersecurity frameworks.
- **Outcomes**: Increased digital trade, improved governance efficiency, and enhanced citizen access to services.
- **Impact**: A digitally integrated COMESA region contributing to economic resilience, social equity, and sustainable development.

5. Scope and Workstreams

The Digitalisation and Connectivity pillar covers **regional digital transformation** across all COMESA Member States, structured into four interdependent workstreams that reflect both infrastructure and governance priorities:

Workstream 1: Backbone and Last-Mile Connectivity

- Deployment of **regional broadband corridors** aligned with COMESA transport and energy corridors.
- Expansion of **national last-mile connectivity** to underserved rural and peri-urban areas.
- Development of a **COMESA Broadband Strategy** harmonized with AU Digital Transformation Strategy and COMESA ICT frameworks.
- Integration of **satellite internet solutions** for remote regions.

Reference: COMESA Infrastructure & Logistics Division

Workstream 2: E-Government Service Stack

- Migration of Member States from fragmented systems to **secure, interoperable platforms** (e.g., Microsoft 365 Government Suite).
- Establishment of **regional cloud infrastructure** and sovereign data centers.
- Rollout of **digital identity systems** and citizen-facing e-services (civil registration, land records, procurement).
- Development of **regional interoperability standards** for cross-border services.

Reference: COMESA Information & Networking Division

Workstream 3: Cybersecurity and Data Governance

- Adoption of **regional cybersecurity frameworks** aligned with COMESA ICT policy and Malabo Convention.
- Establishment of a **Regional Cybersecurity Operations Center (R-CSOC)** for threat detection and incident response.
- Harmonization of **data protection laws** and cross-border data flow protocols.

- Implementation of **ISO/IEC 27001** and **NIST CSF** standards for all digital platforms.

Reference: COMESA ICT Status Report

Workstream 4: Regional Interoperability and Digital Trade

- Integration with **COMESA Digital Free Trade Area (DFTA)** and AU Digital ID initiatives.
- Development of **single-window systems** for trade facilitation and customs.
- Deployment of **regional payment interoperability frameworks** to enable digital commerce.
- Establishment of **open API standards** for private sector innovation.

Reference: COMESA Infrastructure Development

6. Stakeholders

The success of this pillar depends on a **multi-tiered stakeholder ecosystem** spanning policy, technical, and operational domains:

Institutional Stakeholders

- **COMESA Policy Organs**: Authority, Council of Ministers, and Intergovernmental Committee for strategic oversight.
- **CODESA**: Lead specialized agency for digitalisation and connectivity.
- **COMESA Divisions**: Information & Networking (ICT), Infrastructure & Logistics for technical alignment.
- **National Governments**: Ministries of ICT, Finance, Trade, and Justice for policy domestication and implementation.

Reference: COMESA Divisions and Units

Private Sector

- **Telecom Operators and ISPs**: For broadband deployment and last-mile connectivity.
- **Cloud and Technology Providers**: Microsoft, Huawei, and regional ICT firms for cloud migration and platform services.
- **Fintech and Payment Platforms**: For digital trade and interoperability solutions.

Development Partners and DFIs

- **African Development Bank (AfDB)**: Financing for digital infrastructure and governance programs.
- **World Bank, EU, USAID, FCDO**: Grants and technical assistance for ICT policy and capacity building.
- **Nordic Development Fund, Swedfund, SIDA**: Blended finance for connectivity and social inclusion.

Civil Society and Academia

- **Digital Rights Organizations**: For advocacy on privacy, inclusion, and accountability.
- **Universities and Research Institutes**: For curriculum development, innovation hubs, and policy research.

Regional and Continental Bodies

- **African Union Commission**: For alignment with AU Digital Transformation Strategy and AfCFTA digital protocols.
- **Regional CERT Networks**: For cybersecurity collaboration and incident response.

7. Governance

The governance structure for this pillar ensures **institutional legitimacy, fiduciary integrity, and operational accountability** within COMESA's framework.

7.1 Oversight

- **COMESA Council of Ministers**: Provides strategic oversight and policy direction.
- **CODESA Governing Board**: Responsible for programmatic decisions on digitalisation and connectivity.
- **COMESA Secretariat Divisions**: Information & Networking and Infrastructure & Logistics for technical alignment.

Reference: COMESA Divisions and Units

7.2 Joint Steering Committee (JSC)

A **Joint Steering Committee** will be established to:

- Approve annual work plans, budgets, and procurement plans.
- Monitor compliance with fiduciary, environmental, and digital safeguards.
- Resolve escalated issues and authorize corrective measures.

Composition:

- CODESA CEO (Chair), COMESA ICT and Infrastructure Directors, Member State representatives (rotational), DFIs and donors (observer), private sector and civil society (advisory).

7.3 Assurance and Compliance

- **Financial Assurance**: IPSAS-compliant accounting, annual external audits, quarterly financial reporting.
- **Procurement Assurance**: Open Contracting Data Standard (OCDS) for procurement transparency.
- **Digital Safeguards**: ISO/IEC 27001 and NIST CSF for cybersecurity; COMESA Data Privacy Policy for data governance.

7.4 Technical Committees

- **Connectivity Committee**: Oversees broadband and infrastructure rollout.
- **E-Government Committee**: Supervises platform migration and interoperability.
- **Cybersecurity Committee**: Coordinates regional CERT and data protection compliance.

8. Funding and Financial Model

The financial architecture reflects the **scale of ambition** and the **regional nature** of this program.

8.1 Sources of Finance

- **Multilateral and Bilateral Donors**: AfDB, World Bank, EU, USAID, FCDO for grants and concessional loans.
- **Development Finance Institutions (DFIs)**: AfDB and regional DFIs for infrastructure and cloud investments.
- **Private Sector**: PPPs for broadband, data centers, and digital platforms.
- **Member State Contributions**: Annual assessed contributions for core program costs.
- **Innovative Instruments**: Blended finance, credit guarantees, and diaspora investment mechanisms.

8.2 Financial Architecture

- **CODESA Digital Transformation Fund**: A ring-fenced fund under COMESA financial regulations, with IPSAS-compliant reporting and independent audits.
- **Disbursement Mechanism**: Performance-based tranches linked to milestones and safeguards compliance.
- **Transparency**: All procurement and financial transactions disclosed via OCDS-compliant platforms.

8.3 Indicative Budget Envelope

Estimated **USD 150 million, per country, over 10 years**, distributed as:

- Connectivity and Infrastructure: 40%
- E-Government Platforms: 25%
- Cybersecurity and Data Governance: 20%
- Capacity Building and MEL: 10%
- Contingency and Risk Buffer: 5%

Reference: COMESA ICT Status Report

9. Implementation Approach

This pillar will be executed through a phased, corridor-based, and standards-driven delivery model that aligns with COMESA's infrastructure and ICT programmes and reflects lessons from the SUDESA project plan (user-provided, 25 July 2025). It is explicitly structured to achieve depth of implementation in a subset of countries rather than superficial breadth across the entire region.

Delivery model and institutional roles. CODESA will serve as the lead specialized agency, operating a Joint Programme Implementation Unit under the policy oversight of the COMESA Council and with technical co-ordination by the Information & Networking and Infrastructure & Logistics Divisions. National execution will be delegated to line ministries and ICT regulators through country implementation compacts, with clear assignment of responsibilities for sovereign cloud, identity, e-services, and last-mile connectivity. This mirrors COMESA's division-anchored programming and specialized agency practice and ensures legal and procedural compliance under the Treaty organs (Information & Networking Division; Infrastructure & Logistics Division).

Geographic sequencing and coverage ceiling. Implementation will proceed in **three country waves** tied to corridor readiness and ICT policy maturity, with a cumulative ceiling of **10–11 Member States** by Year 10. Wave 1 (Years 1–3) will include four to five countries situated on priority transport corridors with existing fiber or cross-border interconnect prospects; Wave 2 (Years 3–7) will add three to four countries meeting minimum readiness thresholds; Wave 3 (Years 7–10) will add two further countries where reforms and financing have matured. Countries not selected will benefit from regional public goods (standards, specifications, shared cybersecurity capacity, and interoperability frameworks) and may elect to join later under separate financing. Corridor-based sequencing is consistent with COMESA's programme orientation to infrastructure corridors and ICT backbone development (COMESA Infrastructure Development; COMESA ICT Status Report).

Readiness and eligibility. Selection will be governed by a published Readiness Index covering (i) policy and legal alignment (data protection, e-transactions, cybersecurity), (ii) institutional capacity (digital governance structures, SOC/CERT linkages), (iii) infrastructure baselines (backbone presence, spectrum policy, data-center options), and (iv) co-financing commitments. These criteria reflect the SUDESA phasing logic (foundation → scale → consolidation) while scaling to a regional context and are anchored in COMESA's ICT harmonisation direction (COMESA ICT Status Report).

Workstream execution standards. Connectivity investments will follow open-access principles, neutral co-location, and corridor interconnect specifications agreed at regional level. The e-government stack will adopt a reference architecture for identity, payments, registries, workflows, and data exchange; country implementations will be certified against the architecture before scale. Cyber and data governance will conform to ISO/IEC 27001 controls and a NIST-aligned risk framework, with cross-border data transfer governed by COMESA model clauses and the Secretariat's Data Privacy Policy (Data Privacy Policy; COMESA ICT Status Report).

Procurement and fiduciary controls. All major procurements will use open competitive procedures with **OCDS**-compliant disclosure (plans, tenders, awards, contracts) and **IPSAS**-compliant financial reporting. Framework agreements may be established for repeatable categories (connectivity builds, cloud capacity, devices, SOC tooling), subject to gateway reviews at design, award, and operational readiness. This approach is consistent with COMESA's drive for transparency in regional programmes and supports donor assurance.

Safeguards and gateway regime. Subprojects will pass E&S and digital/data safeguard gates prior to contracting and commissioning. Corridor-level ESMFs and data protection impact assessments will be standard. Decision Gates at the end of Years 2 and 7 will condition progression to scale and consolidation on performance and compliance. The gate regime mirrors good practice for regional ICT programmes and the safeguard posture articulated in COMESA materials for ICT and infrastructure (Infrastructure & Logistics Division; COMESA ICT Status Report).

Capacity building and change management. A Digital and Social Innovation Academy will operate practitioner tracks for CIOs, enterprise architects, registrars, NCA regulators, and SOC analysts, complemented by country-specific change management programmes for civil services. This responds to systemic capacity gaps noted in SUDESA and aligns with COMESA's precedent capacity initiatives in the ICT and statistics domains.

Interoperability and regional public goods. Even where country coverage is deferred, the programme will deliver cross-border value through reference architectures, API specifications, e-signature and trust-services mutual recognition, a regional PKI root, federated identity profiles, and shared cyber threat intelligence feeds. This structure enables progressive onboarding and avoids fragmentation across Member States (Information & Networking Division).

10. Timeline and Milestones (2026–2036)

The ten-year horizon is divided into inception, foundation, scale, and consolidation phases with explicit coverage caps per wave and binding decision gates. Dates are indicative and will be confirmed at programme launch.

Inception and design (Months 0–6). The COMESA Council endorses the pillar mandate; CODESA constitutes the Joint Steering Committee and PIU; the Readiness Index and corridor selection criteria are adopted; baseline studies and initial corridor mapping are completed; model legal instruments for data, e-transactions, and cybersecurity are circulated for domestication. These steps align with Secretariat practice and the ICT programme's harmonisation trajectory (COMESA Divisions & Units; COMESA ICT Status Report).

Phase I – Foundation (Years 1–2). Wave 1 countries (four to five) sign implementation compacts. Corridor backbones are designed and contracted under OCDS disclosure; sovereign cloud landing zones and government collaboration suites are stood up; national PKI pilots and digital ID minimum viable products go live in selected registries; a regional CSOC nucleus is commissioned with initial Member State onboarding. **Decision Gate 1 (end-Year 2):** advancement to scale requires demonstrated service availability, security certification, and legal domestication milestones.

Phase II – Scale (Years 3–7). Wave 1 expands from pilots to national deployments of identity, core registries, and priority e-services; corridor backbones are lit and last-mile extensions tendered; Wave 2 countries (three to four) enter compacts and commence foundation builds. Regional interoperability artifacts (open API standards, trust lists, mutual recognition of e-signatures) are ratified for cross-border use, and a regional single-window profile is published for customs and trade facilitation, consistent with COMESA's Digital FTA orientation (COMESA Infrastructure Development; Information & Networking Division). By end-Year 7, cumulative operational coverage reaches **eight to nine countries**.

Phase III – Consolidation and targeted expansion (Years 8–10). Wave 3 countries (two) onboard where readiness and financing permit, while Waves 1–2 consolidate operations, transition to steady-state O&M and fee-for-service models, and complete full compliance with regional data/privacy and cyber protocols. The CSOC achieves full 24×7 regional operations with threat-intel sharing; corridor interconnect SLAs are standardized; cross-border service consumption (identity assertions, e-customs, trade certificates) is audited and certified. By Year 10, cumulative operational coverage is **ten to eleven countries** (not more than half of COMESA), with the balance benefitting from regional public goods and prepared for subsequent phases.

Milestone schedule (illustrative).

- **Q2–Q4 2026:** JSC/PIU constituted; Readiness Index published; corridor shortlist agreed; model clauses issued.
- **Q1 2027:** First compacts executed; corridor engineering designs complete; cloud landing zones established.
- **Q4 2027:** Identity MVPs live; government collaboration suites operational in Wave 1; CSOC nucleus active.
- **Q2 2028:** Gate 1 passed; corridor segments lit in at least two countries; open API and interoperability profiles published.
- **2029–2031:** Wave 2 compacts executed; national e-services scaled in Wave 1; regional trust services mutually recognized.
- **Q4 2032:** Gate 2 mid-term review concluded; coverage reaches eight to nine countries; cross-border single-window profile adopted.
- **2033–2035:** Wave 3 onboarding; fee-for-service models and PPP concessions operational; independent performance evaluation initiated.
- **Q4 2036:** Consolidation complete; ten to eleven countries in steady-state operations; final evaluation issued; scale pathway for remaining countries tabled to Council.

Decision gates and conditions. Progression between phases is conditioned on (i) safeguards compliance (E&S and data/cyber), (ii) fiduciary performance (IPSAS audits without qualification; OCDS completeness), (iii) service performance (uptime, security certifications), and (iv) legal domestication (data protection, e-transactions, cybersecurity). These conditions reflect both COMESA ICT policy expectations and prudent programme assurance for regional digital systems (COMESA ICT Status Report).

References

1. **COMESA – Information & Networking Division (ICT):** <https://www.comesa.int/information-networking-division-2/>
2. **COMESA – Infrastructure & Logistics Division:** <https://www.comesa.int/infrastructure-logistics-division/>
3. **COMESA – ICT Sector Status Report (2023):** <https://www.comesa.int/wp-content/uploads/2023/09/5.-CS.ID_.JTCM_.XIII_.3-ICT_EN_2.pdf>
4. **COMESA – Data Privacy Policy (Secretariat):** <https://www.comesa.int/wp-content/uploads/2022/09/Approved-Data-Privacy-Policy.pdf>

11. Risk Management

The risk management framework for this pillar is structured to address **strategic, operational, fiduciary, environmental, and cyber/data risks** across a multi-country, phased implementation. A formal **Risk Register** will be maintained by the Joint Programme Implementation Unit (PIU) and reviewed quarterly by the Joint Steering Committee.

11.1 Key Risk Categories and Illustrative Risks

- **Strategic and Political Risks**
  - Divergent national priorities delaying legal harmonisation and corridor sequencing.
  - Political instability in corridor countries disrupting infrastructure rollout.
- **Operational Risks**
  - Delays in broadband deployment due to procurement bottlenecks or contractor underperformance.
  - Limited institutional capacity to manage sovereign cloud and e-government platforms.
- **Fiduciary Risks**
  - Non-compliance with IPSAS and OCDS standards in procurement and financial reporting.
  - Risk of cost overruns in corridor builds and data center projects.
- **Cybersecurity and Data Risks**
  - Breaches of digital identity systems or government registries.
  - Cross-border data transfer vulnerabilities and lack of harmonised privacy laws.
- **Environmental and Social Risks**
  - Land acquisition disputes for corridor infrastructure.
  - Exclusion of women, youth, and rural communities from digital services.
- **Financial Risks**
  - Volatility in donor funding and private sector investment flows.
  - Exchange rate fluctuations affecting imported ICT equipment costs.

11.2 Mitigation Measures

- **Governance and Legal Instruments**: Use model clauses for data protection and cybersecurity; enforce readiness criteria before onboarding countries.
- **Capacity Building**: Deploy the Digital and Social Innovation Academy for regulators, SOC analysts, and CIOs.
- **Safeguards**: Apply AfDB ISS and World Bank ESF for E&S compliance; ISO/IEC 27001 and NIST CSF for cyber/data security.

- **Financial Controls**: IPSAS-compliant accounting, external audits, OCDS procurement disclosure.
- **Contingency Planning**: Maintain a financial buffer and cyber incident response protocols with 24-hour reporting to COMESA CERT.

12. Monitoring, Evaluation, and Learning (MEL)

The MEL framework ensures **accountability, adaptive management, and evidence-based decision-making** across the ten-year horizon.

12.1 MEL Architecture

- **Lead Responsibility**: MEL Unit within the Joint PIU, reporting to the Joint Steering Committee and COMESA Secretariat.
- **Evaluation Moments**:
  - **Baseline Assessment**: Completed during inception phase.
  - **Mid-Term Review**: End of Year 5 to inform corridor expansion and course correction.
  - **Final Evaluation**: End of Year 10 to assess impact and sustainability.

12.2 Data Systems

- **Financial Data**: IPSAS-compliant reporting integrated with COMESA systems.
- **Procurement Data**: OCDS-compliant disclosure for transparency.
- **Programme Data**: Digital dashboards tracking KPIs in real time, linked to corridor readiness and service availability metrics.

12.3 Key Performance Indicators (Illustrative)

- **Connectivity**: Kilometers of fiber deployed; % of corridor coverage achieved.
- **E-Government**: Number of Member States with operational digital ID and core registries.
- **Cybersecurity**: Mean time to detect/respond to incidents; number of countries with operational SOC nodes.
- **Interoperability**: Number of cross-border services certified (e-signature, customs single window).
- **Inclusion**: % of women and youth accessing digital services in participating countries.

12.4 Learning and Adaptation

- **Annual Learning Reviews**: Document lessons and best practices for corridor replication.
- **Knowledge Products**: Policy briefs, technical toolkits, and case studies published on COMESA platforms.
- **Regional Knowledge Exchange**: Annual Digital Integration Forum under COMESA auspices.

13. Key Performance Indicators (KPIs)

The KPI framework is designed to be **auditable, regionally comparable, and aligned with COMESA ICT priorities**, the AU Digital Transformation Strategy, and the COMESA Digital Free Trade Area initiative. Indicators will be disaggregated by gender and geography where applicable.

13.1 Core KPI Set

Domain	**Indicator**	**Baseline (2026)**	**Target Y5 (2031)**	**Target Y10 (2036)**	**Source**
Connectivity	Kilometers of fiber backbone deployed in corridors	TBD	8,000 km	15,000 km	PIU reports
	% of corridor coverage with broadband ≥10 Mbps	<10%	50%	80%	COMESA ICT dashboards
E-Government	Member States with operational sovereign cloud environments	0	5	10–11	PIU verification
	Ministries migrated to secure collaboration suites (Wave 1 & 2)	0	50%	100%	Country reports
Digital Identity	Citizens enrolled in digital ID systems in participating countries	0	20M	50M	PIU dashboards
Cybersecurity	Regional CSOC operational with 24/7 coverage	No	Partial	Full	PIU
	Mean time to detect/respond to cyber incidents (MTTD/MTTR)	TBD	≤24/48 hrs	≤8/24 hrs	SOC logs
Interoperability	Cross-border services certified (e-signature, customs single window)	0	3	8	COMESA ICT
Inclusion	% of women and youth accessing e-services in participating countries	TBD	40%	50%	MEL surveys
Transparency	% of procurement packages disclosed via OCDS	0	80%	100%	PIU procurement

Domain	Indicator	Baseline (2026)	Target Y5 (2031)	Target Y10 (2036)	Source
Financial Integrity	IPSAS-compliant financial statements and unqualified audits	N/A	Yes annually	Yes annually	COMESA Finance

Notes: KPI dictionary and verification protocols will be codified in Annex A. All procurement and financial indicators will follow **OCDS** and **IPSAS** standards; cyber metrics will align with **ISO/IEC 27001** and **NIST CSF**.

14. PESTEL Analysis

14.1 Narrative

Political:
The COMESA Treaty and Council decisions provide a strong legal basis for ICT harmonisation and digital trade facilitation. However, political instability in some Member States and divergent national priorities may delay corridor sequencing and legal domestication (COMESA Divisions & Units).

Economic:
Digitalisation is a growth enabler but requires significant upfront investment. Infrastructure finance gaps and limited fiscal space in some countries necessitate blended finance and PPP models. Corridor-based sequencing mitigates cost escalation (COMESA Infrastructure & Logistics Division).

Social:
Digital inclusion is critical in a region where rural connectivity and gender gaps persist. Without targeted interventions, women, youth, and marginalized groups risk exclusion from digital services (COMESA ICT Status Report).

Technological:
ICT readiness varies widely across Member States. Cybersecurity posture and data governance frameworks are uneven, creating interoperability and trust challenges. Harmonised standards and shared SOC capacity are essential (COMESA Data Privacy Policy).

Environmental:
Corridor infrastructure projects may trigger land acquisition and environmental risks. Climate resilience and energy efficiency must be embedded in design (e.g., modular renewable-powered data centers).

Legal:
Data protection, e-transactions, and cybersecurity laws are not uniformly enacted. Harmonisation and mutual recognition agreements are prerequisites for cross-border digital services (COMESA ICT Status Report).

14.2 PESTEL Table

Factor	Drivers / Constraints	Implications	Mitigation / Leverage
Political	Treaty organs; specialized agency mandates; instability in some states	Enables harmonisation; risk of delays	Use Council/IC channels; phased onboarding

Factor	**Drivers / Constraints**	**Implications**	**Mitigation / Leverage**
Economic	Infrastructure finance gaps; SME capital needs	Requires blended finance and PPPs	Corridor sequencing; guarantees; DFI co-financing
Social	Inclusion gaps; digital literacy deficits	Risk of exclusion	Academy programmes; gender/youth quotas
Technological	ICT readiness variance; cyber posture gaps	Interoperability and security risks	Regional standards; SOC/CERT federation
Environmental	Corridor builds; energy intensity	Compliance burden	ESMFs; renewable-powered data centers
Legal	Data/privacy, e-signature, procurement	Compliance complexity	Model clauses; mutual recognition

15. SWOT Analysis

15.1 Narrative

Strengths.

The pillar is anchored in an established regional architecture with clear program lines in **Infrastructure & Logistics** and **Information & Networking (ICT)**, enabling corridor-based broadband deployment and harmonised digital governance instruments. The COMESA Secretariat and its policy organs confer convening power and continuity, while the specialized-agency precedent (e.g., ACTESA) provides a tested institutional model for positioning **CODESA** as the lead digitalisation agency. The Secretariat's **Data Privacy Policy** and ongoing ICT harmonisation agenda furnish normative anchors for trust services, cross-border data flows, and cybersecurity cooperation, which can be embedded into the programme's reference architectures and assurance regimes (Infrastructure & Logistics Division; Information & Networking Division; COMESA Divisions & Units; COMESA Data Privacy Policy; COMESA ICT Status Report 2023).

Weaknesses.

Member States exhibit heterogeneous ICT readiness, legal frameworks, and institutional capacity, creating execution risk and uneven uptake of interoperability standards. Legacy platforms, vendor lock-in, and limited cyber posture (including SOC/CERT maturity) may delay migration to sovereign cloud models and regional trust frameworks. Fragmentation in e-transactions, e-signature, and consumer protection laws remains material, with gaps identified in regional ecommerce legal readiness that can impede cross-border digital services without targeted legal domestication support (COMESA ICT Status Report 2023; COMESA E-commerce Study (Draft), 2022).

Opportunities.

Continental frameworks—the **AU Digital Transformation Strategy (2020–2030)** and the **AfCFTA** digital workstreams—create policy momentum for interoperable identity, e-government, and digital trade, supporting COMESA's **Digital Free Trade Area** orientation. Corridor-based broadband, shared regional data-center capacity, and a federated CSOC can deliver scale economies and trust at lower unit cost. DFIs and partners continue to prioritise digital infrastructure and governance, enabling blended finance for backbones, sovereign clouds, and last-mile access, with design principles traceable to the SUDESA methodology for sequencing, capacity building, and legal enablement (AU Digital Transformation Strategy; AfCFTA Secretariat; Infrastructure & Logistics Division; SUDESA Project Plan – user provided, 25 July 2025).

Threats.
Political instability, fiscal constraints, and currency volatility may disrupt corridor builds and cloud procurements, while sophisticated cyber threats could erode confidence in digital ID and e-services if regional security baselines and incident response are not uniformly applied. Persistent legal heterogeneity across data protection and e-transactions, if unresolved, risks balkanising digital markets and delaying cross-border service certification; likewise, environmental and land-use issues around corridor works can trigger project delays absent robust safeguards instruments (COMESA ICT Status Report 2023; COMESA E-commerce Study (Draft), 2022; Infrastructure & Logistics Division).

15.2 SWOT Tables

Internal Factors

Strengths	**Weaknesses**
Established COMESA programme lines in **Infrastructure & Logistics** and **Information & Networking (ICT)** support corridor-based connectivity and digital governance; Secretariat convening authority and specialized-agency precedent (ACTESA) offer a viable model for CODESA; Secretariat **Data Privacy Policy** and ICT harmonisation workstreams provide normative anchors for trust and interoperability. (Infrastructure & Logistics Division; Information & Networking Division; COMESA Divisions & Units; Data Privacy Policy)	Marked variance in Member State ICT capacity and cyber readiness; legacy systems and vendor lock-in increase migration complexity; gaps in e-transactions, e-signature, and consumer protection laws slow interoperability; uneven MEL and data quality across institutions. (COMESA ICT Status Report 2023; COMESA E-commerce Study (Draft), 2022)

External Factors

Opportunities	**Threats**
AU and AfCFTA digital agendas strengthen the policy case for interoperable identity, e-government, and digital trade; corridor-based backbones, regional data-centre capacity, and a federated CSOC can deliver scale efficiencies; DFI appetite for digital infrastructure and governance supports PPP and blended finance models; SUDESA-style sequencing and capacity building offer tested implementation patterns. (AU Digital Transformation Strategy; AfCFTA Secretariat; Infrastructure & Logistics Division)	Political instability and fiscal constraints may disrupt corridor and cloud rollouts; advanced cyber threats risk undermining trust in digital ID and cross-border services; persistent legal heterogeneity across data protection and e-transactions could fragment markets; land acquisition and environmental issues can delay corridor builds. (COMESA ICT Status Report 2023; COMESA E-commerce Study (Draft), 2022)

16. Safeguards

The safeguards framework integrates **environmental and social (E&S) standards** with **digital and data governance protocols**, ensuring compliance with COMESA policy instruments and international norms.

16.1 Environmental and Social Safeguards

- **Framework Alignment**: AfDB Integrated Safeguards System (ISS) and World Bank Environmental and Social Framework (ESF) adapted to COMESA's regional context.
- **Screening and Categorization**: All corridor and data center projects undergo E&S screening; instruments include ESIA, ESMP, and RPF where land acquisition is involved.
- **Key E&S Risks**:
  - Land acquisition disputes for corridor fiber routes.
  - Biodiversity impacts from infrastructure works.
  - Gender exclusion in digital access.
- **Mitigation Instruments**:
  - **Environmental and Social Management Framework (ESMF)** for corridor-level interventions.
  - **Gender Action Plan (GAP)** to ensure equitable participation.
  - **Grievance Redress Mechanism (GRM)** accessible at national and regional levels.

References:

- AfDB ISS
- World Bank ESF

16.2 Digital and Data Safeguards

- **Policy Anchors**: COMESA Data Privacy Policy and ICT harmonisation instruments (Data Privacy Policy).
- **Standards**:
  - ISO/IEC 27001 for information security management.
  - NIST Cybersecurity Framework for risk-based controls.
- **Controls**:
  - Encryption of digital ID and e-service data at rest and in transit.
  - Role-based access and multi-factor authentication.
  - Incident response protocols with 24-hour reporting to COMESA CERT.
- **Cross-Border Data Governance**:
  - Model clauses for data transfer.

  - Mutual recognition agreements for e-signatures and trust services.

16.3 Safeguards Governance

- **Safeguards Unit**: Embedded in the Joint PIU, reporting to the Joint Steering Committee and COMESA Secretariat.
- **Disclosure**: All safeguards instruments published on COMESA and CODESA portals in line with **OCDS** transparency commitments.

17. Communications and Advocacy

The communications strategy positions this pillar as a **flagship regional integration initiative**, reinforcing COMESA's leadership in digital transformation.

17.1 Objectives

- Build political and public support for ICT harmonisation and corridor-based connectivity.
- Mobilize private sector and DFI participation in blended finance structures.
- Ensure transparency and accountability to Member States and development partners.

17.2 Target Audiences

- **Primary**: COMESA policy organs, Member State ministries, CODESA Board.
- **Secondary**: Development partners, DFIs, private sector, civil society, and media.

17.3 Channels and Tools

- **Institutional Channels**: COMESA and CODESA websites, quarterly bulletins, policy briefs.
- **Digital Platforms**: Social media campaigns aligned with COMESA ICT outreach; webinars and e-learning modules.
- **Advocacy Events**: Annual **COMESA Digital Integration Forum**; side events at AU and AfCFTA summits.
- **Transparency Instruments**: OCDS-compliant procurement disclosures; IPSAS-based financial reporting; MEL dashboards.

17.4 Key Messages

- The pillar delivers **regional public goods**: harmonised ICT policies, interoperable systems, and secure digital corridors.
- It operationalises **Agenda 2063**, **AfCFTA**, and COMESA's Digital FTA commitments.
- It safeguards **inclusion, sustainability, and transparency**, ensuring benefits for women, youth, and SMEs.

References:

- COMESA Information & Networking Division
- COMESA ICT Status Report

18. Sustainability and Exit Strategy

The sustainability framework ensures that the Digitalisation and Connectivity pillar transitions from a **donor-supported program** to a **self-sustaining regional mechanism** embedded within COMESA's institutional architecture and Member State systems.

18.1 Institutional Sustainability

- **Integration into COMESA Structures**:
    - CODESA will be institutionalized as a **COMESA Specialized Agency** under Article 182 of the Treaty, mirroring ACTESA's legal status.
    - Governance functions (Joint Steering Committee, technical committees) will transition into COMESA's standing ICT and infrastructure committees.
- **Member State Ownership**:
    - National ICT authorities and ministries will embed digitalisation mandates into their statutory functions.
    - Regional interoperability standards and cybersecurity protocols will be domesticated by participating countries by Year 7.

Reference: COMESA Specialized Agencies

18.2 Financial Sustainability

- **Cost Recovery and Fee-for-Service Models**:
    - Regional cloud and trust services will adopt subscription-based pricing for government and private sector users.
    - Corridor fiber infrastructure will operate under open-access models with wholesale tariffs to recover O&M costs.
- **Public-Private Partnerships (PPPs)**:
    - Data centers and cybersecurity services will be operated under PPP concessions, reducing fiscal burden on Member States.
- **Regional Digital Transformation Fund**:
    - The CODESA Digital Transformation Fund will evolve into a revolving facility capitalized by Member State contributions, DFI co-financing, and private equity participation.

18.3 Operational Sustainability

- **Capacity Building**:
    - The Digital and Social Innovation Academy will institutionalize continuous training for regulators, SOC analysts, and CIOs.
- **Technology Transfer**:
    - Open-source reference architectures and interoperability standards will reduce vendor lock-in and ensure maintainability.

18.4 Exit and Handover

- **Exit Criteria**:
  - Full operationalization of corridor connectivity and e-government platforms in at least 10–11 Member States.
  - Regional CSOC and interoperability frameworks functioning under COMESA governance.
  - Achievement of ≥80% of KPI targets verified through independent evaluation.
- **Handover Mechanism**:
  - By Year 10, the Joint PIU will be dissolved, and residual functions absorbed by CODESA and COMESA divisions.
  - Knowledge assets (policy toolkits, interoperability profiles, MEL datasets) will be archived in COMESA's Knowledge Management System for open access.