DECEMBER 3, 2025

DESA BROADBAND & INFRASTRUCTURE PROGRAMME

GSIA'S PLATFORM FOR PUBLIC/PRIVATE PARTNERSHIPS

Created by

EUSL AB

Care to Change the World

Table of Contents

DESA Broadband & Infrastructure Program

Chapter 1 — Programme Title, Mandate, Scope, Instruments, and Outcomes

DESA Broadband & Infrastructure Program (DBIP), DBIP, is DESA's sovereign, open-access broadband programme designed to deliver affordable, high-speed Internet at national scale, implemented through a backbone-plus-community model inspired by Sweden's "Open Broadband Community" practice and adapted to local regulatory contexts. The programme establishes neutral wholesale fibre and complementary satellite capacity, and then opens "portals" for EUSL members and other authorised service providers to offer digital services directly to end-users (e.g., streaming, education, e-government, fintech), following non-discriminatory access rules. Sweden's municipal open-access model—where public infrastructure enables multiple retail providers—has delivered near-universal gigabit availability and low consumer prices; its core principles of wholesale neutrality and multi-provider competition inform DBIP's architecture.

Mandate

DBIP's mandate is to deliver affordable, high-speed access through sovereign backbone and community last-mile models, anchored in DESA's equity-first standards and aligned with continental and global agendas. The programme targets entry-level tariffs approximating USD 5/month for 100 Mbps unlimited in qualified urban markets and regulated rural offers that satisfy affordability benchmarks (≤ 2% of monthly GNI per capita, per the UN Broadband Commission). The USD 5 figure is a social-policy target that will be phased via tariff regulation, wholesale price caps, and targeted subsidies—including Universal Service Funds (USFs) and social vouchers—so that effective consumer pricing meets the Commission's affordability thresholds across income quintiles.

Scope

DBIP implements a **n**ational fibre backbone with satellite complements for remote and hard-to-reach areas, Tier III data centres for carrier-neutral co-location and caching, and municipal open-access networks at the metro and community levels. This scope reflects best practice in open access (transparent wholesale access, fair and reasonable non-discriminatory terms), and aligns with OECD recommendations to bridge connectivity divides via affordability, quality, and rural inclusion.

Instruments

DBIP deploys Open Broadband Community frameworks that separate passive/active layers and retail service provision, tariff regulation to enforce affordability goals (benchmarked to ≤ 2% GNI per capita and local cost-of-service), and Universal Service Funds for rural last-mile builds, social tariffs, school connectivity, and devices. USFs are structured per ITU guidance to ensure legal clarity, disbursement capacity, measurable objectives, and transparent accountability, thereby addressing common weaknesses that have limited USF effectiveness in the past.

Outcomes

DBIP delivers mass household and school connectivity, stable uptime through carrier-grade core and edge redundancies, and equitable rural access by blending fibre, fixed-wireless, and satellite. The programme's open-access portals invite EUSL member services (e.g., Spotify or other OTT providers) to

reach users over neutral infrastructure, echoing Sweden's municipal model where service-provider diversity and consumer choice catalysed digital ecosystems and new firms.

Chapter 2 — Legal Mandate and Purpose; Alignment with Continental and Regional Agendas

Compulsory/Elective Status under DESA

DBIP is designated a compulsory programme for DESA national deployments in countries where digital infrastructure gaps impede education, governance, market access, and social equity. In jurisdictions with adequate sovereign broadband, DBIP operates as an elective upgrade and harmonisation track to standardise open-access, affordability safeguards, and MRV (measurement, reporting, verification). The compulsory designation reflects DESA's statutory duty to ensure universal, affordable connectivity as a precondition for equity-led development; the elective track applies where national strategies already meet or exceed DBIP standards but benefit from DESA's compliance and transparency frameworks (open-access neutrality, affordability KPIs, and public dashboards). The programme's legal basis relies on national telecom statutes, DESA Operating Circulars, and ministerial MoUs that recognise open-access wholesale duties and affordability obligations consistent with OECD policy guidance and the UN Broadband Commission's targets.

Alignment with Agenda 2074, Agenda 2063, AfDB High 5, and Regional Strategies

DBIP advances Agenda for Social Equity 2074 by operationalising equitable access to essential digital services (SGGs on education, governance, and ethical technology), embedding affordability and inclusion as measurable standards across infrastructure and markets. It integrates MRV so that connectivity is not merely available but fair in incidence and outcome.

DBIP directly supports Agenda 2063—"The Africa We Want"—by delivering world-class communications infrastructure (Goal 10) that underpins prosperous, inclusive growth (Aspiration 1), continental integration (Aspiration 2), good governance (Aspiration 3), and people-driven development through youth and women's empowerment (Aspiration 6). The fibre backbone, data centres, and open-access municipal networks concretely contribute to "Communications and Infrastructure Connectivity", a named goal under Agenda 2063.

DBIP is aligned with AfDB's High 5 priorities: it *Lights up and Powers Africa* through digital infrastructure and intelligent energy management in data centres; it *Feeds Africa* by enabling precision agriculture, market access, and logistics data; it *Industrialises Africa* via digital manufacturing, fintech rails, and cloud services; it *Integrates Africa* through cross-border fibre corridors and neutral IXPs; and it *Improves Quality of Life* by providing affordable connectivity for education, health, and public services. The alignment is explicit in AfDB strategy documents that link infrastructure, regional integration, governance, and skills to inclusive, green growth.

Regional Strategies and Harmonisation

DBIP's legal purpose includes harmonisation with COMESA, SADC, and EAC standards and programmes, focusing on cross-border backbone interconnection, open-access wholesale rules, and shared affordability benchmarks. The programme's policy architecture references OECD's Recommendation on Broadband Connectivity and open-access principles—wholesale access on fair, transparent, and non-discriminatory terms—to ensure compatibility with regional regulatory reforms and to promote rural inclusion through targeted USF deployment.

Affordability Covenant and Social Pricing
To make the USD 5/month (100 Mbps) target credible, DBIP couples tariff regulation with affordability covenants derived from global benchmarks—entry-level services priced below 2% of monthly GNI per capita by 2025 in LMICs—while acknowledging that poor households may require deeper subsidies or lifeline tiers. ITU and Broadband Commission data show affordability improving globally but still challenging in low-income economies; DBIP's covenant mandates phased reductions, wholesale cost controls, and targeted vouchers funded by USFs and blended finance.

Open Broadband Community Implementation
Legally, DBIP formalises the Open Broadband Community model via Operating Circulars that: (i) separate passive infrastructure ownership from active operations and retail provision; (ii) impose neutrality on access terms; and (iii) create service portals where EUSL member firms (e.g., streaming platforms like Spotify) can register and offer services on equal terms—replicating Sweden's three-tier open-access structure (network owner, communications operator, retail service provider). This structure is proven to expand provider diversity and consumer choice while keeping prices low.

Purpose Statement
DBIP's legal purpose is to guarantee universal, affordable, high-quality connectivity as a public-interest infrastructure, administered under DESA's equity-first standards and audited for compliance. By binding affordability, neutrality, and cross-sector portals into law and Operating Circulars, DBIP transforms broadband from a private-utility paradigm into open public infrastructure that catalyses governance, education, markets, and social equity—meeting Agenda 2063 aspirations and AfDB's High 5 priorities with measurable, transparent outcomes

Chapter 3 — Strategic Objectives

3.1 Purpose of Strategic Objectives

The strategic objectives of DBIP articulate its role as a foundational enabler of DESA's equity-driven digital transformation. These objectives are not isolated technical targets; they are governance instruments designed to advance education, markets, and social inclusion through lawful, affordable, and resilient connectivity. Each objective is framed to deliver measurable socio-economic impact while maintaining compliance with DESA's ethical and fiduciary standards.

3.2 Core Objective 1 — Universal and Affordable Connectivity

DBIP's first strategic objective is to guarantee universal, high-speed broadband access at socially equitable tariffs, anchored in affordability covenants that benchmark entry-level pricing to ≤ 2% of monthly GNI per capita and target USD 5/month for 100 Mbps unlimited in urban markets. This objective operationalises the UN Broadband Commission's affordability standard and integrates tariff regulation, wholesale neutrality, and Universal Service Funds (USFs) to ensure rural inclusion.

Narrative Impact:

- **Governance:** Establishes a legal and regulatory framework for open-access wholesale, preventing monopolistic pricing and ensuring transparency in cost structures.
- **Education:** Enables compliance with FCC-aligned school connectivity benchmarks (≥ 1 Mbps per student), ensuring digital learning continuity and equitable access to online curricula.
- **Markets:** Reduces transaction costs for SMEs and entrepreneurs by providing predictable, low-cost connectivity, fostering e-commerce and fintech adoption.

- **Social Equity:** Bridges the urban-rural divide by subsidising last-mile builds and lifeline tariffs, ensuring that connectivity is not a privilege but a guaranteed public good.

Illustrative Table — Affordability Benchmarks vs. DBIP Targets

Indicator	Global Benchmark	DBIP Target
Entry-level broadband cost as % of GNI per capita	≤ 2% (UN Broadband Commission)	≤ 2%
Urban retail tariff for 100 Mbps unlimited	Varies (USD 15–30 typical LMIC)	**USD 5/month**
Rural lifeline tariff	Subsidised via USF	**≤ USD 3/month**

References: UN Broadband Commission affordability targets; ITU affordability guidelines.

3.3 Core Objective 2 — Sovereign Backbone and Open-Access Architecture

The second objective is to deploy a sovereign fibre backbone complemented by satellite for remote areas, integrated with municipal open-access networks. This architecture ensures neutrality and multi-provider competition, replicating the Swedish "Open Broadband Community" model that catalysed service diversity and consumer choice.

Narrative Impact:

- **Governance:** Positions the backbone as a strategic national asset under DESA stewardship, with Operating Circulars mandating open-access and non-discriminatory wholesale terms.
- **Education:** Guarantees high-capacity interconnection for schools and universities, enabling synchronous learning and research collaboration.
- **Markets:** Creates a level playing field for OTT providers (e.g., Spotify, EdTech platforms) to deliver services via DESA portals, stimulating innovation and local content ecosystems.
- **Social Equity:** Prevents digital exclusion by ensuring rural nodes are connected through hybrid fibre-satellite solutions, supported by USF disbursements.

Table — Infrastructure Layers and Governance Instruments

Layer	Description	Governance Instrument
Passive (fibre, ducts, towers)	Sovereign ownership under DESA	DESA Infrastructure Charter
Active (switching, routing)	Managed by neutral operator	Operating Circular on Open Access
Retail services	Offered via DESA portals	Service Provider MoUs

3.4 Core Objective 3 — Integration of Tier III Data Centres and Edge Infrastructure

DBIP's third strategic objective is to deploy Tier III carrier-neutral data centres and edge nodes to ensure low-latency access, secure hosting, and regional content delivery. These facilities underpin sovereign control over critical data flows and enable caching for high-demand services such as education platforms, health systems, and OTT media.

Narrative Impact:

- **Governance:** Positions data centres as regulated national assets under DESA's Infrastructure Charter, ensuring compliance with data protection laws and algorithmic transparency obligations.
- **Education:** Facilitates local hosting of e-learning platforms and examination systems, reducing latency and improving reliability for schools and universities.
- **Markets:** Provides SMEs and startups with affordable co-location and cloud services, stimulating digital entrepreneurship and reducing dependency on foreign hyperscalers.
- **Social Equity:** Guarantees equitable access to secure hosting for public services and civil society organisations, preventing concentration of digital power in private monopolies.

Table — Data Centre Classification and Service Layers

Facility Type	Uptime Tier	Function	Governance Instrument
National Core DC	Tier III	Sovereign hosting, IXPs, caching	DESA Infrastructure Charter
Regional Edge Node	Tier II+	Content delivery, local caching	Operating Circular on Edge Services
Municipal Micro-DC	Tier I+	Community-level hosting	PPP Framework for Local Access

3.5 Core Objective 4 — Resilience and Continuity for Critical Services

The fourth objective is to embed resilience and continuity measures across DBIP infrastructure, ensuring uninterrupted connectivity for education, health, governance, and emergency services. This includes redundant backbone routes, satellite failover for remote areas, and disaster recovery protocols aligned with NIST SP 800-34 and SP 800-184.

Narrative Impact:

- **Governance:** Establishes mandatory contingency planning and uptime SLAs for all DBIP segments, audited under DESA MRV standards.
- **Education:** Protects school connectivity during fibre cuts or power outages through satellite backup and edge caching.
- **Markets:** Maintains operational continuity for SMEs and financial services during regional disruptions, safeguarding economic activity.
- **Social Equity:** Ensures rural and vulnerable communities retain access to essential services during crises, reinforcing DESA's equity mandate.

Illustrative Table — Resilience Measures by Layer

Layer	Resilience Mechanism	Compliance Standard
Backbone	Dual fibre routes, ROADM mesh	ITU-T G.8080; DESA Circular
Access	Satellite failover for rural nodes	DESA Edge Resilience Protocol
Data Centres	Tier III redundancy, DR drills	NIST SP 800-34 / SP 800-184

Alignment Table — DBIP Objectives vs. Continental and Global Agendas

DBIP Objective	Agenda 2063	Agenda 2074	AfDB High 5
Universal & Affordable Connectivity	Goal 10: World-class infrastructure	SGG: Digital Equity	Improve Quality of Life
Sovereign Backbone & Open Access	Aspiration 2: Integration	SGG: Governance & Transparency	Integrate Africa
Tier III Data Centres & Edge	Aspiration 1: Prosperity	SGG: Ethical Tech	Industrialise Africa
Resilience & Continuity	Aspiration 3: Good Governance	SGG: Social Protection	Light up & Power Africa

3.6 Core Objective 5 — Affordability-Linked Governance and Tariff Regulation

The fifth strategic objective is to institutionalise affordability as a legal and operational standard, ensuring that broadband pricing remains socially inclusive and aligned with global benchmarks. DBIP enforces tariff regulation through DESA Operating Circulars, mandating wholesale price caps, retail affordability covenants, and targeted subsidies funded by Universal Service Funds (USFs).

Narrative Impact:

- **Governance:** Embeds affordability into statutory instruments, preventing market distortion and monopolistic pricing.
- **Education:** Guarantees predictable, low-cost connectivity for schools, enabling sustainable digital learning budgets.
- **Markets:** Reduces barriers for SMEs and startups by stabilising connectivity costs, fostering innovation and competitiveness.
- **Social Equity:** Protects vulnerable households through lifeline tariffs and voucher schemes, ensuring equitable access across income quintiles.

Illustrative Table — Affordability Governance Framework

Mechanism	Description	Compliance Instrument
Wholesale price cap	Limits cost at passive/active layers	DESA Tariff Circular
Retail affordability covenant	≤ 2% GNI per capita; USD 5/month target	DESA Pricing Directive
Lifeline tariff	Subsidised rural/low-income access	USF Disbursement Protocol

3.7 Core Objective 6 — Innovation Ecosystem and Service Portals

The sixth objective is to activate a multi-provider innovation ecosystem through DESA service portals, enabling EUSL members and authorised partners to offer OTT services (e.g., Spotify, EdTech platforms, fintech applications) over DBIP's open-access infrastructure. This replicates Sweden's Open Broadband Community model, which catalysed service diversity and consumer choice by separating infrastructure from retail service provision.

Narrative Impact:

- **Governance:** Creates a transparent, non-discriminatory marketplace for digital services under DESA oversight.
- **Education:** Facilitates integration of e-learning platforms and digital libraries into the national connectivity fabric.
- **Markets:** Stimulates local content creation and digital entrepreneurship by lowering entry barriers for service providers.
- **Social Equity:** Expands consumer choice and cultural access, ensuring rural communities benefit from the same service diversity as urban areas.

Table — Service Portal Structure and Benefits

Portal Layer	Function	Benefit
DESA Core Portal	Registers providers; enforces compliance	Guarantees neutrality and transparency
EUSL Member Portal	Hosts OTT services (e.g., music, EdTech)	Drives innovation and local content
Consumer Access Interface	Single sign-on for multi-service access	Simplifies user experience; promotes inclusion

Quantitative Targets (Illustrative for National Deployment)

Indicator	Year 1	Year 5	Year 10
Households connected	250,000	1,000,000	3,500,000
Schools connected	5,000	20,000	50,000
SMEs onboarded	10,000	50,000	150,000
OTT services registered	50	200	500

3.8 Consolidated Strategic Alignment Narrative

The strategic objectives of DBIP collectively establish a governance and infrastructure framework that transforms broadband from a private utility into a sovereign, equity-driven public infrastructure. By embedding affordability covenants, open-access neutrality, and resilience protocols into law and operational practice, DBIP ensures that connectivity becomes a guaranteed right rather than a discretionary service.

This alignment is not incidental; it is deliberate and multi-layered:

- **Agenda 2063**: DBIP operationalises Goal 10 (world-class infrastructure) and Aspiration 2 (continental integration) by creating cross-border fibre corridors and neutral IXPs.
- **Agenda for Social Equity 2074**: DBIP enforces measurable social equity standards—affordability, inclusion, and transparency—through MRV dashboards and independent audits.
- **AfDB High 5**: DBIP contributes to *Light up and Power Africa* (digital infrastructure), *Integrate Africa* (regional connectivity), *Industrialise Africa* (cloud and data services), and *Improve Quality of Life* (education and health access).

The programme's design draws on proven international models—such as Sweden's Open Broadband Community—while adapting to African regulatory and socio-economic contexts. This ensures that DBIP is not only technically robust but also socially transformative.

3.9 KPI Mapping for Strategic Objectives

To translate objectives into measurable outcomes, DBIP defines KPI families aligned with DESA's MRV framework:

Strategic Objective	KPI Family	Illustrative KPI
Universal & Affordable Connectivity	Affordability	% of entry-level plans ≤ 2% GNI per capita
Sovereign Backbone & Open Access	Infrastructure	Km of fibre deployed; # of open-access nodes
Tier III Data Centres & Edge	Hosting	# of Tier III facilities operational; edge latency < 20 ms

Strategic Objective	KPI Family	Illustrative KPI
Resilience & Continuity	Uptime	Backbone availability ≥ 99.95%; DR drills executed
Affordability Governance	Compliance	# of tariff audits completed; USF disbursement ratio
Innovation Ecosystem	Service Diversity	# of OTT services onboarded; % rural service penetration

3.10 Sweden's Open-Access Success Metrics (Reference)

The Swedish model, which DBIP adapts, achieved near-universal gigabit penetration and significant price reductions through structural separation and wholesale neutrality. Key indicators include:

- **Coverage**: > 90% fibre penetration in municipalities adopting open-access frameworks.
- **Price Impact**: Retail broadband costs reduced by 30–40% compared to vertically integrated markets.
- **Service Diversity**: > 100 retail providers active on municipal networks, fostering competition and innovation.

These metrics validate DBIP's approach and provide a benchmark for African adaptation under DESA governance.

3.11 Closing Paragraph for Chapter 3

DBIP's strategic objectives form a coherent blueprint for inclusive digital transformation. They combine infrastructure sovereignty, affordability enforcement, resilience, and innovation activation into a single governance instrument. By embedding these objectives into DESA's legal and fiduciary architecture, DBIP ensures that broadband becomes a catalyst for education, markets, and social equity—aligned with continental agendas and global best practice, and fully auditable under DESA's MRV standards.

Chapter 4 — Implementation Framework

4.1 Purpose and Structure

The Implementation Framework operationalises DBIP's strategic objectives through a structured, phased approach that ensures technical robustness, governance compliance, and socio-economic impact. It is organised into three tiers—Infrastructure, Application, and Capacity—and sequenced across three phases: Initiation, Scale-Up, and Consolidation. This framework embeds fiduciary safeguards, ethical compliance, and harmonisation with regional standards, ensuring that DBIP functions as a sovereign, auditable, and inclusive broadband programme.

4.2 Three-Tier Model

Tier I — Infrastructure (Physical and Core Layer)

- **Components:** National fibre backbone, cross-border interconnection, satellite overlays for remote areas, Tier III data centres, municipal open-access networks.
- **Governance:** Infrastructure Charter mandates sovereign ownership of passive assets and neutrality in wholesale access.

- **Compliance:** ITU-T G.652/G.655 fibre standards; Tier III uptime certification; DESA Operating Circulars on open-access obligations.

Tier II — Application (Service Enablement Layer)

- **Components:** DESA service portals for OTT providers, wholesale APIs for EUSL members, caching and CDN integration, security overlays (encryption, lawful interception compliance).
- **Governance:** Operating Circulars enforce non-discriminatory service onboarding and algorithmic transparency for AI-driven applications.
- **Compliance:** GDPR and African Union Data Policy Framework for data handling; WCAG 2.2 for accessibility in consumer interfaces.

Tier III — Capacity (Human and Institutional Layer)

- **Components:** Programme Office with directorates for Infrastructure, Regulatory Affairs, Finance, and Community Engagement; training tracks for network engineers, tariff auditors, and portal administrators; certification pathways for compliance officers.
- **Governance:** DESA MRV protocols for KPI tracking; independent audit committees; grievance redress mechanisms integrated with AfDB IRM for financed components.

4.3 Sequencing Phases

Phase	Duration	Key Activities
Initiation	Months 0–12	Legal and regulatory mapping; backbone route design; USF structuring; pilot municipal networks; initial service portal deployment
Scale-Up	Months 12–36	Backbone build-out; Tier III data centre commissioning; wholesale onboarding of OTT providers; tariff enforcement; rural satellite activation
Consolidation	Months 36–60+	Regional harmonisation (COMESA, SADC, EAC); MRV dashboards live; independent audits; performance-linked refinancing; expansion of service diversity

4.4 Fiduciary Architecture and Financing Instruments

DBIP adopts a blended finance model combining concessional loans, PPP equity, and Universal Service Funds. It integrates with the DESA Technology & Innovation Fund (DTIF) as a ring-fenced vehicle for backbone, data centre, and portal development. Financing instruments include:

- Viability-gap grants for rural last-mile builds.
- Performance-based grants for affordability compliance and open-access neutrality.
- Subordinated debt and guarantees for PPP risk mitigation.
  Tariff safeguards enforce USD 5/month for 100 Mbps unlimited in urban markets and subsidised rural lifeline tariffs, benchmarked to ≤ 2% GNI per capita affordability standards.

4.5 Compliance and Ethics
DBIP enforces lawful processing and privacy safeguards under GDPR and the African Union Data Policy Framework, algorithmic transparency for AI-driven services, and accessibility compliance (WCAG 2.2). Grievance redress mechanisms operate through DESA's internal complaint system and escalate to AfDB's Independent Recourse Mechanism for financed components. Annual independent audits verify compliance with tariff covenants, open-access obligations, and MRV standards.

4.6 Regional Replication and Integration
DBIP harmonises with COMESA, SADC, and EAC connectivity strategies by adopting shared standards for open-access wholesale, affordability benchmarks, and cross-border interconnection. Knowledge platforms and regional IXPs are integrated to enable roaming, content peering, and regulatory convergence.

4.7 Programme Benefits and Economic Rationale
DBIP is projected to deliver:

- **Employment:** Thousands of jobs in fibre deployment, data centre operations, and portal administration.
- **Cost Savings:** Reduction of retail broadband tariffs by 30–40% compared to vertically integrated markets.
- **Service Efficiency:** Improved uptime and latency for education, health, and SME services.
- **Competitiveness:** Enhanced digital readiness for national economies, attracting OTT providers and fintech innovators.

4.8 Measurement, Reporting, and Verification (MRV)
DBIP defines KPI families for affordability, uptime, service diversity, and compliance. Reporting cadence includes quarterly internal reviews, semi-annual public dashboards, and annual independent audits. KPIs include:

- % of entry-level plans ≤ 2% GNI per capita.
- Backbone availability ≥ 99.95%.
- Number of OTT services onboarded.
- Rural penetration ratio vs. urban baseline.

4.9 Stakeholder Engagement and Capacity Building
Engagement spans ministries (ICT, Finance, Education), regulators, academia, private sector, and civil society. Capacity-building tracks include:

- Network Engineering Certification (ITU-aligned).
- Tariff Audit and Compliance Training.
- Portal Administration and Consumer Protection Modules.

4.10 Participation and Partnership Framework
Participation is formalised through MoUs, Operating Circulars, and partner entry conditions. Calls to Action (CTAs):

- **Investors/DFIs:** Commit concessional tranches and guarantees under blended finance principles.
- **Technology Partners:** Co-develop portal APIs and caching systems; certify compliance with open-access and affordability standards.
- **OTT Providers:** Register services on DESA portals to expand consumer choice and cultural access.

4.11 Closing Statement for Chapter 4

The Implementation Framework transforms DBIP from a policy vision into an operational reality. By sequencing infrastructure, application, and capacity layers under a legally enforceable governance model, DBIP guarantees universal, affordable, and resilient connectivity. It positions broadband as a sovereign, ethical, and scalable public infrastructure aligned with Agenda 2063, Agenda 2074, and AfDB High 5 priorities.

Chapter 5 — Governance, Risk, and Safeguards

5.1 Purpose and Scope

This Chapter defines the governance architecture, risk taxonomy, and safeguard mechanisms that ensure DBIP operates as a lawful, ethical, and resilient programme. It establishes oversight bodies, compliance instruments, fiduciary controls, and grievance pathways, embedding transparency and accountability across all tiers of implementation.

5.2 Governance Architecture

Programme Office Structure

DBIP governance is exercised through a Programme Office comprising:

- **Directorate of Infrastructure & Operations** — oversees backbone deployment, data centre commissioning, and municipal network integration.
- **Directorate of Regulatory Affairs & Compliance** — enforces open-access obligations, tariff covenants, and data protection standards.
- **Directorate of Finance & Fiduciary Oversight** — manages blended finance instruments, USF disbursements, and PPP compliance.
- **Directorate of Community Engagement & Service Portals** — administers OTT onboarding, consumer protection, and grievance redress.

Oversight Bodies

- **DBIP Steering Committee** — strategic decision-making, chaired by DESA Central Unit.
- **Independent Audit & Ethics Board** — annual audits of tariff compliance, open-access neutrality, and MRV integrity.
- **Regulatory Liaison Unit** — harmonises DBIP standards with COMESA, SADC, and EAC frameworks.

Reporting Lines

Programme Office reports quarterly to DESA Central Governance Board; audit findings escalate to AfDB and national regulators for financed components.

5.3 Risk Taxonomy and Control Framework

Risk Families

Risk Category	Examples	Control Instruments
Infrastructure Risks	Fibre cuts, power outages, data centre cooling failures	Redundant routes, Tier III standards, DR drills
Fiduciary Risks	PPP cost overruns, tariff non-compliance	Blended finance covenants, independent audits
Data Protection Risks	Unlawful processing, breach of lawful basis	GDPR/AU Data Policy compliance, DPIAs
Algorithmic Risks	Bias in AI-driven portals, opaque service ranking	OECD AI principles, transparency modules
Accessibility Risks	Non-conformance with WCAG 2.2	Accessibility audits, remediation plans

5.4 Safeguards and Compliance Instruments

- **Legal Bases:** GDPR, African Union Data Policy Framework, national telecom statutes.
- **Open-Access Enforcement:** Operating Circulars mandating wholesale neutrality and non-discriminatory terms.
- **Affordability Compliance:** Tariff audits benchmarked to ≤ 2% GNI per capita; USF disbursement tracking.
- **Algorithmic Transparency:** Mandatory disclosure of AI logic for service portals; bias testing protocols.
- **Accessibility:** WCAG 2.2 AA conformance for all consumer interfaces.
- **Grievance Redress:** Multi-channel complaint intake; escalation to AfDB IRM for financed components.
- **Audit Obligations:** Annual independent audits covering fiduciary, technical, and social compliance.

5.5 Governance Instruments Table

Instrument	Purpose	Enforcement Body
DESA Infrastructure Charter	Sovereign ownership and neutrality	Programme Office

Instrument	Purpose	Enforcement Body
Operating Circulars	Open-access, tariff, and portal rules	Regulatory Affairs Directorate
PPP Framework	Risk-sharing and performance-linked payments	Finance Directorate
MRV Protocol	KPI tracking and public dashboards	Independent Audit Board

5.6 Closing Statement for Chapter 5

DBIP's governance and safeguard architecture ensures that the programme is not only technically sound but also legally enforceable and ethically compliant. By embedding fiduciary integrity, algorithmic transparency, and accessibility into its operational DNA, DBIP guarantees trust, resilience, and accountability—positioning broadband as a sovereign public infrastructure aligned with DESA's long-term vision and continental development agendas.

Chapter 6 — Technical Standards & Assurance Profiles

6.1 Purpose and Scope

This Chapter codifies the technical standards and assurance profiles governing DBIP's infrastructure, application, and capacity layers. It ensures interoperability, security, accessibility, and lawful compliance across all components, referencing globally recognised frameworks such as ITU-T, ISO/IEC, NIST, and WCAG. These standards provide the foundation for certification, audit, and presumption of conformity under DESA's MRV protocols.

6.2 Standards Stack by Layer

Layer	Applicable Standards	Assurance Objective
Fibre Backbone & Transport	ITU-T G.652/G.655 (optical fibre); ITU-T G.8080 (ROADM mesh); IEEE 802.3 (Ethernet)	High-capacity, low-latency transport; optical integrity
Data Centres	ISO/IEC 27001 (ISMS); ISO/IEC 22301 (BCMS); Uptime Institute Tier III	Security, continuity, and resilience
Access Networks	ITU-T G.984/G.987 (GPON/XG-PON); ETSI EN 301 549 (ICT accessibility)	Open-access neutrality; accessibility compliance
Service Portals & Applications	WCAG 2.2 AA; ISO/IEC 27701 (Privacy); GDPR; African Union Data Policy Framework	Inclusive design; lawful data processing
Cybersecurity & DevSecOps	NIST SP 800-218 (SSDF); NIST SP 800-53 Rev. 5; ISO/IEC 27002	Secure-by-design development; risk-based controls
AI Governance	EU AI Act (Arts. 10–15); OECD AI Principles	Transparency, robustness, and human oversight

6.3 Assurance Profiles

Baseline Assurance

- ISMS certification (ISO/IEC 27001) for data centres and portals.
- WCAG 2.2 AA conformance for all consumer interfaces.
- ITU-T compliance for backbone and GPON deployments.

Enhanced Assurance

- Independent audits of tariff compliance and open-access neutrality.
- Cybersecurity posture validated against NIST SP 800-53 control families.
- Privacy governance certified under ISO/IEC 27701.

Sovereign Assurance

- AI systems onboarded through DESA portals meet EU AI Act obligations (technical documentation, transparency, human oversight).
- Accessibility and inclusion verified through periodic audits and public dashboards.

6.4 Compliance Matrix

Component	Standard	Evidence Required
Fibre Backbone	ITU-T G.652/G.655	Optical test reports; route certification
Data Centres	ISO/IEC 27001; Tier III	ISMS certificate; uptime SLA logs
Service Portals	WCAG 2.2; GDPR	Accessibility audit; DPIA reports
OTT Onboarding	OECD AI; EU AI Act	Algorithmic transparency statements
DevSecOps	NIST SSDF	Secure coding attestations; SBOMs

6.5 Closing Statement for Chapter 6

By embedding ITU, ISO/IEC, NIST, and WCAG standards into DBIP's technical architecture, the programme guarantees interoperability, security, and inclusivity. These assurance profiles enable independent audits and presumption of conformity, reinforcing DBIP's position as a sovereign, ethical, and scalable broadband infrastructure aligned with DESA's compliance mandate and global best practice.

Chapter 7 — Operational Security & Incident Response

7.1 Purpose and Scope

This Chapter establishes DBIP's operational security doctrine and incident response lifecycle, ensuring resilience against cyber threats, service disruptions, and data breaches. It integrates NIST SP 800-61

Rev. 3 guidance for incident handling, ISO/IEC 27035 principles for structured response, and DESA's MRV protocols for transparency and accountability.

7.2 Incident Response Governance

DBIP maintains a dedicated Computer Security Incident Response Team (CSIRT) under the Directorate of Infrastructure & Operations, with authority to coordinate across backbone, data centres, and service portals. Roles and responsibilities are codified in Operating Circulars, ensuring clear escalation paths and compliance with national CERT frameworks.

Governance Instruments:

- **Incident Response Policy** — aligns with NIST SP 800-61 lifecycle (Preparation, Detection & Analysis, Containment, Eradication, Recovery, Post-Incident).
- **ISO/IEC 27035** — defines principles for incident classification, triage, and evidence preservation.
- **AfDB IRM Integration** — escalates grievances for financed components to AfDB's Independent Recourse Mechanism.

7.3 Risk Scenarios and Preparedness

Risk Scenario	Impact	Mitigation
Fibre cut or power outage	Service disruption	Dual routes, ROADM mesh, Tier III redundancy
Ransomware attack on data centre	Data loss, downtime	Immutable backups, offline restore, NIST SP 800-184 recovery
Portal compromise	Consumer data breach	MFA, zero-trust, DPIA, GDPR compliance
DDoS on backbone	Network congestion	Scrubbing centres, rate-limiting, upstream filtering

7.4 Lifecycle and Procedures

Preparation:

- Incident playbooks for backbone, data centres, and portals.
- Secure logging and immutable audit trails.

Detection & Analysis:

- SIEM monitoring with ATT&CK-based detection use cases.
- Automated alerts for anomalies in traffic and access patterns.

Containment & Eradication:

- Isolation of affected nodes; rollback to clean configurations.

- Malware eradication and patching under controlled conditions.

Recovery:

- Service restoration using pre-approved DR plans (NIST SP 800-184).
- Validation of data integrity and SLA compliance.

Post-Incident:

- Lessons learned documented; corrective actions tracked in MRV dashboards.

7.5 Vulnerability Disclosure and Coordination

DBIP enforces ISO/IEC 29147 for vulnerability disclosure and ISO/IEC 30111 for handling processes. OTT providers onboarded via DESA portals must adhere to coordinated disclosure timelines and remediation SLAs. Public advisories are issued through authorised channels with clear remediation guidance.

7.6 Metrics and MRV

Key KPIs include:

- Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
- % of incidents resolved within SLA.
- of vulnerability advisories published and closed.
- Compliance with GDPR breach notification timelines (≤ 72 hours).

Quarterly reports feed into DESA governance; anonymised statistics appear on public dashboards to reinforce transparency.

7.7 Closing Statement for Chapter 7

DBIP's operational security and incident response framework ensures lawful, resilient, and auditable handling of cyber threats and service disruptions. By embedding NIST and ISO standards into its lifecycle and integrating MRV for transparency, DBIP safeguards critical infrastructure and consumer trust—reinforcing its role as a sovereign, ethical, and scalable broadband programme.

Chapter 8 — Data Governance & DPIA Execution

8.1 Purpose and Scope

This Chapter establishes DBIP's data governance framework and the mandatory execution of Data Protection Impact Assessments (DPIAs) for all processing activities likely to present high risks to individuals' rights and freedoms. It integrates GDPR Articles 5, 6, and 35, the African Union Data Policy Framework, and EU AI Act Article 10 for high-risk AI systems onboarded through DESA service portals. The framework ensures lawful processing, algorithmic transparency, and accessibility compliance, embedding privacy-by-design principles into DBIP's operational architecture.

8.2 Data Governance Principles

DBIP enforces the following principles across all infrastructure and service layers:

- **Lawfulness, Fairness, and Transparency:** All processing activities must have a documented lawful basis and provide clear information to data subjects.

- **Purpose Limitation and Minimisation:** Data collected for connectivity, billing, or service onboarding must be limited to what is strictly necessary.
- **Integrity and Confidentiality:** Encryption, access controls, and immutable logging are mandatory for backbone, data centres, and portals.
- **Accountability:** Operators and OTT providers must maintain auditable records of processing activities and DPIA outcomes.

8.3 DPIA Mandate and Triggers

A DPIA is **compulsory** for:

- Large-scale processing of personal data (e.g., subscriber databases).
- AI-driven service portals involving profiling or automated decision-making.
- Cross-border data transfers between IXPs and regional nodes.

Legal Basis: GDPR Article 35 and AU Data Policy Framework provisions on risk-based assessments.

8.4 DPIA Content Requirements

Each DPIA must include:

Section	Description
Processing Description	Nature, scope, context, and purposes of processing
Lawful Basis	Contractual necessity, consent, or legitimate interest
Risk Assessment	Likelihood and severity of harm to data subjects
Safeguards	Technical and organisational measures (encryption, access control, anonymisation)
Residual Risk and Consultation	Prior consultation with supervisory authority if high risk remains

8.5 AI-Specific Governance (EU AI Act Article 10)

For high-risk AI systems onboarded via DBIP portals:

- **Data Governance Plan:** Document dataset origin, preparation, and bias mitigation measures.
- **Quality and Representativeness:** Ensure datasets are relevant, complete, and statistically appropriate for intended use.
- **Bias Detection:** Implement periodic bias testing and corrective actions.
- **Exceptional Processing of Special Categories:** Allowed only for bias correction under strict safeguards and deletion post-correction.

8.6 Governance Artefacts and Evidence

DBIP maintains:

- **Records of Processing Activities (RoP)** for all data flows.
- **DPIA Reports** for high-risk processing and AI onboarding.
- **Privacy Information Management System (PIMS)** aligned with ISO/IEC 27701 for accountability and audit readiness.

8.7 MRV and Reporting Cadence

KPIs include:

- % of DPIAs completed before go-live.
- Number of AI systems with documented bias mitigation plans.
- Accessibility compliance rate (WCAG 2.2 AA).
  Reporting cadence: quarterly internal reviews, annual independent audits, and public dashboards summarising DPIA coverage and compliance metrics.

8.8 Closing Statement for Chapter 8

DBIP's data governance and DPIA framework ensures lawful, ethical, and transparent handling of personal and algorithmic data. By embedding GDPR, AU Data Policy, and EU AI Act obligations into operational practice, DBIP safeguards individual rights while enabling innovation—reinforcing its role as a sovereign, compliant, and socially responsible broadband programme.

Chapter 9 — Technology Operations & Secure DevSecOps

9.1 Purpose and Scope

This Chapter defines DBIP's operational technology framework and secure development lifecycle, ensuring that all infrastructure and service components are engineered under secure-by-design principles. It codifies requirements for DevSecOps, software supply-chain integrity, and continuous assurance, referencing global standards such as NIST SP 800-218 (SSDF), ISO/IEC 27001, OWASP ASVS, and SLSA for build provenance.

9.2 Secure-by-Design Mandate

DBIP enforces **secure-by-design** as a compulsory principle across all technology layers. This includes:

- **Infrastructure as Code (IaC):** Automated provisioning with security controls embedded in templates.
- **Policy as Code:** Enforcement of access, encryption, and compliance rules within CI/CD pipelines.
- **Immutable Logging:** Tamper-evident audit trails for all operational events.

Governance Instrument: DESA Operating Circular on Secure Development and Deployment.

9.3 DevSecOps Architecture

DBIP adopts a **continuous integration and delivery (CI/CD)** model with integrated security gates:

- **Static and Dynamic Analysis:** Mandatory SAST/DAST scans for all code before deployment.
- **Container Security:** Image signing and vulnerability scanning for Kubernetes-based workloads.

- **Secrets Management:** Encrypted vaults and rotation policies for credentials and API keys.

Reference Standards:

- **NIST SP 800-218 (SSDF)** — Secure software development practices.
- **OWASP ASVS v5** — Application security verification requirements.

9.4 Software Supply-Chain Integrity

DBIP mandates Software Bill of Materials (SBOM) for all components, following NTIA Minimum Elements and open standards such as SPDX and CycloneDX.

- **Build Provenance:** Enforced through **SLSA Level 3**, requiring signed attestations and hardened build environments.
- **Third-Party Components:** Verified against vulnerability databases; onboarding contingent on compliance with SBOM and SLSA requirements.

Table — Supply-Chain Assurance Framework

Requirement	Standard	Evidence
SBOM	SPDX / CycloneDX	Machine-readable SBOM file
Build Integrity	SLSA Level 3	Signed provenance attestation
Vulnerability Disclosure	ISO/IEC 29147	Coordinated disclosure policy

9.5 OTT Service Portal Security

All OTT providers onboarded via DESA portals must:

- Implement **OAuth 2.0 / OpenID Connect** for secure authentication.
- Provide **algorithmic transparency statements** for AI-driven services.
- Comply with **GDPR** and **AU Data Policy Framework** for lawful data processing.

9.6 MRV and Assurance Metrics

KPIs include:

- % of releases with SBOM and signed provenance.
- Number of vulnerabilities remediated within SLA.
- Compliance rate with WCAG 2.2 AA for consumer-facing portals.
- Secure coding attestations verified against SSDF.

Reporting cadence: quarterly internal reviews, annual independent audits, and public dashboards summarising compliance metrics.

9.7 Closing Statement for Chapter 9

DBIP's technology operations framework embeds security, transparency, and resilience into every stage of deployment. By enforcing secure-by-design principles, SBOM requirements, and supply-chain integrity standards, DBIP ensures that its infrastructure and service portals remain trustworthy, auditable, and aligned with DESA's ethical and fiduciary mandates.

Chapter 10 — Transparency, Communications, and Public Reporting

10.1 Purpose and Scope

This Chapter establishes DBIP's transparency and communications framework, ensuring lawful disclosure to stakeholders, compliance with privacy and AI transparency obligations, and public accountability through structured reporting. It integrates GDPR Articles 13–14, Articles 33–34 for breach notifications, EU AI Act Articles 13 and 50, and DESA's MRV protocols for open dashboards and independent audits.

10.2 Transparency Principles

DBIP adopts the OECD openness and accountability principles, requiring proactive disclosure of policies, tariffs, and service conditions. All consumer-facing portals must provide clear, accessible information on data processing, pricing, and service diversity.

10.3 Privacy Notices and Data Subject Information

Under **GDPR Articles 13 and 14**, DBIP ensures:

- **At Collection:** Identity of controller, lawful basis, purposes, retention periods, rights of data subjects, and existence of automated decision-making.
- **Indirect Collection:** Source of data, categories processed, and safeguards for cross-border transfers.

  Privacy notices are published on DESA portals and updated in line with regulatory changes.

10.4 AI Transparency Obligations

For high-risk AI systems onboarded via DBIP portals:

- **Article 13 (EU AI Act):** Deployers receive clear instructions on intended purpose, accuracy metrics, performance conditions, and human oversight measures.
- **Article 50:** AI systems interacting with natural persons must disclose their nature; synthetic content (audio, video, text) must be labelled as artificially generated or manipulated.

10.5 Breach Notification and Incident Communications

- **Supervisory Authority:** Notify within 72 hours of awareness (GDPR Article 33).
- **Data Subjects:** Communicate breaches likely to result in high risk, using clear language and mitigation guidance (Article 34).

  Templates and escalation paths are codified in DBIP's Incident Response Policy (Chapter 7).

10.6 Vulnerability Disclosure and Security Advisories

DBIP enforces **ISO/IEC 29147** for coordinated vulnerability disclosure. OTT providers must adhere to remediation SLAs and publish advisories through DESA-authorised channels.

10.7 Public Reporting and MRV

DBIP issues semi-annual transparency reports covering:

- Tariff compliance and affordability metrics.
- Breach statistics and remediation timelines.
- OTT onboarding and service diversity indicators.
- Accessibility audits (WCAG 2.2 AA compliance).

Public dashboards display anonymised KPIs, reinforcing trust and accountability.

10.8 Closing Statement for Chapter 10

DBIP's transparency and communications framework transforms compliance into a public trust instrument. By embedding GDPR and AI Act obligations, breach protocols, and MRV-driven reporting, DBIP guarantees openness, accountability, and lawful governance—positioning broadband as a sovereign, ethical, and socially inclusive infrastructure.

Chapter 11 — Operations Security & Resilience (Business Continuity and Disaster Recovery)

11.1 Purpose and Scope

This Chapter defines DBIP's resilience architecture, ensuring uninterrupted connectivity for critical services during disruptions. It integrates NIST SP 800-34 Rev. 1 for contingency planning and SP 800-184 for cybersecurity event recovery, embedding redundancy and disaster recovery (DR) protocols across backbone, data centres, and municipal networks.

11.2 Continuity Governance

- **Programme Office Mandate:** Directorate of Infrastructure & Operations oversees BC/DR planning; independent audits validate readiness.
- **Plan Components:** Business Impact Analysis (BIA), recovery priorities, preventive controls, DR playbooks, and communication protocols.
- **Integration:** BC/DR plans align with DBIP's Incident Response lifecycle (Chapter 7) and MRV dashboards for transparency.

11.3 Resilience Measures by Layer

Layer	Mechanism	Compliance Standard
Backbone	Dual fibre routes, ROADM mesh	ITU-T G.8080
Data Centres	Tier III redundancy, immutable backups	ISO/IEC 22301
Access	Satellite failover for rural nodes	DESA Edge Resilience Protocol

11.4 Testing and Metrics

- **Exercises:** Annual table-top and full-interruption drills; ransomware and fibre-cut scenarios.

- **KPIs:**
    - Backbone availability ≥ 99.95%.
    - Recovery Time Objective (RTO) ≤ 4 hours for core services.
    - % of DR drills completed on schedule.

11.5 Closing Statement for Chapter 11

DBIP's resilience framework guarantees service continuity under stress, protecting education, governance, and market operations. By embedding NIST and ISO standards into BC/DR protocols, DBIP ensures lawful, auditable recovery and reinforces its role as a sovereign, ethical infrastructure.

Chapter 12 — Quantitative Data Usage Analysis (Fiber Optics Justification)

12.1 Purpose and Scope

This Chapter quantifies DBIP's projected data volumes to justify multi-terabit fibre backbone deployment. It translates busy-hour engineering into monthly and annual traffic estimates, demonstrating why fibre optics—and not legacy copper or wireless alone—are indispensable for national-scale connectivity.

12.2 Methodology

- **Busy-Hour Engineered Capacity:** 1.6 Tbps (including buffers and diversity).
- **Average Utilisation:** ~20% of BH (industry norm).
- **Conversion:**
    - 320 Gbps average load = 40 GB/s.
    - Per hour: 144 TB.
    - Per day: ~3.46 PB.
    - Per month: ~103 PB.
    - Per year: ~1.25 EB.

12.3 Visualisation Table — Monthly and Annual Volumes

Metric	Value
Busy-Hour Capacity	1.6 Tbps
Average Load	320 Gbps
Daily Volume	~3.46 PB
Monthly Volume	~103 PB

Metric	Value
Annual Volume	~1.25 EB

12.4 Why Volumes Are High

- **Cross-Sector Scope:** DBIP carries education, household streaming, SME traffic, and OTT services concurrently.
- **Education Standards:** ≥ 1 Mbps per student (FCC benchmark) drives large school-day peaks.
- **Streaming Adoption:** Netflix HD ~5 Mbps; 4K ~15 Mbps; YouTube Live up to 30 Mbps ingest.
- **Collaboration Traffic:** Zoom/Teams ~3–4 Mbps per participant for HD sessions.
- **Busy-Hour Engineering:** Designed for peak resilience, not average conditions.

Comparative Note: DESA Health Enablement Programme estimated ~64 PB/year because its scope is narrower (health facilities only). DBIP is a national backbone serving all sectors, hence volumes scale exponentially.

12.5 Growth Projection
With **25–30% CAGR** for busy-hour traffic:

- Year 1: ~1.25 EB/year.
- Year 5: ~4 EB/year.
- Year 10: ~10–12 EB/year.

This trajectory demands modular DWDM systems scalable to multi-terabit per fibre pair, with coherent 400G/800G upgrades and ROADM flexibility.

12.6 Closing Statement for Chapter 12
DBIP's projected volumes—**~**103 PB per month and 1.25 EB annually—validate the need for fibre optics as the sovereign backbone technology. Wireless and satellite cannot economically sustain these loads at required latency and reliability. Fibre ensures future-proof scalability, enabling DBIP to meet national and regional connectivity mandates for decades.

Closing Statement

The DESA Broadband & Infrastructure Program (DBIP) is a sovereign, ethical, and future-proof connectivity framework designed to transform broadband into a public-interest infrastructure. It integrates affordability covenants, open-access neutrality, and resilience protocols into a legally enforceable governance model, ensuring that connectivity becomes a guaranteed right rather than a discretionary service.

DBIP's architecture—anchored in a national fibre backbone, Tier III data centres, and municipal open-access networks—delivers universal, high-speed access at socially inclusive tariffs. By coupling tariff regulation with Universal Service Funds and blended finance instruments, DBIP enforces affordability benchmarks aligned with global standards (≤ 2% GNI per capita; USD 5/month for 100 Mbps unlimited). Its service portals activate a multi-provider innovation ecosystem, enabling EUSL members and OTT

platforms to deliver education, health, and cultural services directly to end-users, replicating the success of Sweden's Open Broadband Community model.

The programme's compliance framework embeds GDPR, AU Data Policy, and EU AI Act obligations, ensuring lawful data governance, algorithmic transparency, and accessibility (WCAG 2.2). Technical operations adopt secure-by-design principles, SBOM requirements, and supply-chain integrity standards (SLSA), while resilience is guaranteed through NIST-aligned business continuity and disaster recovery protocols.

Quantitative analysis confirms DBIP's strategic necessity: projected volumes of ~103 PB per month and 1.25 EB annually validate fibre optics as the only viable backbone technology for national-scale connectivity. These figures underscore DBIP's role as a catalyst for education, governance, and market activation—aligned with Agenda 2063, Agenda for Social Equity 2074, and AfDB High 5 priorities.

DBIP is not merely an infrastructure programme; it is a governance instrument for trust, transparency, and socio-economic inclusion. By embedding affordability, neutrality, and resilience into its operational DNA, DBIP positions itself as a cornerstone of DESA's long-term vision—a lawful, ethical, and scalable solution for Africa's digital future.