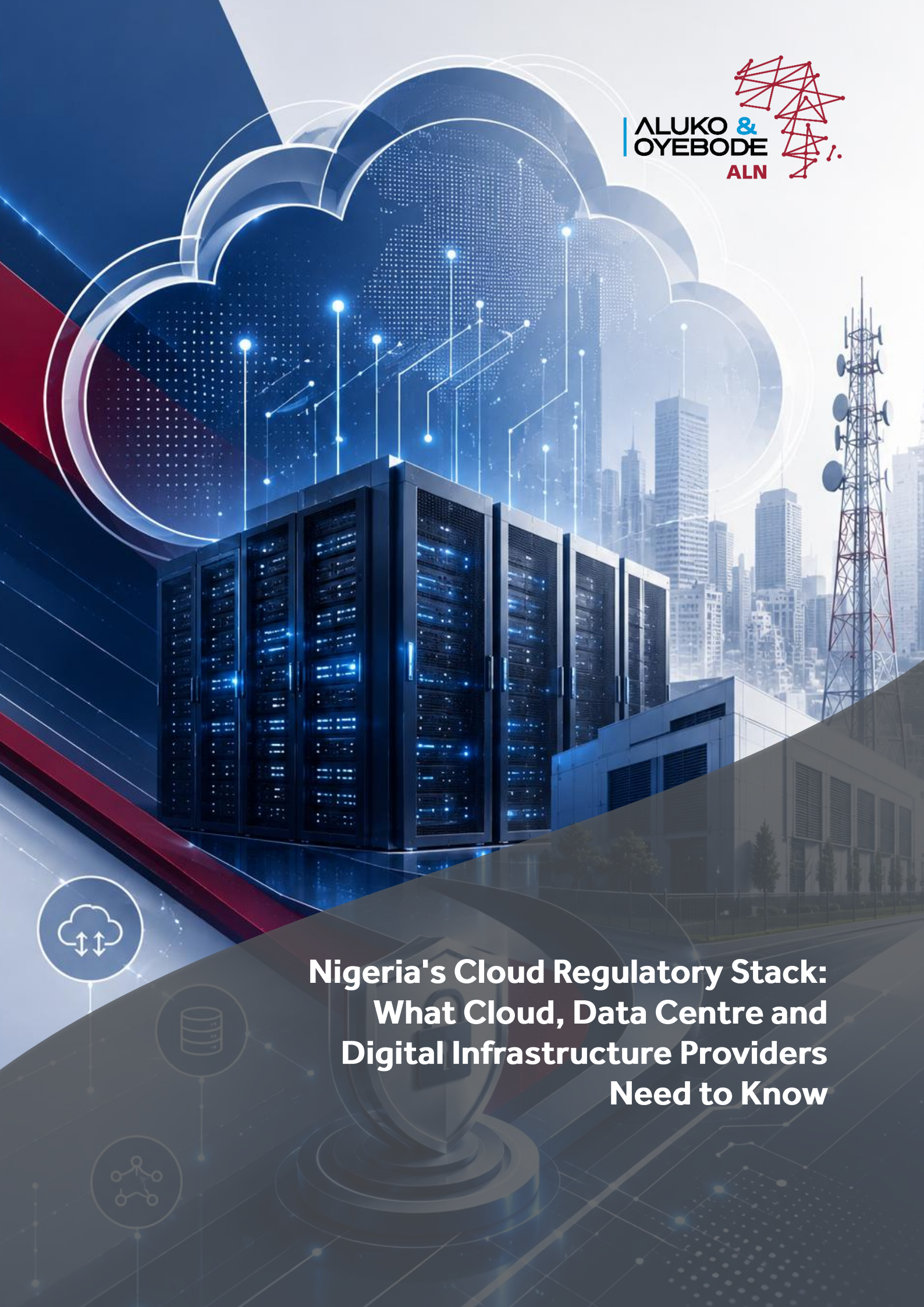


Nigeria's Cloud Regulatory Stack: What Cloud, Data Centre and Digital Infrastructure Providers Need to Know

Contents

BACKGROUND

Recently, the Federal Government of Nigeria, through the instrumentality of the Federal Ministry of Communications, Innovation, and Digital Economy, and the National Information Technology Development Agency (NITDA), introduced a suite of five interconnected cloud and digital infrastructure instruments driven by two key objectives: responding to the growing global demand for cloud computing and strengthening Nigeria's data sovereignty.

The five instruments are: (a) the National Digital Cloud Policy 2026; (b) the National Cloud Computing Guideline 2026 (NCCG); (c) the National Cloud Technical Guideline 2026 (NCTG); (d) the National Digital Infrastructure Assurance Framework 2026 (NDIAF); and (e) the National Cloud Investment Strategy 2026 (together, the "Cloud Framework").

Scoped with a two-year (24 months, starting from the publication month) implementation roadmap, the Cloud Framework establishes mandatory technical standards, financial requirements, certification metrics, ongoing compliance obligations, investor facilitation/incentives mechanisms, among others. In this piece, we map out the regulatory architecture, identify some of the key obligations, and highlight the strategic implications, impacted entities need to be aware of.

OVERVIEW: UNDERSTANDING THE REGULATORY STACK

The Cloud Framework is not a single monolithic regulation. It is a layered regulatory architecture, in which each of the five instruments performs a distinct function and applies to a different, and sometimes overlapping, group of entities. Understanding the scope of each instrument is essential to identifying which obligations apply to a particular organisation.

National Digital Cloud Policy

The National Digital Cloud Policy (the "Policy") is the overarching instrument from which the other components of the Cloud Framework derive direction.[1] The Policy has the broadest scope. Parts I and IV apply generally across the market, to investors, providers and government. Part II applies specifically to Federal Ministries and Federal Public Institutions (FPIs), on cloud adoption and procurement, while State and Local Governments may adopt it voluntarily. Part III applies only to sovereign data, as specifically defined and designated; this requires presidential approval.

The Policy supersedes the Nigeria Cloud Computing Policy of 2019. It establishes the Federal Government's vision for cloud investment, trade, government adoption and data sovereignty. The Policy speaks to the Nigerian Government's intent to make the investment climate as it concerns cloud infrastructure a temperate one, through fiscal incentives, regulatory facilitation, and the provision of anchor demand by positioning government as a major and reliable customer for cloud services. At the same time, the Policy mandates a Cloud First[2] approach for all FPIs of the Federal Government, while imposing risk-based sovereignty requirements dependent on the defined category of government and regulated data.[3]

While there is a general pursuit for data sovereignty, the Policy is not intended to mandate the localisation of ordinary commercial activity or general private data, neither does it: (a) discriminate between providers based on nationality, ownership or domiciliation; (b) require the use of Nigerian infrastructure for commercial workloads; or

[1] Issued by the federal government through the Federal Ministry of Communications, Innovation, and Digital Economy

[2] Similar to the National Cloud Computing Policy, 2019

[3] We explain this in greater detail below in this piece.

(c) condition market access on local establishment, except where a provider seeks incentives or government business in line with the provision of the Policy.[4]

The Policy supersedes the Nigeria Cloud Computing Policy 2019, and it expressly designates the NCCG, NCTG and NDIAF as its implementing instruments. Should any conflict arise between these documents, the Policy prevails, and the National Information Technology Development Agency (NITDA) must amend any inconsistent provision.[5]

The government has also indicated the definitive period within which to expect a list of recognised jurisdictions as affording appropriate protection as required under the NDPA.[6] This is strategically important to facilitate cross-border data transfer approvals required to implement the objectives of the Policy, whilst also providing comfort for businesses in general from a data protection compliance perspective.

> ***Whilst the Policy is effective from publication, Part III of the Policy, in respect of sovereign data, is not operational until approved by the President of the Federal Republic of Nigeria, given the economic significance of residency requirements and their implications for Nigeria's trade position and investment climate.***[7]

National Cloud Computing Guideline (NCCG) 2026

The NCCG is a mandatory guideline issued by NITDA effective from 1 January 2027. It applies to (a) Federal Public Institutions (FPIs),[8] (b) Cloud and Digital Service Providers; (c) Contractors, Partners, and Outsourcing Providers; (d) State and Local governments if adopted by them specifically; and (e) providers supporting regulated sectors and organisations processing, storing, transmitting or managing data designated as being of strategic national importance by NITDA, ONSA or relevant sector regulator.[9]

It introduces requirements that affect not only how cloud services are hosted and secured, but also how providers structure their contracts, manage data, support Federal Public Institutions (FPIs), respond to incidents, demonstrate compliance and address migration and exit. Central to its design is the Cloud First mandate, which requires all Federal Public Institutions (FPIs) to prioritize cloud-based solutions, with a target of 75% cloud adoption by 31 December 2030. The NCCG also establishes the Sovereign Cloud Governance Committee (SovGov), an advisory body with a mandate to ensure a coordinated approach to cloud adoption, enforce compliance with national standards, and steer the strategic evolution of Nigeria's sovereign cloud ecosystem.[10]

The NCCG (in line with the Policy) provides the classification framework for data localisation based on sensitivity:

- **Level 4:** data is strictly classified and must be hosted in the country, without exception. It consists of Military Intelligence, Critical National Information Infrastructure and strategic national secrets.
- **Level 3** data is highly sensitive and comprises data from regulated sectors and sensitive personal data with potential impact on national interest, intergovernmental communications, internal memorandums and related records. These must be hosted primarily in a private or secure cloud within Nigeria. Cross-border transfer is permissible under legal preconditions.

[4] Part 4.6 National Digital Cloud Policy, 2026
[5] National Digital Cloud Policy, Part 14.5.
[6] Parts 13.2 and 11.5 National Digital Cloud Policy, 2026
[7] Part 11.7 National Digital Cloud Policy, 2026
[8] 6.1 National Cloud Computing Guidelines, 2026.
[9] 6.1 (v) National Cloud Computing Guidelines, 2026.
[10] 12.1 National Cloud Computing Guidelines, 2026. A critical consideration on the establishment of the SovGov is the fact that, the mandate of the SovGov has been limited from the broad mandate in the Nigeria Digital Cloud Policy, and the composition is different from the composition under the Nigeria Digital Cloud Policy.

- **Level 2** (health and social information) is highly recommended to be hosted within Nigeria with cross-border hosting permitted subject to NITDA authorisation, an applicable NDPA transfer mechanism, and confirmation that the receiving jurisdiction meets adequate data protection, latency, and access standards.
- **Level 1** (public data, voluntarily shared personal information) is the most flexible tier, allowing hosting in any public cloud environment meeting recognised security standards.[11] Conditional exceptions exist for data classified as moderate and of limited sensitivity.[12]

All FPIs cloud procurement must flow through the Digital Regulatory Platform (DRP) that NITDA intends to publish in the future,[13] and only NITDA-certified providers may participate. This is likely to be similar to the current portal maintained for Indigenous IT service providers and contractors. The framework also gives priority to indigenous Cloud Service Providers (CSPs) and Service Integrators (SIs). The NCCG and its Schedules carry the same binding legal force as the main body of the NCCG, and any breach is treated as a breach of the NITDA Act 2007.[14]

Whilst the NCCG refers to the Nigerian Sovereign Cloud Policy, there is no indication as to the issuance of this policy, and may only refer to the Policy, and this is likely to be a clerical error.

National Cloud Technical Guideline (NCTG) 2026

The NCTG provides the technical details required for the implementation of the Cloud Framework. It applies to new and existing cloud services and supporting digital infrastructure used by FPIs as well as CSPs, 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 the following cloud deployment and service models: (a) Infrastructure-as-a-Service (IaaS), (b) Platform-as-a-Service (PaaS), (c) Software-as-a-Service (SaaS), (d) Functions as a Service (FaaS), and any other cloud deployment and service models recognised by NITDA. It requires FPIs and regulated sector entities to procure services only from the providers that comply with the technical guidelines. Effective date is 1 January 2027.

The NCTG specifies the security, operational and infrastructure standards that providers must meet. Among its key requirements are the adoption of Zero Trust Architecture for cloud environments supporting government and regulated sector workloads; adherence to international and national standards (including the ISO/IEC 17203, 27017, 27018, 19086), Cloud Security Alliance Star certifications and Service Organization Control Attestation reports. Importantly, the NCTG expressly defers to the NDIAF on matters of certification, accreditation and assurance processes; and where procedural questions arise, the NDIAF takes precedence.[15]

National Digital Infrastructure Assurance Framework (NDIAF) 2026

> ***The NDIAF is the national certification and continuous-assurance framework for digital infrastructure providers; it will take effect on 1 January 2027, or a later date approved and published by NITDA.***[16]

It prescribes national assurance requirements, conformity assessment mechanisms, workload assurance, continuous regulatory assurance, compliance monitoring, regulatory oversight, and the recognition of international assurance mechanisms for the digital infrastructure supporting Government, regulated sectors, Critical Information Infrastructure,[17] and other nationally significant digital services. It establishes Assurance Certification; a confirmation that a provider conforms with the framework. The certification is recognition based, that is, it

[11] Schedule A, National Cloud Computing Guidelines, 2026.
[12] Paragraph Section 10(IV)(c) National Cloud Technical Guidelines, 2026.
[13] On or before October 2026. Paragraph 17.1 (b), National Cloud Computing Guidelines, 2026.
[14] Section 13.2, National Cloud Computing Guidelines, 2026.
[15] Section 13.4, National Cloud Technical Guidelines, 2026.
[16] Paragraphs 5 and 9.1, National Digital Infrastructure Assurance Framework, 2026
[17] Paragraph 3.1, National Digital Infrastructure Assurance Framework, 2026; see also, Critical National Information Infrastructure as designated by Designation and Protection of Critical National Information Infrastructure Order, 2024

recognises international certification (particularly for corresponding technical requirements) and certifies Nigerian regulatory conformity.[18]

It establishes four certification classes:

- **Tier 1 - Integrated Digital Infrastructure Provider Certification:** this covers combined data centre, cloud, and integration services;
- **Cloud Infrastructure Provider Certification:** this covers the establishment and operation of data centres and related physical digital infrastructure;
- **Cloud Service Provider Certification:** this covers cloud services delivered from approved Deployment Regions or Availability Zones within Nigeria; and
- **Service Integration Provider Certification:** this covers integration services provided as a partner of, or under authorisation from, an NDIAF-certified Cloud Service Provider.

The NDIAF accepts international certifications such as ISO/IEC 27001, SOC 2 and CSA STAR, amongst others, as evidence of technical conformity, while reserving its own assessment for Nigeria-specific matters such as sovereignty, governance and resilience. Enforcement is graduated, ranging from advisory notices through to suspension and withdrawal of certification.[19]

The framework applies to Cloud Service Providers (CSPs), Cloud Infrastructure Providers (CIPs), Service Integrators (SIs), Data Centre Operators, Managed Service Providers (MSPs), Artificial Intelligence Infrastructure Providers, Sovereign Compute Providers, and such other entities providing, operating, supporting, or managing cloud and digital infrastructure services within Nigeria as may be designated by NITDA, in each case to the extent that they provide data centre services, cloud services, or integration services supporting Public Institutions,[20] Regulated Sectors,[21] operators of Critical Information Infrastructure, critical digital infrastructure supporting essential national services, and other high-impact organisations designated by NITDA. Specifically, certification becomes applicable in these instances:[22]

- *(i) FPIs (and State and Local Government institutions that adopt this Framework) are required to procure and utilise services by providers with valid NDIAF Assurance Certification of the relevant class, and with the workload assurance endorsements, appropriate to the relevant workload classification;*
- *(ii) NDIAF Assurance Certification constitutes the national assurance baseline for regulated sector Workloads. Regulated sectors, in the instance of the NDIAF, are sectors designated by NITDA as regulated and listed in a designated sector list.*
- *(iii) operators of Critical Information Infrastructure, and operators of critical digital infrastructure supporting essential national services, would be required to utilise NDIAF certified providers where certification is required under applicable national critical infrastructure protection requirements or sector-specific obligations; and*
- *(iv) organisations designated by NITDA, or by another competent authority in coordination with NITDA, as requiring trusted digital infrastructure services would need to utilise NDIAF-certified providers in accordance with the terms of the designation.*

[18] Paragraph 3.4 National Digital Infrastructure Assurance Framework, 2026

[19] NDIAF 2026, Paragraph 18.6 (Three-Stage Assurance Model).

[20] "Public Institution" means a Federal Public Institution, and any State or Local Government institution that adopts this Framework by law, policy, or a formal instrument of adoption.

[21] "Regulated Sector" means a sector of the economy designated by NITDA, in concurrence with the relevant sector regulator, and published in the Designated Regulated Sectors List issued under the NDIAF, having regard to the sector's significance for national security, public safety, financial stability, public health, or the delivery of essential services.

[22] Paragraph 7 National Digital Infrastructure Assurance Framework, 2026

Other providers not covered above are not required to obtain certification.

Notably, as regards what constitutes a "Regulated Sector", the documents adopt different approaches to the concept, and this distinction is important when reading their requirements together. Under the NDIAF, a "Regulated Sector" is a sector specifically designated by NITDA in concurrence with the relevant sector regulator and included in the Designated Regulated Sectors List issued by NITDA.[23] By contrast, both the NCTG and NCCG adopt a broader, function-based definition, covering any sector subject to the oversight, supervision, licensing, registration or regulation of a competent statutory or regulatory authority established under Nigerian law, while also expressly including sectors designated as critical to national security, public safety, financial stability, public health or the delivery of essential public services.[24]

National Cloud Investment Strategy 2026

Unlike the other four instruments, the Investment Strategy[25] is non-binding. Its purpose is to translate the regulatory framework into an investor-facing proposition, articulating the commercial opportunity, government's long-term commitment, and the pathway into the Nigerian market. The Investment Strategy rests on six pillars: policy and regulatory environment; funding and investment mobilisation; infrastructure development and connectivity; digital skills and workforce development; innovation and local content development; and cybersecurity and data protection.

A particularly useful feature is the Approval in Principle (AIP) process. This is a structured, time-bound preliminary facilitation instrument issued by NITDA confirming that a proposed investment is consistent with the NDIAF, NCCG and applicable data governance requirements. However, it is important to note that an AIP does not constitute a statutory licence, final certification, procurement commitment, fiscal-incentive approval, land allocation, foreign-exchange guarantee or exclusivity; it is a starting point, not an end point.[26]

The table below summarises the key distinguishing features of each instrument.

[23]Paragraph 8 National Digital Infrastructure Assurance Framework, 2026. Designation is based on considerations such as national security, public safety, financial stability, public health and the delivery of essential services

[24]Paragraph 8 National Cloud Technical guideline, 2026; and Paragraph 8 National Cloud Computing Guideline, 2026.

[25]Investment Strategy denotes the roadmap to harness resources and opportunities that position the country as the preferred destination for cloud infrastructure, hyperscale data centres, sovereign compute, and digital infrastructure investment.

[26]National Cloud Investment Strategy 2026, Section 6 (Six Pillars); Section 14 (AIP Process).

FIG. 1.0 CLOUD FRAMEWORK – COMPARATIVE SUMMARY:

	National Digital Cloud Policy	NCCG 2026	NCTG 2026	NDIAF 2026	Investment Strategy 2026
Legal Nature	Federal Government policy; overarching framework. Parts I, II, IV effective on publication; Part III requires Presidential approval.[27]	Mandatory guideline under NITDA Act 2007; effective 1 January 2027.[28]	Mandatory technical guideline under NITDA Act 2007; effective 1 January 2027 or such other date as specified by NITDA.[29]	Mandatory assurance/certification framework under NITDA Act 2007; effective 1 January 2027 or such other date as specified by NITDA.[30]	Non-binding strategy document.[31]
Addressees	Market-wide (Parts I & IV); FPIs (Part II); holders of sovereign data (Part III); State/Local Governments (voluntary).[32]	FPIs; CSPs, SIs, data centre operators, digital infrastructure providers; contractors handling government data; regulated sectors; State/Local Governments (opt-in).[33]	FPIs; all CSPs, SIs, data centre operators, managed service providers, AI infrastructure providers, sovereign compute providers operating in Nigeria.[34]	Providers serving Public Institutions, designated regulated sectors, CII operators, designated organisations; voluntary for others.[35]	Investors, development partners, financial institutions, technology providers.[36]
Key Triggers	Publication (general); handling of sovereign data (Part III).[37]	Provision of cloud services to FPIs or regulated sectors; processing government or strategically important data; FPI cloud procurement.[38]	Operation of cloud services or digital infrastructure in Nigeria; procurement by FPIs or regulated sectors.[39]	Provision of data centre, cloud or integration services to Public Institutions, designated regulated sectors, CII operators or other designated organisations.[40]	Interest in cloud or data centre investment in Nigeria.[41]

[27] National Digital Cloud Policy, Parts 1.5, 11.7, 14.5.
[28] NCCG 2026, Paragraphs 4, 5.
[29] NCTG 2026, Paragraphs 4, 5.
[30] NDIAF 2026, Paragraphs 4, 5.
[31] National Cloud Investment Strategy 2026, Section 1.
[32] National Digital Cloud Policy, Parts 1.6, 10.5.
[33] NCCG 2026, Paragraph 6.1.
[34] NCTG 2026, Paragraph 6.
[35] NDIAF 2026, Paragraph 7.2.
[36] National Cloud Investment Strategy 2026, Executive Summary.
[37] National Digital Cloud Policy, Parts 1.6, 11.7.
[38] NCCG 2026, Paragraphs 9.1, 9.2.
[39] NCTG 2026, Paragraph 6.
[40] NDIAF 2026, Paragraphs 7.2, 7.3.
[41] National Cloud Investment Strategy 2026, Section 14.

	National Digital Cloud Policy	NCCG 2026	NCTG 2026	NDIAF 2026	Investment Strategy 2026
Enforcement	Policy prevails over implementing instruments; NITDA audits; ICT project clearance withheld for non-compliance; sanctions, suspension or revocation of registration.[42]	Breach is a violation of NITDA Act 2007; graduated sanctions (warnings to DRP suspension and recertification); NDPA and Cybercrimes Act penalties also apply.[43]	Is silent on penalties but notes that it exists to provide the technical implementation aspects of the NCCG.	NDIAF Certification required; continuous assurance (annual surveillance, reassessment, risk-based inspections); graduated enforcement (advisory to withdrawal of certification); financial assurance for sovereign workload holders, amongst others.[44]	None (non-binding); AIP is a facilitation instrument, not a licence.[45]

[42] National Digital Cloud Policy, Parts 11.10, 14.5.
[43] NCCG 2026, Paragraph 13.2.
[44] NDIAF 2026, Paragraphs 9.12, 9.14, 18.6.
[45] National Cloud Investment Strategy 2026, Section 14.1.

KEY HIGHLIGHTS OF THE CLOUD FRAMEWORK:

Data Classification, Residency and Sovereignty

The Cloud Framework establishes a mandatory four-tier data classification system - Classified (Level 4), Highly Sensitive (Level 3), Sensitive (Level 2), and Open (Level 1) - that determines how government, regulated sector, and citizen data must be handled. Each tier prescribes specific hosting requirements (from exclusive on-premises infrastructure for Level 4 to any compliant public cloud for Level 1), cross-border transfer permissions (prohibited for Level 4, NITDA-approval required for Levels 3 and 2, unrestricted for Level 1). It includes backup and recovery obligations (geographically separated within Nigeria for Levels 4 and 3), and encryption key custody arrangements (government-controlled in Nigeria for Level 4). Hosting requirements attach to classification rather than to data type, sector, or provider identity, so that identical protections apply to identical risk regardless of which institution holds the data. Below is a summary of the classification framework.

FIG. 1.1 NATIONAL DATA CLASSIFICATION FRAMEWORK

Classification Level	Sensitivity	Data Types / Examples	Hosting Requirement	Cross-Border Transfer	Backup & Recovery
Level 4 (Classified)	Classified	Military intelligence; Critical National Information Infrastructure (CNII) schematics; strategic national secrets; diplomatic communications[46]	Exclusively on-premises within the FPI, in a collocated private data centre, or in a NITDA-certified private cloud located within Nigeria[47]	Prohibited under any circumstances[48]	Geographically separated recovery site within Nigeria; backup may not leave the country[49]
Level 3 (Highly Sensitive)	Highly Sensitive	Regulated sector data; sensitive personal data (financial, health, biometric, identity); intergovernmental communications; internal memorandums; PPP data; designated CNII data[50]	Primarily in a private or secure hybrid cloud within Nigeria[51]	Permissible only under NDPA-compliant lawful transfer mechanisms and subject to NITDA approval[52]	Geographically separated recovery site within Nigeria; backup may not leave the country[53]
Level 2 (Sensitive)	Sensitive (Moderate)	Personal health and social information; confidential reports; internal records of public institutions and SMEs; non-sensitive personal data under NDPA[54]	Hosted in Nigeria by default; cross-border hosting permitted with prior NITDA authorisation[55]	Permitted subject to: (i) prior NITDA authorisation; (ii) applicable NDPA transfer mechanism; (iii) adequate data protection standards in receiving jurisdiction; (iv) recognised latency and access requirements[56]	Standard disaster recovery protocols with defined RTOs and RPOs[57]

[46]NCCG 2026, Schedule A, Paragraph 15.1.
[47]National Digital Cloud Policy, Part 11.4; NCCG 2026, Schedule A, Paragraph 15.1(d).
[48]National Digital Cloud Policy, Part 11.4.
[49]National Digital Cloud Policy, Parts 5.2, 11.4.
[50]NCCG 2026, Schedule A, Paragraphs 15.2(I), 15.2(II).
[51]National Digital Cloud Policy, Part 11.4; NCCG 2026, Schedule A, Paragraph 15.2(I)(d).
[52]National Digital Cloud Policy, Part 11.5; NCCG 2026, Paragraph 9.2.
[53]National Digital Cloud Policy, Parts 5.2, 11.4.
[54]NCCG 2026, Schedule A, Paragraphs 15.3(I), 15.3(II).
[55]National Digital Cloud Policy, Part 11.4; NCCG 2026, Schedule A, Paragraph 15.3(I)(d).
[56]National Digital Cloud Policy, Part 11.4; NCCG 2026, Paragraph 9.3.
[57]NCCG 2026, Paragraph 10.3.

Classification Level	Sensitivity	Data Types / Examples	Hosting Requirement	Cross-Border Transfer	Backup & Recovery
Level 1 (Open)	Open (Low)	Open government data; public reports; personally shared information; corporate non-confidential data (annual reports, marketing materials)[58]	May be hosted on any public cloud environment meeting nationally or internationally recognised security standards[59]	No residency restriction[60]	Standard backup practices

[58] NCCG 2026, Schedule A, Paragraphs 15.4(I), 15.4(II).
[59] National Digital Cloud Policy, Part 11.4; NCCG 2026, Schedule A, Paragraph 15.4(I)(d).
[60] National Digital Cloud Policy, Part 11.4.

One critical point to note is that the classification framework and the residency requirement would require presidential approval on the recommendation of the Federal Executive Council to be effective. This requirement ensures that restrictions on data location are adopted deliberately, at the highest level of government, with their economic consequences expressly weighed. Designation of regulated (sector) data for the purpose of this classification into Levels 3 and 4 is also expected to have presidential approval on the recommendation of the Federal Executive Council, following the assessment of the SovGov.[61]

Localisation of Financial Data

All financial data generated, processed, transmitted or stored by regulated financial institutions are required to be primarily hosted, processed and stored within the territorial boundaries of the Federal Republic of Nigeria.[62] This represents a significant shift from the CBN's recent circular requiring payment data generated within Nigeria to be stored within Nigeria; it also represents a shift from the Policy position requiring presidential approval for this level of residency requirement. This requirement stretches to both CBN and SEC regulated entities.[63]

Certification and Registration

Where an organisation intends to provide cloud or digital infrastructure services to Federal Public Institutions, designated regulated sectors, Critical Information Infrastructure (CII) operators or other designated organisations, it must obtain and maintain the relevant NDIAF Assurance Certification. The applicable certification class will depend on the nature of the provider's role, whether as an integrated digital infrastructure provider, cloud infrastructure provider, cloud service provider or service integration provider.

In addition, workload assurance endorsements would be required for government workloads,[64] regulated-sector workloads, CII-related services or other nationally significant digital services.

Further, the provider must also be listed on NITDA's Digital Regulatory Platform, which is intended to operate as the mandatory procurement channel for eligible cloud services. Although local incorporation or establishment is not presented as a general market-entry requirement, applicants seeking NDIAF certification must provide evidence of incorporation either in Nigeria or in a foreign jurisdiction approved by NITDA, together with evidence of registered place of business in Nigeria.[65]

Data Centre and Physical Infrastructure Standards

The minimum standard for data centre and physical infrastructure providers intending to be certified by NITDA or seeking national digital infrastructure assurance status would be required to be designed, constructed, and operated to a minimum auditable standard. The following are minimum standards required based on the data classification level:

- 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.
- Facilities hosting Level 2 data must, at a minimum, meet the requirements of Uptime Institute Tier II or TIA-942 Rated-2.

[61]Paragraph 11.7 of the Policy.
[62]Paragraph 9.2 of the NCCG.
[63]This is particularly given that the NCCG does not define the term "financial institutions".
[64]Workload means an application, system, dataset, service, or computing process hosted or executed on digital infrastructure.
[65]Paragraph 9.3 b National Digital Infrastructure Assurance Framework, 2026. Notably, this seems to allow foreign entities to carry out business activities in Nigeria without having to locally incorporate as required under Section 78 of the Companies and Allied Matters Act 2020.

Reporting Obligations & Audit

The reporting obligations under this framework are substantial and time-sensitive. The following are some of the reporting obligations:

- **Incident:** The 72-hour incident notification rule applies to both personal and non-personal government and regulated sector data. When a qualifying incident occurs, the service provider must notify the affected FPI, NITDA, the NDPC (where personal data is involved) and any relevant sector regulator. Qualifying service providers (CSPs and SIs) are also required to maintain comprehensive incident logs and make them available to law enforcement upon lawful request.[66]
- **Infrastructure Status Reporting:** service providers are required to submit quarterly infrastructure status reports.[67]
- Data Center Power Usage Effectiveness (PUE) Reporting: PUE must be reported to NITDA annually.
- **Compliance Audit:** Certified providers are required to conduct and submit regulatory compliance returns in a manner prescribed by NITDA no later than 90 days after the end of each calendar year.[68]
- **NITDA Audit:** NITDA and certified third party will perform audit to (a) validate agreed controls, and (b) verify compliance with security, data handling, and localisation requirements.
- **Risk-Based Monitoring Exercise:** Apart from the above obligations, certified providers will experience risk-based surveillance assessment proportional to their certification classes.[69]

Procurement and Compliance

Cloud procurement by Federal Public Institutions, or other regulated sectors, must be conducted through the Digital Regulatory Platform (DRP), and the engagement of unlisted providers is prohibited and may attract administrative sanctions.[70] Cloud service arrangements must also be governed by Service Level Agreements (SLAs) addressing, at a minimum, availability commitments, data protection, business continuity and disaster recovery, remedies for non-performance, data ownership, exit and migration arrangements, and the parties' respective obligations under the Shared Responsibility Model.[71] In addition, a Privacy Impact Assessment (PIA) or Data Protection Impact Assessment (DPIA), as applicable, must be completed under the Nigeria Data Protection Act 2023 before any new cloud procurement is undertaken.

Indigenous Participation

The framework includes meaningful indigenous participation requirements. All Service Integrators must be indigenous companies, and FPIs are required to give priority to indigenous CSPs when procuring cloud services. Foreign CSPs may obtain provisional indigenous status through a Strategic Investment Waiver recommended by SovGov, but this is limited to one year and renewable only once. SIs must also provide detailed local content development plans covering job creation and human capital development. These requirements reflect the Government's broader objectives around building domestic capacity in the digital infrastructure sector.[72]

[66]Paragraph 10.3 (iv) NCTG.
[67]Paragraph 12.2 of the NCTG.
[68]Paragraph 18.1 (g) of the NDIAF.
[69]Paragraph 18.3 of the NDIAF.
[70]NCCG, s 17.2.
[71]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. Paragraph 8 NCTG
[72]NCCG 2026, ss 9.1, 17.4; Schedule D, s 19.2.

Minimum Capitalisation and Other Financial Requirements

The NDIAF prescribes minimum capitalisation and financial assurance/guarantee requirements that scale by certification class. Below is an instructive overview of some of the financial requirements for NDIAF assurance certification:[73]

FIG. 2 NSCI FINANCIAL REQUIREMENTS:

Certification Class	Minimum Financial Capacity (paid-up capital or equivalent)	Minimum Combined Professional Indemnity and Cyber Liability Insurance (per occurrence)	Financial Assurance[74]
Tier 1 — Integrated Digital Infrastructure Provider Certification	₦1,000,000,000	₦500,000,000	₦200,000,000
Cloud Infrastructure Provider Certification	₦500,000,000	₦250,000,000	₦100,000,000
Cloud Service Provider Certification	₦100,000,000	₦250,000,000	₦20,000,000
Cloud Service Provider Certification (Restricted)	₦25,000,000	₦50,000,000	Nil[75]
Service Integration Provider Certification	₦10,000,000	₦50,000,000 (professional indemnity)	-

Application and certification fees range from ₦500,000 to ₦1,000,000 and ₦5,000,000 to ₦15,000,000 respectively.[76]

Transition Deadlines Are Already Running

There are transitional provisions which impacted entities must pay attention to. For instance, existing data centre operators must obtain the relevant NDIAF certification within 12 months of commencement. Existing cloud service providers and service integrators serving Public Institutions, regulated sectors or Critical Information Infrastructure operators have 24 months. Providers already serving FPIs must onboard to the Digital Regulatory Platform from commencement, amongst others. These are hard deadlines unless otherwise varied by NITDA.[77]

Contract Restructuring Requirements

FPIs cloud service contracts are now required to be structured on a consumption (pay-as-you-go) or subscription basis aligned with an operational expenditure model.[78] Contracts must include clear anti-vendor lock-in provisions, documented exit and migration arrangements, data extraction in non-proprietary formats, deletion or return of data, and transition timelines.[79] Every SLA must define the shared responsibility model between the CSP, the FPI and the SI, covering who is responsible for security of the cloud versus security in the cloud. Existing contracts with

[73] Schedule 1.3 to the NDIAF
[74] For Sovereign Workload Assurance Holder and systemically significant service providers.
[75] Does not qualify for sovereign workload. See S1.7 to the NDIAF
[76] S1.6 to the NDIAF
[77] Paragraph 21.3 of the NDIAF
[78] Paragraph 12.3, 17.2 and 17.3 of the NCCG
[79] Paragraph 11.2 of the NCCG

Public Institutions that do not meet these requirements must be brought into compliance during the transition period.[80]

Beneficial Ownership Transparency

Every applicant for NDIAF certification must disclose full beneficial ownership information, including the identity, jurisdiction and regulatory history of its ultimate beneficial owners.[81] Any change in ownership or control must be notified to NITDA within 30 days. A change in control through acquisition or merger requires advance notice. Any material misrepresentation in ownership information may result in refusal, suspension or withdrawal of certification.

Cross-Border Transfer

The Cloud Framework creates a dual cross-border transfer framework. Impacted entities that intend to transfer data outside Nigeria, which includes personal and non-personal data, must now fulfil NITDA and NDPC transfer requirements.

CONCLUSION AND STRATEGIC CONSIDERATIONS

Whilst regulatory clarity is needed around the classification framework and the required presidential approval, impacted entities may need to critically consider how the Cloud Framework will impact their business during the transitional period. Hyperscalers and other cloud service providers would need to critically assess the impact of the technical guideline and the certification requirements against their current posture and clientele. For instance, operators with the relevant international standards would currently have a good posture towards NITDA compliance. Operators with international standards and local registration would have a great posture towards meeting the NITDA requirements.

Whilst the Policy indicates that financial data be stored primarily within the boundaries of Nigeria, stakeholders may want to engage with NITDA and the ministry to ascertain if this has been pre-approved by the Presidency in line with the Policy or if this requirement is meant to operate within level 2 of classification, where NITDA approval is required to host data out of the country and localisation is only recommended. This remains very critical given the reliance of the financial sector on cloud services. For instance, what happens to cross-border transactions? What impact is this likely to have on international card schemes? Etc. These are risks that the regulator may want to consider in making these determinations.

If you would like further guidance on compliance planning, certification applications or investment structuring under Nigeria's cloud regulatory framework, please do not hesitate to contact us at tmtpractice@aluko-oyebode.com

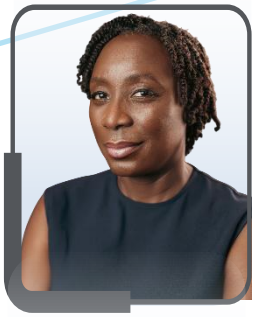
[80] Paragraph 17.3 (vii) of the NCCG.
[81] Paragraph 9.3, and 9.4 of the NDIAF

Disclaimer

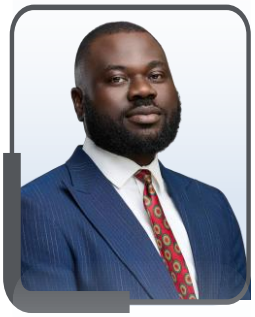
The publication is from Aluko & Oyebode and is intended only for its recipients. If you are not the intended recipient(s), please contact Aluko & Oyebode via telephone (+234 1 4628360) or e-mail (***ao@aluko-oyebode.com***).

Further information about the firm, its practice areas, client briefing notes and details of seminars/events are available at ***www.aluko-oyebode.com***. This is a publication of Aluko & Oyebode and is for general information only. It should not be construed as legal advice under any circumstances.

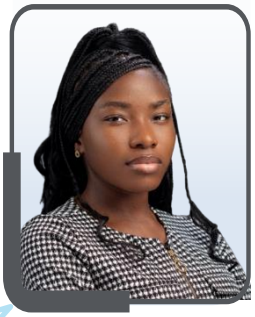
Key Contacts



Sumbo Akintola
Partner
Lagos, Nigeria
Sumbo.Akintola@aluko-oyebode.com



Timothy Ogele
Senior Associate
Lagos, Nigeria
Timothy.Ogele@aluko-oyebode.com



Thelma Georgewill
Associate
Lagos, Nigeria
Thelma.Georgewill@aluko-oyebode.com

Collins Okoh
Associate
Lagos, Nigeria
Collins.Okoh@aluko-oyebode.com

Office Locations

Lagos

1, Murtala Muhammed Drive
(formerly Bank Road)
Ikoyi, Lagos, Nigeria

T: +234 1 462 8360-71
F: +44 207 681 3402
E: ao@aluko-oyebode.com
W: www.aluko-oyebode.com

Abuja

Plot 1348A Agulu Lake
Maitama, Abuja.
Nigeria

Port Harcourt

3rd Floor, Plot 173,
Sani Abacha Road
GRA Phase III, Port Harcourt
Rivers State, 234
Nigeria

T: +234 703 192 2607