NATIONAL CLOUD TECHNICAL GUIDELINE

2026

Document Information

S/N	Data Element	Value
1	Title	National Cloud Technical Guideline 2026
2	Short Title	National Cloud Technical Guideline
3	Document Identifier	
4	Version	Version 1.0
5	Approval Date	4 August 2026
6	Effective Date	1 January 2027
7	Publisher	National Information Technology Development Agency (NITDA)
8	Document Type	Technical Guideline
9	Enforcement Status	Mandatory
10	Document Owner	National Information Technology Development Agency (NITDA)
11	Custodian	Regulations & Compliance Department
12	Target Audience	Federal Public Institutions (FPIs); State Governments; Cloud Service Providers; Data Centre Operators; Managed Service Providers; Service Integrators; ICT Service Providers; Government Contractors; Technology Vendors; Professional Bodies; Development Partners; and other organisations responsible for the design, deployment, operation, audit, or management of cloud infrastructure supporting public institutions.
13	Legal Authority	NITDA Act, 2007 and other applicable laws, regulations and government policies.
14	Related Documents	National Sovereign Cloud Policy; National Cloud Computing Guideline; National Data Classification & Localisation Framework; National Digital Infrastructure Assurance Framework.
15	Review Cycle	Every three (3) years or as required.
16	Language	English
17	Format	Electronic (PDF)
18	Subject	Cloud Architecture, Cloud Security, Technical Standards, Interoperability, Data Residency, Infrastructure Assurance and Cloud Service Management
19	Classification	Public
20	Copyright	

Table of Contents

1	This Guideline shall be described as '**National Cloud Technical Guideline, 2026**'.	**Long Title**
2	This Guideline may also be cited as 'National Cloud Technical Guideline'.	**Short Title**
3	This guideline provides the detailed technical and operational standards required to implement the National Cloud Computing Guideline (NCG). It serves as a practical guide for Federal Public Institutions (FPIs), Cloud Service Providers (CSPs), Service Integrators (SIs) and other stakeholders, outlining the mandatory requirements for procuring, deploying, and managing cloud services securely and efficiently. The Guideline covers procurement models, security operations, migration methodologies, and the compliance framework needed to ensure Nigeria's sovereign cloud ecosystem is resilient, interoperable, and aligned with global best practices.	**Explanatory Note**
4	In the exercise of the mandate conferred on it by Section 6 of the National Information Technology Development Agency Act, 2007, the National Information Technology Development Agency (NITDA), in compliance with the provisions of Section 32 of the NITDA Act, hereby issues the "National Cloud Technical Guideline".	**Authority**
5	This Guideline shall come into effect on 1 January 2027 or on such other date as may be determined by the Agency.	**Commencement**
6	This Technical Guideline establishes the minimum technical, security, operational, resilience, interoperability, and assurance requirements necessary to support the secure, reliable, and sustainable deployment, operation, and management of cloud services and supporting digital infrastructure in Nigeria. It translates the principles and policy objectives of the National Cloud Computing Guideline into practical technical requirements and implementation measures. The Guideline applies to all new and existing cloud services	**Application and Scope**

and supporting digital infrastructure used by Federal Public Institutions (FPIs), as well as to Cloud Service Providers (CSPs), Service Integrators (SIs), Data Centre Operators, Managed Service Providers, Artificial Intelligence Infrastructure Providers, Sovereign Compute Providers, and other Digital Infrastructure Providers operating or providing cloud-related services within Nigeria. It covers Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and other cloud deployment and service models recognised by NITDA.

Federal Public Institutions and regulated sector entities shall procure cloud services only from providers that comply with this Technical Guideline, while providers within scope shall comply with applicable technical and assurance requirements irrespective of whether they currently serve government and regulated sector workloads.

Governing Instruments

The technical standards and operational mandates within this Guideline are designed to ensure compliance with a unified set of national legal and regulatory frameworks. All FPIs, CSPs, and SIs must ensure their cloud procurement, deployment, and management activities adhere to the following key instruments and additional instruments that may be developed by NITDA:

I. The NITDA Act 2007 (the statutory basis for NITDA's regulatory authority)

II. The National Cloud Computing Guideline – the accompanying guideline

III. The Nigeria Data Protection Act (NDPA) 2023

IV. The Guidelines for Nigerian Content Development in ICT

V. The NITDA IT Project Clearance Regulation

VI. The Public Procurement Act

VII. The Cybercrimes (Amendment) Act 2024

7 The National Cloud Technical Guideline aims to provide a clear, unified, and enforceable set of standards for the deployment and operation of sovereign cloud infrastructure in Nigeria. **Objectives**

I. To Standardise Technical and Operational Requirements

This guideline establishes in-country data centre deployment standards aligned with national security, scalability, and sustainability requirements. It provides clarity on the technical specifications for project design and public tenders, covering physical infrastructure, network, compute, and storage. It also includes guidelines for energy-efficient design to reduce carbon footprint and operational costs.

II. To Define Best Practices for a Secure and Resilient Cloud Ecosystem

It defines best practices for cybersecurity, interoperability, and data portability across all cloud platforms. The guideline incorporates recognition of global security standards and defines clear metrics for availability, resilience, and disaster recovery to ensure the protection of government and regulated sector data and the continuity of digital services.

III. To Stimulate Investment and Local Innovation

By creating a clear and stable technical environment, the guideline aims to stimulate targeted investment and the development of compatible services for the Nigerian market. It provides a predictable framework that helps attract global hyperscalers while encouraging local partnerships and fostering a competitive market for Nigerian Cloud Service Providers (CSPs).

IV. To Establish a Unified Compliance Framework

The guideline develops a unified compliance and reporting framework for CSPs to ensure adherence to both national and international standards. This includes designing a template for periodic

infrastructure status reports and recommending monitoring tools, audit protocols, and certification pathways to enforce compliance effectively.

8 In this Guideline, unless the context otherwise requires, the following terms shall have the meanings assigned to them below: **Definitions**

Artificial Intelligence (AI) Infrastructure Provider means a provider of specialised computing infrastructure, platforms, or services used to support artificial intelligence workloads, including graphics processing units (GPUs), high-performance computing, model training, model inference, and related AI-enabled services.

Bureau of Public Procurement (BPP) means the primary public procurement regulator established under the Public Procurement Act, 2007.

Capital Expenditure (CapEx) means upfront investment in fixed IT assets or infrastructure, as opposed to operational subscription models.

Cloud First means a directive requiring Federal Public Institutions to prioritise cloud-based solutions over on-premises alternatives when procuring or deploying new information technology resources, unless there is a clear and documented justification.

Cloud Readiness Assessment means a structured evaluation of an FPI's ability to migrate to the cloud, covering security, legal, technical, operational, financial, and lifecycle considerations.

Cloud Service Provider (CSP) means an entity that provides cloud computing services, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), storage, or other cloud-based services, and is contractually responsible for the service levels and security of such services. A CSP may operate its own infrastructure or utilise contracted facilities or partners, including large-scale providers commonly

referred to as hyperscalers.

Data Breach means any confirmed or suspected incident resulting in the unauthorised access, disclosure, alteration, destruction, or loss of data processed under this Guideline.

Data Controller and **Data Processor** shall have the meanings assigned to them under the Nigeria Data Protection Act, 2023, whereby a controller determines the purpose and means of processing personal data and a processor acts on behalf of the controller.

Data Residency means the physical or geographical location where data or information is stored or processed.

Data Sharing Agreement (DSA) means a legally binding agreement between Federal Public Institutions governing the lawful basis, scope, security, and auditability of inter-agency data exchanges in accordance with the Nigerian e-Government Interoperability Framework (Ne-GIF).

Digital Regulatory Platform (DRP) means the digital platform established by the Agency for the administration of regulatory, registration, certification, licensing, assurance, compliance, monitoring, and other digital regulatory services, including such modules and services as the Agency may prescribe from time to time.

Federal Public Institution (FPI) means any Ministry, Department, Agency, or other public institution of the Federal Government of Nigeria, including any entity that processes government data or provides digital services under government mandate or contract.

Financial Operations (FinOps) means the principles, processes, and practices applied to cloud cost optimisation, including continuous monitoring, rightsizing, forecasting, and the use of cost-saving instruments.

Hybrid Cloud means a cloud deployment model that combines private and public cloud infrastructure, where sensitive data may be retained in private environments and other workloads hosted in public or community clouds.

Infrastructure-as-a-Service (IaaS) means a cloud service model that provides virtualised computing resources, including servers, storage, networking, and related infrastructure services.

Indigenous Cloud Service Provider or **Indigenous Service Integrator** means a CSP or SI incorporated in Nigeria and certified by NITDA as compliant with local content requirements as prescribed in the Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) 2019. Foreign CSPs may be granted provisional indigenous status under strategic investment rules. Any other CSP or SI that does not meet these criteria is considered a Foreign CSP or SI.

Latency and Access Benchmarks means nationally or internationally recognised standards for network speed, availability, and reliability required to ensure that government and regulated sector services hosted in the cloud remain accessible to end users.

Mutual Legal Assistance Treaty (MLAT) means an international agreement establishing lawful frameworks for cross-border government-to-government data access requests.

Nigeria Data Protection Act (NDPA), 2023 means the principal legislation governing personal data protection and cross-border data transfers in Nigeria.

Nigeria Data Protection Commission (NDPC) means the statutory body responsible for enforcing compliance with the Nigeria Data Protection Act, 2023.

Nigerian e-Government Interoperability Framework (Ne-GIF) means the federal framework for ensuring that government systems can securely exchange and utilise data across institutions.

National Information Technology Development Agency (NITDA) means the Agency established under the National Information Technology Development Agency Act, 2007 and the lead coordinating body for the implementation

of this Guideline.

Office of the National Security Adviser (ONSA) means the lead authority on matters of national security, including the management and protection of highly sensitive and classified government information.

Operational Expenditure (OpEx) means ongoing subscription-based, consumption-based, or pay-as-you-go information technology costs as opposed to upfront capital investments.

Platform-as-a-Service (PaaS) means a cloud service model that provides platforms and runtime environments for developing, testing, deploying, and managing applications.

Privacy Impact Assessment (PIA) or **Data Protection Impact Assessment (DPIA)** means assessments required under the Nigeria Data Protection Act, 2023 for systems or activities involving the processing of personal data.

Public-Private Partnership (PPP) means a contractual arrangement between the government and private entities for the financing, development, operation, or delivery of infrastructure or services.

Recovery Point Objective (RPO) means the maximum acceptable amount of data loss measured in time.

Recovery Time Objective (RTO) means the maximum acceptable period of downtime before services must be restored following a disruption.

Regulated Sector means any sector of the economy that is subject to the oversight, supervision, licensing, registration, or regulation of a competent statutory or regulatory authority established under any applicable law in Nigeria, including sectors designated as critical to national security, public safety, financial stability, public health, or the delivery of essential public services.

Role-Based Access Control (RBAC) means a security

principle whereby users are granted only those access rights necessary to perform their assigned responsibilities.

Service Integrator (SI) means a legal entity, including a company, partnership, or registered business name with the Nigerian Corporate Affairs Commission, or a consortium led by such an entity, that plans, designs, procures, implements, configures, supports, and manages cloud solutions for customers, often by integrating services from one or more CSPs. SIs are delivery and integration partners engaged within the aggregated framework agreements established under the National Cloud Computing Guideline and are provisioning entities for government and regulated sector services under this Guideline.

Service Level Agreement (SLA) means a contractual agreement specifying minimum service levels, security requirements, liabilities, penalties, and exit provisions between an FPI and its CSP or SI.

Shared Responsibility Model means the framework that delineates the respective responsibilities of cloud service providers, Federal Public Institutions, and service integrators for the security, management, and operation of cloud services.

Software-as-a-Service (SaaS) means a cloud service model in which software applications are delivered over the internet on a subscription or consumption basis.

Sovereign Cloud Governance Committee (SovGov) means the inter-agency and stakeholder advisory and coordination mechanism established to support the implementation of the National Cloud Computing Guideline and promote coordinated oversight of government and regulated sector cloud adoption.

Sovereign Compute Infrastructure means compute infrastructure designed, deployed, and operated to support sensitive, critical, artificial intelligence, high-performance computing, or strategic workloads in accordance with Nigerian jurisdictional, security, resilience, and data

governance requirements.

Strategic Investment Waiver means a temporary localisation waiver granted by NITDA, upon recommendation of the Sovereign Cloud Governance Committee, to a foreign CSP that commits to significant, verifiable, and time-bound investments in local cloud or data centre infrastructure.

Vendor Lock-in means a condition in which an FPI becomes dependent on a single provider and is unable to migrate to another provider without significant technical, contractual, operational, or financial barriers.

9 Procurement and Service Management

9.1 Sourcing Cloud Services

I. Entities may source services from public, private, or hybrid cloud models, depending on the data classification and business need. Procurement must prioritise local content and indigenous CSPs in line with the Guidelines for Nigerian Content Development in ICT.

II. The "Cloud First" directive requires a thorough evaluation of the best execution venue for each government workload, considering factors such as cost, performance, security, and data sovereignty. For predictable, long-term workloads, FPIs and their SIs must conduct a Total Cost of Ownership (TCO) analysis to determine if a managed private or hybrid cloud model offers better economic value and control than a purely public cloud solution.

9.2 Recognised Deployment Models and Standards

I. **Adherence to International and National Standards:** To ensure interoperability, security, and trust, all cloud services procured by FPIs must align with recognised international standards. This guideline mandates adherence to the following as a baseline:

a. ISO/IEC 17203: for workload portability and the prevention of vendor lock-in (Open Virtualisation Format).
b. ISO/IEC 27017: for a code of practice on information security controls for cloud services.
c. ISO/IEC 27018: for a code of practice on the protection of Personally Identifiable Information (PII) in public clouds.
d. ISO/IEC 19086: for a standardised framework on Cloud Service Level Agreements (SLAs).
e. Cloud Security Alliance (CSA) STAR Certification (Level 1 minimum).
f. Service Organisation Control (SOC) 2 Type II Attestation Report.

While adherence to these global standards is the ultimate goal for ensuring competitiveness and interoperability, this Guideline also strongly encourages the development of equivalent national standards. This approach is intended to build local expertise, foster a domestic certification ecosystem, and ensure that standards are precisely tailored to Nigeria's unique regulatory and operational context. Indigenous providers may demonstrate compliance through these recognised national standards as they become available.

II. **Cloud Service Models (IaaS, PaaS, SaaS, FaaS):** FPIs, working with SIs, shall select the cloud service model that best fits their specific technical requirements and operational needs. The following models are recognised by this Guideline:

a. **Infrastructure as a Service (IaaS):** For foundational compute, storage, and networking resources.

b. **Platform as a Service (PaaS):** For application development and deployment environments.

c. **Software as a Service (SaaS):** For pre-built,

ready-to-use software applications.

d. **Functions as a Service (FaaS) / Serverless:** For event-driven applications where infrastructure management is fully abstracted. The choice of service model must be based on a thorough analysis of the FPI's needs and guided by a fiscally responsible approach that optimises public expenditure. While public cloud (IaaS, PaaS) is suitable for workloads with variable demand, FPIs should consider managed private or hybrid cloud models for stable, high-utilisation applications, as these can offer significant cost savings and greater control over the long term. The Sovereign Cloud Governance Committee (SovGov) may advise NITDA on updated recommendations on the appropriate use of these models. Furthermore, NITDA may provide guidance to FPIs on the choice of model for specific projects as part of its routine IT project clearance process to ensure alignment with national strategic objectives.

III. **Deployment Model Use Cases:** FPIs, in consultation with their SIs, shall select a deployment model based on the data classification and specific use case. The following table provides the recognised models and their primary preferred applications:

Primary Use Case	Preferred Deployment Model	Remarks
Non-sensitive workloads and citizen-facing services (Level 1 & 2 Data).	**Public Cloud**	Providers must be certified and listed on the NITDA Digital Regulatory Platform.
Sensitive and classified government and regulated sector data (Level 3 & 4 Data).	**Private Cloud**	Must be hosted in-country, with a strong preference for indigenous CSPs.
Workloads requiring a mix of security levels or inter-agency integration.	**Hybrid Cloud**	Secure orchestration and data flow between environments is mandatory.
Shared services and platforms used by multiple FPIs.	**Community Cloud**	Must be hosted in-country and may be co-managed by the participating FPIs or a lead agency.

9.3 Technical Requirements for Service Level Agreements (SLAs)

I. **Availability and Support Requirements:** SLAs must meet the following minimum tiered availability and support requirements, which apply 24 hours a day, 7 days a week (24x7). The requirements are linked to the National Data Classification Framework:

a. For services hosting **Level 4 and Level 3 data:**

i. Minimum Availability (Uptime): **99.99%**

ii. Critical Incident Support Response Time: **< 15 minutes**

iii. Critical Incident Support Resolution Time: **< 4 hours**

b. For services hosting **Level 2 data:**
    i. Minimum Availability (Uptime): **99.95%**
    ii. Critical Incident Support Response Time: **< 1 hour**
    iii. Critical Incident Support Resolution Time: **< 8 hours**
c. For services hosting Level 1 data:
    i. Minimum Availability (Uptime): **99.9%**

II. Support Response Time: **< 4 business hours (during standard Nigerian working hours)**

III. Support Resolution Time: **Best effort, with a target of < 24 business hours**

IV. **Network Latency:** SLAs must also guarantee a reasonable network latency of between 50ms and 150ms for all services delivered between the CSP's in-country data centre and the end-user within Nigeria.

V. **Performance Monitoring and Reporting:** CSPs and SIs shall provide FPI governance officers with continuous access to performance monitoring dashboards covering availability, latency, and SLA compliance, with monthly summary reports submitted to the FPI's Accounting Officer.

VI. **Justifiable Variations to SLA Metrics**: The standards defined above are the mandatory default for all mission-critical and citizen-facing government and regulated sector services irrespective of data classification level. However, these network latency and support requirements can be adjusted on a case-by-case basis if a compelling justification is provided in the solution's design. This flexibility is intended for non-critical, internal, or back-office applications where high availability and low latency are demonstrably not essential for the service's primary function. FPIs must formally acknowledge that any decision to procure services with relaxed SLAs will

directly impact user experience and may conflict with the government's commitment to service delivery excellence, as outlined in frameworks like SERVICOM. Therefore, any justification for lower SLA targets must include an impact assessment on citizen satisfaction and overall service quality.

9.4 Service Offerings from Pre-approved Cloud Service Providers

I. **Market-Driven Approach:** To simplify procurement for FPIs, this Guideline encourages a market-driven approach to service offerings while maintaining rigorous oversight. The **Digital Regulatory Platform**, managed by NITDA, will serve as the authoritative directory of certified Cloud Service Providers (CSPs) and Service Integrators (SIs) eligible to provide services to the government and regulated sectors.

II. **Service Bundles and the Digital Regulatory Platform:** Instead of NITDA pre-approving specific service bundles, certified Cloud Service Providers (CSPs) and Service Integrators (SIs) are encouraged to create and prominently display service bundles on their own websites and product pages. These bundles should be pre-configured to meet the tiered security, availability, and compliance requirements outlined in this Guideline.

III. **Audit and Delisting of Service Bundles:** The Digital Regulatory Platform will provide direct links to these offerings on the certified providers' sites. While providers are responsible for creating these bundles, they must ensure that all components and services within a marketed bundle are fully compliant with the standards herein. NITDA reserves the right to audit these offerings and can delist any bundle that fails to meet the required standards.

10 10.1 Cybersecurity Standards and Controls

Security and Resilience Operations

I. Cloud environments supporting government and regulated sector workloads shall adopt a Zero Trust Architecture (ZTA) approach. This principle assumes that no user or device is trusted by default, requiring continuous verification for every access request.

II. Providers supporting government and regulated sector workloads shall establish, implement, maintain, and continually improve an Information Security Management System (ISMS) aligned with ISO/IEC 27001 or any other standard recognised by NITDA. Providers shall also align with the NITDA Information Security Management System Guideline for Federal Public Institutions and any successor instruments issued by the Agency.

III. Encryption for data at rest and in transit must utilise **AES-256 encryption or higher**.

IV. Annual, independent **third-party penetration testing** is mandatory for all CSP and SI infrastructure hosting government and regulated sector data. **Continuous automated vulnerability scanning** must be operational for all internet-facing systems.

V. A **Web Application Firewall (WAF)** must be deployed and properly configured to protect all public-facing government and regulated sector web applications and APIs.

VI. Risk assessments shall be conducted periodically and shall include operational, cybersecurity, concentration, systemic, cloud dependency, supply chain, outsourcing, and exit risks, proportionate to the criticality of the workload, service, or digital

infrastructure.

VII. Providers shall establish supply chain risk management measures covering hardware, software, firmware, cloud services, managed services, and third-party dependencies that may affect the security, resilience, or integrity of government and regulated sector workloads.

VIII. Security operations capabilities required under this Guideline may be delivered internally, through shared government services, or through accredited managed service providers, provided that accountability, reporting, and compliance obligations remain clearly assigned.

10.2 Cloud Governance and Access Management Protocols

I. **Foundational Access Controls:** Access must be governed by Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) to ensure only authorised personnel can access sensitive government data. Multi-Factor Authentication (MFA) must, at a minimum, utilise Time-based One-Time Password (TOTP) applications. For access to environments hosting Level 3 or 4 data, the use of FIDO2-compliant hardware security keys is mandatory.

II. **Network and Location-Based Access Controls:** Access to cloud services hosting Level 2 data and above shall, by default, utilise location-aware and risk-based access controls. Such controls may include restrictions to approved Nigerian IP address ranges, device-based authentication, geofencing, secure VPN access, or other compensating controls approved by the respective FPI. Exceptions for legitimate international access (e.g., for diplomatic missions, travelling officials, or approved

international partners) must be formally justified, time-bound, and approved through a documented risk assessment process managed by the respective FPI.

III. **Privileged Access Management:** All privileged administrative access to the cloud environment must be managed through a Privileged Access Management (PAM) solution. This system must enforce ephemeral access (just-in-time), session recording, and a detailed, immutable audit log of all privileged actions.

10.3 Incident Reporting Procedures

I. **Immediate Reporting Obligation:** In accordance with the Shared Responsibility Model, the Federal Public Institution (FPI) holds ultimate accountability for its data. However, the operational duty to report rests with the service providers. Therefore, any data breach or significant security incident impacting government and regulated sector data or cloud infrastructure must be reported upon discovery. This obligation falls upon the contracted Service Integrator (SI) and the underlying Cloud Service Provider (CSP).

II. **Reporting Timeline and Recipients:** Upon a verified incident, the responsible SI or CSP shall provide immediate notification to:

a. The affected FPI.

b. The Nigeria Data Protection Commission (NDPC), in the case of personal data breaches, and any relevant sector regulator where the affected service or data falls within a regulated sector.

c. The National Information Technology Development Agency (NITDA), as the lead

coordinating body for this Guideline.

This notification must be made without undue delay and, in any case, **not later than 72 hours** after becoming aware of a verified incident, as mandated by the Nigeria Data Protection Act (NDPA) 2023. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the FPI must ensure the affected data subjects are notified immediately. For breaches of personal data, the 72-hour timeline is mandated by NDPA 2023. For breaches of non-personal government and regulated sector data, the same 72-hour timeline shall apply under this Guideline.

III. **Minimum Content of Breach Notification:** The initial notification report submitted to the NDPC and NITDA must, at a minimum, contain the following information as stipulated in the NDPA General Application and Implementation Directive (GAID):

a. A description of the circumstances and nature of the breach, including the data categories and approximate number of data subjects and personal data records concerned.
b. The date or time period during which the breach occurred.
c. An assessment of the likely risk of harm to individuals.
d. A description of the measures taken or proposed to be taken to address the breach and mitigate its adverse effects.
e. The name and contact information of the designated Data Protection Officer (DPO) or other relevant contact person who can provide further information.

IV. **Incident Logging and Cooperation:** CSPs and SIs must maintain comprehensive logs and detailed reports of all security incidents, not limited to verified

incidents. These records must document the timeline of events, the findings of internal investigations, and all remedial actions taken. These incident logs and reports are critical for forensic analysis and must be made available to national law enforcement and security agencies upon lawful request. CSPs and SIs are required to provide full cooperation to support investigations, national security efforts, and the overall strategic goal of enhancing Nigeria's cybersecurity resilience.

V. **Definitions**: For the purpose of this section, 'Discovery' is the initial identification of a potential security event. A 'Verified Incident' is an event confirmed, after triage, to be a security breach. The mandatory reporting timeline commences upon the confirmation of a 'Verified Incident'.

10.4 Backup and Disaster Recovery Requirements

I. **Vendor Transparency in Disaster Recovery and Backup:** Data centres hosting government and regulated sector information must implement comprehensive, tested, and documented disaster recovery (DR) plans to ensure business continuity and the resilience of public services. These plans must include geographically distributed backups and automated failover mechanisms to secondary sites. Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are mandatory components of all Service Level Agreements (SLAs). SIs are required to be aware of these capabilities and to verify them as part of their due diligence.

II. **Service Integrator (SI) Due Diligence:** The Service Integrator, in its capacity as the primary provisioning entity for the FPI, is required to conduct thorough due diligence on the DR capabilities disclosed by the CSP. The SI must ensure that the chosen CSP's services align with the specific RTO and RPO requirements mandated in the FPI's Service

Level Agreement (SLA). The SI's knowledge and management of these capabilities are critical components of its contractual obligation to the FPI.

III. **Audit and Certification Requirement:** As a mandatory component of NITDA's certification and annual recertification process, both CSPs and SIs must provide evidence of successful DR testing for the infrastructure hosting government and regulated sector data. This evidence may include recent third-party audit reports (e.g., SOC 2 reports covering availability) or documented results from a simulated live failover and recovery exercise. Failure to provide satisfactory proof of DR testing may result in the suspension or revocation of certification.

IV. **Guideline on Cross-Border Transfers for Backup and Disaster Recovery:** To uphold Nigeria's data sovereignty, this Guideline establishes a **"Nigeria-First"** principle for disaster recovery infrastructure. While fully acknowledging the convenience of utilising existing infrastructure outside the country to aid in fulfilling redundancy and resilience of cloud services, the objective of this Guideline is to build capacity within the country for all such services to be provided locally in the near term.

a. **Primary and Secondary Sites within Nigeria:** For data at Level 2 and above, both the primary production site and the secondary (failover) disaster recovery site **must be located within Nigeria's territorial boundaries**. This ensures that the first lines of data hosting and recovery reside locally, supporting the national interest.

The primary and secondary sites required under this provision shall be located in different geopolitical zones of the Federation, or at such distance as is necessary to ensure continuity in the event of localised disruption, in accordance with the geographic distribution requirements of

the National Sovereign Cloud Policy.

b. **Prohibition for High-Sensitivity Data:** Under no circumstances shall data classified as LEVEL 4 (Classified) or LEVEL 3 (High Sensitivity) be backed up or transferred outside of Nigeria. All copies, including archival and backup data, must remain within the country.
c. **Conditional Waivers for Tertiary Backups:** An exception for a *tertiary* (out-of-country) backup is permissible only for data classified as LEVEL 2 (Moderate Sensitivity) and LEVEL 1 (Limited Sensitivity), and only when all of the following stringent conditions are met:
    - **Demonstrable Need:** The FPI must provide a formal justification to NITDA demonstrating that in-country DR sites are insufficient to meet specific, heightened resilience or business continuity requirements that cannot otherwise be fulfilled.
    - **Compliance with the NDPA 2023:** Any cross-border transfer must be executed in strict accordance with the Nigeria Data Protection Act (NDPA) 2023. This requires the destination country to either have an **adequacy decision** from the Nigeria Data Protection Commission (NDPC) or for the transfer to be governed by an **approved protective instrument**, such as Standard Contractual Clauses (SCCs).
    - **Mandatory Encryption:** All data transferred and stored in a tertiary backup site outside Nigeria must be encrypted both in-transit and at-rest using security standards specified in the National Cloud Technical Guideline, 2026. The FPI or its SI must ensure that it retains full control over the encryption keys, which must be generated and managed from within Nigeria.

V. **NITDA Approval:** Before any such arrangement is made, the FPI or covered entity shall obtain explicit prior written approval from NITDA, supported by a documented risk assessment and justification demonstrating why the proposed arrangement is necessary. NITDA may consult relevant government institutions or sector regulators where necessary.

Any such arrangement shall follow the authorisation pathway in the National Cloud Computing Guideline and the National Sovereign Cloud Policy and remains limited to Level 1 workloads and NITDA approved Level 2 exceptions meeting the conditions of this Guideline, including encryption keys generated and managed within Nigeria.

VI. **Impact on Service Level Agreements (SLAs):** The restrictions on cross-border data transfers detailed in this section may impact the standard Service Level Agreements (SLAs), particularly the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) offered by global Cloud Service Providers (CSPs).

a. Therefore, NITDA is required to conduct a thorough assessment of these impacts during the transition phase of this Guideline's implementation. This assessment shall be performed in consultation with Federal Public Institutions (FPIs) and accredited CSPs to identify potential conflicts between the guideline's data residency requirements and the providers' global disaster recovery architectures.
b. Following the assessment, NITDA shall develop and issue guidance for FPIs on negotiating SLAs that align with this Guideline while still meeting their operational resilience requirements. This may include frameworks for risk acceptance or templates for customised SLA clauses.

10.5 Supply Chain Security Standard

The supply chain risk management measures established under section 10.1 shall be aligned with internationally recognised standards, including ISO/IEC 27036, NIST SP 800-161, or equivalent frameworks recognised by NITDA.

11 Technical Guidelines for Migration and Deployment

11.1 Pre-migration Assessment and Planning

FPIs must conduct a cloud readiness assessment, identify sources of value (efficiency, agility), and create a roadmap for migration. This phase must include a detailed Discovery and Dependency Mapping exercise to catalogue all applications, databases, network configurations, and their interdependencies. This prevents service disruptions caused by migrating an application without its required components. Applications must be classified to determine the appropriate migration strategy (e.g., rehost, refactor, re-platform, re-architect). This roadmap shall also include a formal **Rollback Plan**, detailing the procedures to revert to the legacy system in case of an unsuccessful migration.

11.2 Pilot Migration and Validation

Before a full-scale migration, the SI must execute a **Pilot Migration** involving a small, non-critical subset of the services slated for transition. The purpose of this pilot is to test the migration methodology, validate security controls in the target cloud environment, and confirm performance benchmarks. Learnings from this phase must be documented and used to refine the full migration plan, ensuring a more predictable and successful outcome.

11.3 Secure Migration Methodologies

Data migration must be secured using end-to-end encryption and secure transfer protocols (SSL/TLS, IPsec). Data integrity must be verified post-migration using hashing or checksums. Secure transfer protocols for data migration must be configured to use the latest secure versions, specifically **TLS 1.2 or higher**. All migration

activities must be logged in an **immutable audit trail** to ensure accountability and support forensic analysis if an incident occurs. Providers may align with internationally recognised interoperability standards and frameworks where such alignment is consistent with Nigerian laws, supports trusted interoperability, preserves national jurisdictional control, promotes portability, and reduces vendor lock-in.

11.4 Post-deployment Validation and Optimisation

After migration, FPIs must validate application performance and data integrity against pre-defined success criteria established during the planning phase. Continuous monitoring of SLAs is required to ensure compliance and drive continuous improvement. Furthermore, the SI must implement a Continuous Optimisation and Cost Management (FinOps) process. This involves regularly analysing cloud usage, right-sizing resources (e.g., adjusting virtual machine sizes to match workload demands), and identifying cost-saving opportunities to ensure that the FPI's cloud expenditure is financially efficient.

11.5 Legacy Infrastructure Decommissioning

I. **Framework and Responsibility:** The secure and efficient decommissioning of legacy physical infrastructure is a mandatory final phase of any cloud migration project. While the FPI retains ultimate ownership of and accountability for its legacy assets, the contracted Service Integrator (SI) is responsible for planning, executing, and documenting the entire decommissioning process in accordance with this framework.

II. **Decommissioning Plan:** As part of the migration roadmap, the SI must submit a formal **Decommissioning Plan** to the FPI for approval. This plan must include, at a minimum:

   a. **Asset Inventory:** A comprehensive inventory

of all hardware to be decommissioned, including servers, storage arrays, and networking equipment.

b. **Data Destruction:** A detailed procedure for the secure and permanent sanitisation of all data from storage media. The process must align with internationally recognised standards such as **NIST SP 800-88 (Guidelines for Media Sanitisation)**. The SI must provide a formal **Certificate of Data Destruction** to the FPI for every storage device.

c. **Environmental Disposal:** A plan for the environmentally sound recycling or disposal of all hardware components, conducted through a government-certified e-waste management partner. The plan must adhere to all national environmental protection regulations.

d. **Asset Value Recovery:** A process for assessing the residual value of decommissioned assets. The SI shall manage the logistics of remarketing, reallocating, or repurposing viable equipment to "realise value" for the FPI.

e. **Chain of Custody:** A documented and auditable chain of custody that tracks each hardware asset from the point of shutdown to its final disposition (destruction, recycling, or resale).

III. **Final Verification:** Upon completion of the process, the SI must submit a Final Decommissioning Report to the FPI, which includes all asset tracking logs, Certificates of Data Destruction, and e-waste disposal receipts. This report serves as the official record of a securely completed migration project.

11.6 Sovereign Compute Infrastructure: Providers supporting AI, high-performance computing, or other advanced digital workloads for Federal Public Institutions shall implement appropriate controls for workload isolation,

access management, monitoring, resilience, data governance, and secure operation of compute environments.

Where AI infrastructure is used for government and regulated sector workloads, providers shall implement appropriate AI governance, AI risk management, security, monitoring, incident response, and auditability measures, including alignment with recognised AI governance standards where applicable.

Where appropriate, providers supporting AI workloads should align with internationally recognised AI governance standards, including ISO/IEC 42001 and applicable NITDA AI governance instruments.

12 Data Sovereignty Compliance

12.1 Technical Compliance Framework for FPIs

FPIs must use the national Data Classification Framework to categorise their data and ensure it is stored in a cloud environment that meets the required security and residency standards.

12.2 Service Integrator and CSP Reporting Requirements

CSPs and SIs must provide government entities and sector regulators with access to audit logs and compliance dashboards. A standardised infrastructure status report must be submitted to NITDA on a **quarterly basis**, using the template provided in Annex A of this Guideline. This report must capture metrics on location, tier certification, security posture, power, and disaster recovery test results.

12.3 Audit and Verification Procedures

NITDA and certified third parties will perform regular audits to validate contractually agreed controls. These audits will verify compliance with security, data handling, and localisation mandates.

12.4 Providers supporting regulated sector workloads or nationally significant digital services shall comply with the

applicable requirements of this Guideline and any additional sector-specific requirements lawfully issued by competent sector regulators. Such sector-specific requirements may prescribe higher or additional standards relating to data governance, data classification, data localisation, cybersecurity, operational resilience, supervisory access, or related matters, provided that they shall not diminish, derogate from, or prescribe standards lower than the minimum requirements established under this Guideline or any other regulatory instrument issued by NITDA.

13 Data Centre and Physical Infrastructure Standards

13.1 Minimum Tier Certification

The minimum technical standards in this section shall apply to data centres and digital infrastructure providers seeking NITDA certification, Digital Regulatory Platform onboarding, government and regulated sector recognition, or national digital infrastructure assurance status. All primary and secondary data centres hosting government and regulated sector data must be designed, constructed, and operated to a minimum auditable standard.

I. Facilities hosting Level 4 or Level 3 data must be deployed according to Uptime Institute Tier III or TIA-942 Rated-3 for both the design and the constructed facility.
II. Facilities hosting Level 2 data must, at a minimum, meet the requirements of Uptime Institute Tier II or TIA-942 Rated-2.

13.2 Power and Cooling Redundancy

I. Power infrastructure must provide a minimum of N+1 redundancy for all critical components, including UPS systems, power distribution units, and backup generators.
II. The data centre's Power Usage Effectiveness (PUE) must be reported to NITDA annually, with a target of

1.6 – 3.6 or lower range to ensure energy efficiency.

13.3 Physical Security Controls

I. Physical access to data halls must be governed by a multi-layered security model, requiring a minimum of three distinct authentication factors (e.g., key card, PIN code, biometric scan) for entry.

II. 24x7x365 on-site security personnel are mandatory. A comprehensive Closed-Circuit Television (CCTV) system must monitor all perimeter, entry, and critical interior zones, with footage retained for a minimum of 90 days.

13.4 NITDA shall establish and administer technical assessment, registration, certification, accreditation, and assurance programmes for Cloud Service Providers, Service Integrators, Data Centre Operators, Artificial Intelligence Infrastructure Providers, Digital Infrastructure Providers, and such other entities as the Agency may designate, in accordance with applicable laws, standards, guidelines, and other regulatory instruments issued by the Agency.

Such programmes shall be implemented through the National Digital Infrastructure Assurance Framework (NDIAF) and any associated operational manuals, standards, codes of practice, technical specifications, certification schemes, accreditation requirements, advisories, implementation guidelines, templates, or other instruments issued by NITDA. For implementation purposes, the instruments issued under the NDIAF shall govern and, to the extent of any inconsistency, prevail over any corresponding procedures, templates, or operational requirements contained in this Guideline.

Certified or registered providers shall maintain continuous compliance with the applicable requirements and promptly notify NITDA of any material changes that may affect their registration or certification status, including changes in ownership or control, infrastructure location, operational capability, security posture, international certifications,

data residency arrangements, significant third-party dependencies, or major cybersecurity incidents.

14 This Technical Guideline shall be reviewed every three (3) years or earlier as may be determined by NITDA to reflect technological developments, implementation experience, emerging risks, and changes in applicable standards or national priorities. **Review**

ANNEXES

To aid in the practical implementation of this Guideline, the following annexes form an integral part of this technical document:

- **Annex A:** Standardised Template for Quarterly Infrastructure Status Reports
- **Annex B:** Sample Service Level Agreement (SLA) Template
- **Annex C:** Government and Regulated Sector Risk Assessment and Threat Modelling Tool
- **Annex D:** Cloud Provider Accreditation Checklist
- **Annex E:** Standardised Incident Reporting Form
- **Annex F:** Disaster Recovery Test Attestation Form
- **Annex G:** FinOps and Cloud Cost Reporting Template
- **Annex H:** Framework for Evaluating Foreign CSP Strategic Investment

Annex A: Standardised Template for Quarterly Infrastructure Status Reports

Purpose: To establish a uniform and transparent reporting mechanism for CSPs and SIs, enabling NITDA and FPIs to consistently track the compliance, health, and performance of the cloud infrastructure hosting government and regulated sector data.

Quarterly Infrastructure Status Report

a. **Reporting Period**: [Q1, Q2, Q3, Q4] [YEAR]

b. **Provider (CSP/SI)**: [Provider Name]

FPI Client(s) Covered: **[List of FPIs]**

Metric	**Current Status**	**Notes / Changes Since Last Quarter**
Data Centre Location(s)	[e.g., Ikeja, Lagos; Maitama, Abuja]	[e.g., New availability zone added]
Tier Certification	[e.g., Uptime Institute Tier III - Constructed Facility]	[e.g., Recertification completed on DD/MM/YY]
Security Certifications	[e.g., ISO 27001, CSA STAR, SOC 2 Type II]	[e.g., ISO 27017 certification in progress]
Quarterly Uptime %	[e.g., 99.98%]	[Details of any downtime incidents]
Security Incidents	[Number of major/minor incidents]	[Brief, non-sensitive summary of incidents]
Power Usage Effectiveness (PUE)	[e.g., 1.58]	[e.g., Cooling system upgrade improved PUE]

Annex B: Sample Service Level Agreement (SLA) Template

Purpose: To provide a standardised and comprehensive starting point for SLAs between FPIs and their service providers, ensuring all critical performance, security, and compliance metrics are contractually defined and enforceable.

Key Sections of an FPI Service Level Agreement

I. **Service Description**: Details of the cloud services being provided (e.g., Secure IaaS for Level 3 Data).

II. **Performance Metrics**:

a. **Availability (Uptime)**: Tiered uptime guarantees (99.9%, 99.95%, 99.99%) based on the data classification level being hosted.

b. **Network Latency**: Commitment to <150ms latency within Nigeria.

c. **Sovereign Interconnect and Domestic Routing:** Commitment to maintain active, high-bandwidth peering with at least one NCC-licensed Internet Exchange Point (IXP), such as the Internet Exchange Point of Nigeria (IXPN), to ensure domestic routing of in-country workloads and minimise reliance on international transit.

d. **Recovery Time Objective (RTO)**: [e.g., < 1 hour].

e. **Recovery Point Objective (RPO)**: [e.g., < 4 hours].

III. **Support and Incident Response**: Tiered 24x7 support response and resolution times based on data classification.

IV. **Data Governance**: Commitment to Nigerian data residency, security standards, and the NDPA 2023.

V. **Penalties for Non-Compliance**: Clear financial penalties (e.g., service credits) for failing to meet agreed-upon metrics.

VI. **Exit Strategy**: Procedures for secure data repatriation and deletion upon contract termination.

Annex C: Government and Regulated Sector Risk Assessment and Threat Modelling Tool

Purpose: To provide a simple, standardised framework for FPIs and SIs to identify, assess, and mitigate risks associated with migrating and operating services in the cloud.

Sample Risk Register

Risk ID	Risk Description	Impact (1-5)	Likelihood (1-5)	Risk Score (I x L)	Mitigation Plan	Owner
001	Data breach due to misconfigured access controls	5	3	15	Implement PAM; conduct quarterly access reviews.	SI
002	Service outage due to DR failover failure	5	2	10	Conduct annual live DR failover test.	CSP/SI
003	Non-compliance with data residency for Level 3 data	4	2	8	Configure location-based policies; regular audits.	SI
004	Unauthorised access of cloud services	5	4	20	Train FPI employees on proper security practices. Zero Trust Architecture.	SI/FPI

Annex D: Cloud Provider Accreditation Checklist

Purpose: To outline the core criteria that will form the basis of the official NITDA certification checklist, ensuring a transparent and comprehensive evaluation process for all providers.

Governance and Oversight

The certification process for all Cloud Service Providers (CSPs) and Service Integrators (SIs) seeking inclusion on the Digital Regulatory Platform shall be managed by NITDA. This process ensures that all providers meet the mandatory security, operational, and compliance standards outlined in this Guideline.

Illustrative Accreditation Criteria

The summary below is illustrative and is intended to highlight the spirit in which the official checklist will be created, focusing on key domains of compliance.

I. **Corporate Compliance**:

a. Valid registration with the Corporate Affairs Commission (CAC).

b. Current Tax Clearance Certificate.

c. Demonstrated adherence to the Guidelines for Nigerian Content Development in ICT.

II. **Technical Standards**:

a. Data Centre Tier Certification (e.g., Uptime Institute, TIA-942).

b. Evidence of adherence to or a formal roadmap for achieving relevant ISO certifications.

c. Current SOC 2 Type II and/or CSA STAR attestation reports.

III. **Security Controls**:

a. Proof of annual, independent third-party

penetration testing.

b. Documentation of a security framework aligned with Zero Trust Architecture principles.

c. Details of implemented Privileged Access Management (PAM) and Multi-Factor Authentication (MFA) solutions.

IV. **Data Sovereignty Compliance**:

a. Attestation of the technical capability to host data of Level 2 and above securely within Nigeria.

b. Documentation of in-country encryption and key management protocols.

V. Requirements for Strategic Investment Waiver:

a. Minimum technical and investment requirements to qualify for and maintain a Strategic Investment Waiver, which grants foreign CSPs indigenous status and listing on the Digital Regulatory Platform. This could include phased data centre construction timelines, minimum Tier certification for local facilities, and local talent development targets.

Provisional Certification Pathway

I. To foster the development of local industry and ensure Nigerian providers can compete, a **Provisional Certification** pathway is established. This allows indigenous CSPs making verifiable progress towards meeting all required international standards to be listed on the Digital Regulatory Platform. For the purpose of fair competition, a Provisional Certification will be listed with the same standing as a Full Certification and will not be indicated differently on the Digital Regulatory

Platform.

II. To qualify for Provisional Certification, an indigenous provider must submit the following to NITDA:

   a. A documented and board-approved **roadmap to achieve full certification** within a maximum period of **24 months**.

   b. Verifiable evidence of having formally **engaged a certified auditor** to conduct a gap analysis and guide the implementation of required controls.

III. Providers holding a Provisional Certification may be restricted, at the discretion of NITDA, to hosting government and regulated sector data classified only as **LEVEL 1 (Limited Sensitivity)** and **LEVEL 2 (Moderate Sensitivity)**. This status is subject to a mandatory **annual review** by NITDA to assess progress. Provisional Certification will be revoked if satisfactory progress towards full certification is not demonstrated.

Annex E: Standardised Incident Reporting Form

Purpose: To ensure that data breach notifications submitted to NITDA and the NDPC are consistent, complete, and contain all necessary information for a rapid and effective regulatory response.

Data Breach Notification Form

I. **Section 1: Incident Overview**

a. **Reporting Organisation**: [CSP/SI Name]

b. **Affected FPI(s)**: [FPI Name]

c. **Date and Time of Discovery**: [DD/MM/YYYY HH:MM]

d. **Date and Time Range of Breach**: [DD/MM/YYYY to DD/MM/YYYY]

e. **Nature of Breach**: [e.g., Ransomware, Unauthorised Access, Misconfiguration]

II. **Section 2: Impact Assessment**

a. **Data Classes Involved**: [e.g., PII, Financial Records]

b. **Estimated Number of Data Subjects Affected**: [Number]

c. **Assessment of Risk/Harm to Individuals**: [Low/Medium/High, with justification]

III. **Section 3: Response and Mitigation**

a. **Measures Taken to Contain Breach**: [Description of actions]

b. **Plan to Notify Affected Individuals (if required)**: [Yes/No, with timeline]

IV. **Section 4: Contact Information**

a. **DPO / Primary Contact**: [Name, Email, Phone]

Annex F: Disaster Recovery Test Attestation Form

Purpose: To provide a formal, standardised document for service providers to certify that successful disaster recovery tests have been completed, fulfilling a key requirement for NITDA accreditation.

Disaster Recovery Test Attestation

This form attests that **[Provider Name]** successfully completed a disaster recovery test for the cloud infrastructure supporting **[FPI Name / "All Government Clients"]**.

I. **Date of Test**: [DD/MM/YYYY]

II. **Type of Test**: [e.g., Full Failover Simulation, Tabletop Exercise]

III. **Outcome**: **[ ] SUCCESSFUL [ ] PARTIAL SUCCESS [ ] UNSUCCESSFUL**

IV. **Summary of Results**: The test confirmed a successful failover to the secondary site located in [City, Nigeria]. The RTO of [e.g., 45 minutes] and RPO of [e.g., 5 minutes] were met.

V. **Attested By (Third-Party Auditor, if applicable)**: [Auditor Name/Firm]

VI. **Provider Representative**: [Name, Title, Signature]

Annex G: FinOps and Cloud Cost Reporting Template

Purpose: To provide a standardised framework for SIs to report on cloud spending to FPIs, ensuring fiscal transparency and accountability. This template also serves as the required format for mandatory submission to the Sovereign Cloud Governance Committee (SovGov), enabling its whole-of-government cost aggregation and negotiation functions as stipulated in the National Cloud Computing Guideline.

Quarterly Cloud Cost and Optimisation Report

I. **Reporting Period**: [Q1, Q2, Q3, Q4] [YEAR]

II. **FPI Name**: [FPI Name]

Prepared By: **[SI Name]**

Category	**Amount (NGN)**	**Notes / Key Changes**
Total Cloud Spend (This Quarter)		
Spend by Service (Top 5)	[e.g., Compute, Storage, Database]	[e.g., Increased compute for new e-service]
Budget vs. Actual Spend	[Budget: NGN, Actual: NGN, Variance: %]	[Explanation for variance]
Cost Savings Achieved		[e.g., NGN saved via reserved instances]
Cost Optimisation Recommendations		[e.g., Decommission unused resources, right-size VMs]

Annex H: Framework for Evaluating Foreign CSP Strategic Investment

This Annex is designated as the evaluation framework for strategic partnerships and Strategic Investment Waivers under Section 6.1 of the National Sovereign Cloud Policy and Section 9.1 of the National Cloud Computing Guideline.

Purpose: This framework provides a standardised guide for the Sovereign Cloud Governance Committee (SovGov) to evaluate the degree and strategic value of investments made by foreign Cloud Service Providers (CSPs) in Nigeria. The evaluation will inform decisions regarding procurement priority, the granting of temporary data localisation waivers, and eligibility for strategic partnerships under the National Cloud Computing Guideline.

I. **Evaluation:** The framework uses a colour-coded system to classify the level of investment commitment.

   a. **GREEN (Strongest Investment):** Indicates a direct, significant, and long-term capital investment in Nigeria's physical, economic, or human capital infrastructure. These actions directly support the core objectives of data sovereignty and local content development.

   b. **BLUE (Case-by-Case Determination):** Represents a valuable contribution but one that requires further assessment of its long-term impact and strategic alignment. These actions are positive but may be less capital-intensive or more commercially focused.

   c. **GRAY (Lukewarm Investment):** Describes actions that are minimal, primarily sales-driven, or leverage global programmes with no specific commitment to the Nigerian ecosystem.

Category 1: Local Data Centre Infrastructure

This evaluates direct investment in physical data centre facilities within Nigeria.

Level	Criteria for Evaluation
GREEN	I. Direct capital investment in the construction and operation of a **hyperscale availability region** with **multiple availability zones** within Nigeria. II. Facility(ies) must be certified as **Uptime Institute Tier III** (or TIA-942 Rated-3) for both the design and the constructed facility. III. Demonstrable use of local construction, engineering, and facilities management firms.
BLUE	I. Investment in a **single availability zone** or a dedicated local zone for specific services. II. A fully-funded, time-bound commitment (≤ 24 months) with financial guarantees to build a local data centre. III. A long-term, high-capacity co-location agreement with an indigenous data centre provider where the CSP owns and manages all core compute, storage, and network hardware.
GRAY	I. Reliance on data centres located in other African countries (e.g., South Africa, Kenya) to serve Nigerian customers. II. Presence is limited to an edge location or a network Point-of-Presence (PoP) only. III. Vague or non-committal statements about future data centre investments.

Category 2: Network Connectivity Infrastructure

This evaluates investment in the core network infrastructure that enhances national and international connectivity.

Level	Criteria for Evaluation
GREEN	I. Direct capital investment in landing new subsea cables in Nigeria. II. Funding and construction of terrestrial fibre-optic backbone routes connecting multiple states or underserved regions. III. Establishing multiple, high-bandwidth, geographically redundant peering points across NCC-licensed Internet Exchange Points (IXPs), demonstrably reducing reliance on international transit and reinforcing sovereign interconnect resilience.
BLUE	I. Significant investment in dedicated, redundant last-mile fibre connectivity to major government, enterprise, or technology hubs. II. Verified high-bandwidth interconnection with one or more NCC-licensed IXPs, with demonstrated capability for domestic routing of workloads in support of data localisation objectives. III. Co-investment partnerships with local telecommunications companies to expand fibre infrastructure.
GRAY	I. Sole reliance on leasing capacity from existing network providers, with no investment in independent transport infrastructure. II. Peering only at a single IXP at the minimum certification level, with no additional bandwidth, redundancy, or ecosystem contribution.

Category 3: Application & Service Localisation

This evaluates the extent to which a CSP's platform and services are tailored for the Nigerian market.

Level	Criteria for Evaluation
GREEN	I. Full localisation of the cloud platform, including user interfaces, technical documentation, and customer support in **major Nigerian languages**. II. Full integration with Nigeria's financial system, including **billing in Nigerian Naira (NGN)** and direct integration with local payment gateways. III. Development of **Nigeria-specific cloud services** or features that address local industry needs (e.g., in fintech, agriculture, healthcare).
BLUE	I. Platform available in English only but with full NGN billing and local payment support. II. Basic localisation of marketing materials and sales support.
GRAY	I. Platform and support are English-only. II. Billing is exclusively in a foreign currency (e.g., USD). III. Services are generic global offerings with no adaptation to the Nigerian context.

Category 4: Training & Capacity Building for SIs and Partners

This evaluates investment in developing the local technical and commercial partner ecosystem.

Level	Criteria for Evaluation
GREEN	I. Establishment of a **physical training and certification centre** in Nigeria. II. A comprehensive, locally-run programme to train and certify Nigerian SIs and partners on technical, security, and governance tracks, offered at **no cost or heavily subsidised**. III. Provision of dedicated, in-country partner development and technical support teams.
BLUE	I. Partner enablement programmes that are **primarily marketing-driven**, focused on co-selling and lead generation. II. Provision of online training vouchers and subsidies for remote certification exams.
GRAY	I. Reliance on global online training resources with no localised content or support. II. Partner programmes that require high fees or have significant barriers to entry for Nigerian companies.

Category 5: Local IT Industry & Startup Ecosystem Support

This evaluates direct contributions to fostering innovation and growth in Nigeria's broader tech industry.

Level	Criteria for Evaluation
GREEN	I. Establishment of a **local Venture Capital (VC) fund** or a formal partnership with a Nigerian VC to invest in tech startups. II. Creation and funding of a local **startup accelerator or incubator programme** in Nigeria. III. Establishment of a **local R&D centre** focused on cloud technologies or related fields.
BLUE	I. Offering significant, long-term cloud credits to startups registered in recognised Nigerian tech hubs. II. Sponsoring major local tech conferences and innovation challenges. III. Ad-hoc partnerships with universities or tech hubs without sustained funding.
GRAY	I. Global startup programmes that Nigerian companies can apply to, but with no specific local track or resources. II. Minimal engagement with the local tech community beyond sales and marketing efforts.

Other Strategic Considerations

In addition to the criteria above, SovGov will take the following factors into account to form a holistic view of a CSP's strategic commitment to Nigeria:

I. **Global Regulatory Compliance History:** The CSP's track record in other jurisdictions regarding compliance with data protection laws (e.g., GDPR), including any history of significant penalties or sanctions for non-compliance.

II. **Public Sector & Citizen Digital Skills Development:** The degree of investment in broad-based digital literacy programmes for government employees and the general public, including partnerships with educational institutions to develop a national digital skills curriculum.

III. **Local Supply Chain Development:** The CSP's commitment to procuring services and materials from local Nigerian businesses for its operations (e.g., facilities management, marketing, legal services), thereby contributing to the broader local economy.

IV. **Adherence to Data Ethics:** The CSP's demonstrable commitment to ethical data handling, particularly in the deployment of AI and automated systems, in alignment with the principles outlined in the NDPA General Application and Implementation Directive (GAID).

V. **Commitment to Open Standards:** The CSP's approach to interoperability and the use of open standards (e.g., Open Virtualisation Format) to prevent vendor lock-in, which is a key objective of the NCG2026.

VI. **Investment in Renewable Energy:** The extent to which the CSP invests directly in local renewable energy sources (e.g., solar farms) or enters into long-term Power Purchase Agreements (PPAs) with Nigerian green energy providers to power its infrastructure, as opposed to relying on diesel generators.

VII. **Transparent Protocols for Lawful Data Access:** The existence of clear, legally compliant, and transparent processes for responding to lawful requests for data access from Nigerian government and security agencies, in accordance with the NDPA and Mutual Legal Assistance Treaties (MLATs).

This Instrument was signed this 4th Day of August 2026

Kashifu Inuwa Abdullahi, *CCIE*

Director-General/CEO

National Information Technology Development Agency