NATIONAL DIGITAL INFRASTRUCTURE ASSURANCE FRAMEWORK (NDIAF)

Table of Contents

Document Information

S/N	Data Element	Value
1	Title	National Digital Infrastructure Assurance Framework, 2026
2	Short Title	Digital Infrastructure Assurance Framework (NDIAF)
3	Document Identifier	
4	Version	Version 2.0
5	Approval Date	4th august 2026
6	Effective Date	1st January 2027
7	Publisher	National Information Technology Development Agency (NITDA)
8	Document Type	Framework
9	Enforcement Status	Mandatory for procurement and use by Public Institutions; adopted in regulated sectors through sector-specific regulatory instruments; applicable to Critical Information Infrastructure in accordance with national critical infrastructure protection requirements, as set out in Part 7
10	Document Owner	National Information Technology Development Agency (NITDA)
11	Custodian	Regulations and Compliance Department
12	Target Audience	Public Institutions; Cloud Service Providers; Cloud Infrastructure Providers; Data Centre Operators; Service Integrators; Managed Service Providers; Artificial Intelligence Infrastructure Providers; Sovereign Compute Providers; Government Contractors; Operators of Critical Information Infrastructure; Professional Bodies; Development Partners; and other organisations providing or supporting digital infrastructure and services within Nigeria.
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 Cloud Technical Guideline; National Data Classification & Localisation Framework
15	Review Cycle	Every three (3) years or as required.
16	Language	English

17	Format	Electronic (PDF)
18	Subject	Digital Infrastructure Assurance, NDIAF Certification, Cloud Services Assurance, Continuous Regulatory Assurance, Data Centre Assurance, ICT Governance, and Regulatory Compliance
19	Classification	Public
20	Copyright	

1. Long Title

A Framework to establish national assurance requirements, a certification and conformity assessment regime, and continuing regulatory oversight for data centre services, cloud services, and integration services supporting Public Institutions, Regulated Sectors, and Critical Information Infrastructure in Nigeria; and for related matters.

2. Short Title

This Framework may be cited as the National Digital Infrastructure Assurance Framework.

3. Explanatory Note

3.1 This Framework establishes Nigeria's national assurance framework for trusted digital infrastructure, covering data centres, cloud services, integration services, artificial intelligence infrastructure, sovereign compute, and related digital services. 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, and other nationally significant digital services. NDIAF Assurance Certification is the principal mechanism through which conformity with the Framework is demonstrated and is one component of the Framework rather than the Framework itself.

3.2 NDIAF Assurance Certification is the Agency's formal confirmation that a provider conforms to Nigeria's National Digital Infrastructure Assurance Framework. The Certification evidence compliance with the national assurance requirements applicable to the relevant Certification Class, including the Nigerian Regulatory Assurance Requirements consolidated in Schedule 2, and confirms the provider's participation in the Framework's continuous assurance regime. It rests on the Agency's statutory functions of standards development, certification, conformity assessment, and compliance monitoring, and it operates alongside the licences of sector regulators and internationally recognised technical certifications, each of which serves its own distinct purpose.

3.3 The Framework establishes four classes of NDIAF Assurance Certification, namely the Integrated Digital Infrastructure Provider Certification (Tier 1), the Cloud Infrastructure Provider Certification, the Cloud Service Provider Certification, and the Service Integration Provider Certification, as the recognised assurance pathway for providers serving Public Institutions, regulated sectors, operators of Critical Information Infrastructure, and other designated organisations, and for onboarding onto the NITDA Digital Regulatory Platform (DRP) established under the National Cloud Computing Guideline.

3.4 The Framework adopts a recognition-based assurance philosophy: recognise internationally accepted technical assurance; certify Nigerian regulatory conformity. Internationally recognised certifications, independent conformity assessments, and technical audits verify conformance with technical standards and are recognised, not replicated, by the Agency. NDIAF Assurance Certification accordingly addresses only the additional Nigerian requirements digital sovereignty, localisation, governance, operational resilience, regulatory obligations, reporting, public interest requirements, and continuous compliance and the Agency accepts recognised international assurance as evidence of compliance with corresponding technical requirements.

3.5 All regulatory decisions under this Framework, including the grant, refusal, renewal, variation, suspension, and withdrawal of NDIAF Assurance Certifications and workload assurance endorsements, and all enforcement action, are vested directly in the Agency, which supervises Certified Providers on a risk-based basis and may coordinate with other competent authorities where regulatory responsibilities intersect.

3.6 Certification under this Framework is not a one-time assessment. The Framework establishes a continuous assurance lifecycle, initial certification, annual surveillance, periodic reassessment, incident reporting, compliance monitoring, material change notification, risk-based inspection, corrective action, and, where necessary, suspension or withdrawal of certification, because the digital infrastructure supporting Government, regulated sectors, and Critical Information Infrastructure constitutes critical national assets whose assurance engages digital sovereignty, national security, and the public interest. Continuous assurance provides supervision throughout the life of an operation, enforceable certification conditions, market visibility, and proportionate regulatory intervention, which a

point-in-time assessment cannot deliver. The Framework directly supports the National Sovereign Cloud Initiative, Nigeria's data localisation objectives, the implementation of sector-specific localisation requirements, the protection of Critical Information Infrastructure, trusted government procurement, and the development of indigenous digital infrastructure.

3.7 The Framework is implemented on a risk-based, proportionate, and phased basis. It applies enhanced requirements where workloads are sensitive, critical, or strategic, and proportionate requirements elsewhere, and it avoids imposing regulatory burden on lower-risk market participants that fall outside its mandatory scope. It is expected to deliver regulatory certainty for investors, a trusted and competitive market for providers, stronger protection for customers and government, and durable assurance of Nigeria's digital sovereignty and national resilience.

3.8 The value of NDIAF Assurance Certification to a provider is concrete. Certification demonstrates Nigerian regulatory conformity through a single, nationally recognised confirmation; establishes eligibility for, and a trusted position in, Government procurement; is recognised across regulated sectors as the national assurance baseline, so that a provider is assessed once rather than sector by sector; reduces duplicative compliance by carrying with it the recognition of international certifications under Part 16; strengthens market confidence through publicly verifiable trusted-provider status on the Digital Regulatory Platform; and positions the provider to participate in sovereign cloud adoption under the National Sovereign Cloud Initiative.

3.9 The Agency regulates conformity with this Framework; it does not regulate the day-to-day operation of providers. Every operational obligation imposed under this Framework serves one or more of four objectives: maintaining conformity with the national assurance requirements; protecting Government and regulated sector workloads; protecting Critical Information Infrastructure; and protecting digital sovereignty. The provisions of this Framework, and every instrument made under it, shall be interpreted and applied in the light of these objectives, and regulatory assurance under this Framework shall not unnecessarily inhibit innovation, competition, or market entry.

4. Authority

In exercise of the powers conferred on it by Sections 6 and 32 of the National Information Technology Development Agency Act, 2007, its function under Section 6(a) to create a framework for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of information technology practices, activities and systems in Nigeria; its functions under Sections 6(b)–(e) to issue guidelines, including guidelines for the standardization and certification of information technology; its function under Section 6(i) to introduce appropriate regulatory policies and incentives to encourage private sector investment in the information technology industry; and Section 17(4) of the Act, under which failure to comply with guidelines and standards prescribed by the Agency constitutes an offence, the National Information Technology Development Agency hereby issues the National Digital Infrastructure Assurance Framework. The Framework is made in exercise of the Agency's express statutory powers relating to regulation, standardisation, certification, guideline development, and compliance monitoring, and it establishes national assurance requirements, a certification and conformity regime, and continuing regulatory oversight for digital infrastructure and cloud services pursuant to that mandate. The Framework operates within the statutory scheme of existing laws in Nigeria, the licences, permits, and approvals of sector regulators and other competent authorities continue to govern the matters entrusted to them under their enabling laws, and this Framework addresses the distinct subject of national digital infrastructure assurance.

5. Commencement

This Framework shall take effect on such date as may be approved and published by the National Information Technology Development Agency. The Agency may prescribe transitional arrangements and implementation timelines for specific provisions of this Framework where necessary.

6. Objectives

The objectives of this Framework are to:

a. establishes Nigeria's national digital infrastructure assurance framework, with NDIAF Assurance Certification as the principal mechanism for demonstrating conformity, for providers serving Public Institutions, regulated sectors,

operators of Critical Information Infrastructure, critical digital infrastructure supporting essential national services, and other designated organisations;

b. defines clear classes of NDIAF Assurance Certification, together with the eligibility, technical, operational, and governance requirements applicable to each class;

c. establishes a risk-based, continuous assurance regime, with workload assurance endorsements for providers seeking to serve Public Institutions and to host sensitive, critical, or strategic workloads;

d. promotes secure, resilient, trusted, and investment-ready digital infrastructure ecosystems, including the development of indigenous digital infrastructure capacity;

e. facilitates the onboarding of Certified Providers onto the Digital Regulatory Platform (DRP) and support trusted provider discovery across the national digital economy;

f. recognises internationally accepted standards, certifications, and independent conformity assessments as technical assurance, while focusing the Agency's oversight on Nigeria-specific regulatory obligations;

g. strengthen confidence in Nigeria's digital infrastructure ecosystem through continuing, risk-based regulatory supervision by the Agency, in cooperation with other competent authorities; and

h. supports the implementation of the National Sovereign Cloud Initiative, national and sector-specific data localisation objectives, the protection of Critical Information Infrastructure, trusted government procurement, the National Cloud Computing Guideline, and the National Cloud Technical Guideline.

7. Scope and Applicability

7.1 This Framework establishes Nigeria's national assurance, conformity, and oversight framework for cloud services and digital infrastructure, comprising NDIAF Assurance Certification, workload assurance endorsements, and the assessment, supervision, and enforcement mechanisms set out in this Framework. The providers and institutions to which this Framework applies are set out in Section 7.2.

7.2 This 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 the Agency, in each case to the extent that they provide data centre services, cloud services, or integration services supporting Public Institutions, Regulated Sectors, operators of Critical Information Infrastructure, critical digital infrastructure supporting essential national services, and other high-impact organisations designated by the Agency. NDIAF Assurance Certification becomes applicable to such providers as follows:

a. Public Institutions including Federal Public Institutions and State and Local Government institutions that adopt this Framework or are designated under it shall procure and utilise data centre services, cloud services, and integration services only from providers holding valid NDIAF Assurance Certification of the class, and with the workload assurance endorsements, appropriate to the relevant workload classification;

b. NDIAF Assurance Certification constitutes the national assurance baseline for Regulated Sector Workloads. The Agency shall work collaboratively with relevant sector regulators to facilitate its recognition and integration within sector-specific regulatory and supervisory frameworks, while respecting the statutory mandates of the respective competent authorities.

c. operators of Critical Information Infrastructure, and operators of critical digital infrastructure supporting essential national services, shall utilise NDIAF-certified providers where certification is required under applicable national critical infrastructure protection requirements or sector-specific obligations; and

d. organisations designated by the Agency, or by another competent authority in coordination with the Agency, as requiring trusted digital infrastructure services shall utilise NDIAF-certified providers in accordance with the terms of the designation.

7.3 A provider seeking to serve the institutions, sectors, or workloads described in Section 7.2 shall obtain and maintain the NDIAF Assurance Certification of the

appropriate class, together with any applicable workload assurance endorsement, before providing the relevant services.

7.4 Providers that do not serve the institutions, sectors, or workloads described in Section 7.2 are not required to obtain an NDIAF Assurance Certification. Such providers remain eligible to obtain Certification under this Framework and, upon certification, shall assume the same obligations and enjoy the same recognition as Certified Providers of the applicable Certification Class. Nothing in this Framework shall be construed as requiring every provider of cloud or digital infrastructure services in Nigeria to obtain an NDIAF Assurance Certification, unless otherwise required under this Framework or any other applicable law or regulatory instrument.

7.5 For the purposes of this Framework: Managed Service Providers shall obtain the Service Integration Provider Certification in respect of the management, operation, or support of cloud and digital infrastructure services on behalf of another entity, or the Cloud Service Provider Certification where they provide cloud services in their own right; and Artificial Intelligence Infrastructure Providers and Sovereign Compute Providers shall obtain the Cloud Infrastructure Provider Certification, the Cloud Service Provider Certification, or both, according to the nature of their activities, together with such endorsements as the Agency may prescribe for artificial intelligence and sovereign compute infrastructure.

7.6 Nothing in this Framework shall be construed as negating, waiving, replacing, or otherwise affecting any licence, permit, or authorisation required under the exclusive licensing jurisdiction of another competent authority, including the Central Bank of Nigeria, the Nigerian Communications Commission, and other sector regulators. An NDIAF Assurance Certification does not substitute for, and holding or complying with this Framework does not relieve a provider of, any obligation to obtain or maintain such other licence, permit, or authorisation.

7.7 Nothing in this Framework shall be construed as replacing, limiting, or superseding the statutory mandates of any competent authority, including authorities responsible for telecommunications, electricity, environmental protection, building standards, public procurement, data protection, cybersecurity, financial services, or national security. The Agency shall, where appropriate, collaborate with such authorities including through memoranda of understanding, mutual recognition arrangements, information sharing, and coordinated

assessments and inspections, to facilitate the effective and non-duplicative implementation of this Framework. The Agency shall seek mutual recognition of assurance outcomes with sector regulators wherever appropriate, so that a provider is assessed once, and the outcome is recognised many times.

8. Definitions

In this Framework, unless the context otherwise requires:

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

"Availability Zone" means one or more discrete data centre facilities within a Deployment Region, with independent power, cooling, and networking, designated by a Cloud Service Provider for the purposes of service resilience and fault isolation.

"Certification Class" means a class of NDIAF Assurance Certification established under Section 9.2, including any sub-class established under this Framework.

"Certified Provider" means a person or organisation holding a valid NDIAF Assurance Certification issued under this Framework.

"Cloud Infrastructure Provider (CIP)" means a person or organisation responsible for the establishment, management, operation, or provision of data centre facilities and related physical digital infrastructure, including colocation, hosting, power, cooling, and intra-facility connectivity services.

"Cloud Service Provider (CSP)" means a person or organisation that provides cloud computing services, including infrastructure, platform, software, storage, or other cloud-based services, whether delivered from infrastructure it owns or from infrastructure operated by a Cloud Infrastructure Provider holding an NDIAF Assurance Certification.

"Continuous Assurance" means the lifecycle of regulatory assurance established under this Framework, comprising initial certification, annual surveillance, periodic reassessment, incident reporting, compliance monitoring, material change

notification, risk-based inspection, corrective action, and, where necessary, suspension or withdrawal of certification.

"Critical Information Infrastructure (CII)" means critical national information infrastructure within the meaning of Section 3 of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, as amended, and includes any asset, system, or network designated as such under the Designation and Protection of Critical National Information Infrastructure Order, 2024, as such other order made pursuant to that Act.

"Critical Workloads" means systems, applications, data, or digital services whose compromise, unavailability, or disruption could have a significant adverse impact on national security, public safety, critical infrastructure, economic stability, or the delivery of essential services.

"Data Centre Operator" means a person or organisation responsible for the establishment, management, operation, or provision of data centre infrastructure and services, and, for the purposes of this Framework, certified as a Cloud Infrastructure Provider.

"Data Classification Framework" means the data classification scheme set out in Schedule A to the National Cloud Computing Guideline, as may be revised from time to time, by reference to which workloads are classified and NDIAF Assurance Certifications and workload assurance endorsements are issued under this Framework.

"Deployment Region" means a defined geographic area within the territory of the Federal Republic of Nigeria, comprising one or more Availability Zones, from which a Cloud Service Provider delivers cloud services under an NDIAF Assurance Certification issued pursuant to this Framework.

"Design Assurance Review (DAR)" means a pre-deployment conformity review conducted by the Agency to assess whether a proposed facility or infrastructure is capable of achieving NDIAF Assurance Certification. A Design Assurance Review supports certification readiness only; it does not constitute planning approval, and it does not replace any environmental, telecommunications, energy, construction, or other approval required under applicable laws.

"Digital Infrastructure" means the physical and virtual infrastructure that enables the storage, processing, transmission, management, and delivery of digital services,

including data centres, cloud infrastructure, compute infrastructure, networks, and supporting systems.

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

"Enhanced Workload Assurance (EWA)" means a workload assurance endorsement issued by the Agency and endorsed on an NDIAF Assurance Certification, confirming that a Certified Provider has demonstrated compliance with the enhanced technical, operational, security, and governance requirements necessary to support Government Workloads, Sensitive Workloads, and Regulated Sector Workloads at the corresponding classification levels.

"Federal Public Institution (FPI)" has the meaning assigned to it under applicable laws and regulations, and includes Ministries, Departments, Agencies, and other public institutions of the Federal Government.

"Financial Assurance" means an irrevocable on-demand bank guarantee or a performance bond, in the form and amount prescribed under Section 9.12 and Schedule 1, maintained as security for the performance of obligations under this Framework by a Certified Provider holding a Sovereign Workload Assurance endorsement or designated as systemically significant.

"Government Workloads" means data, systems, applications, platforms, or services owned, operated, managed, or utilised by Public Institutions.

"Integrated Digital Infrastructure Provider (IDIP)" means a person or organisation holding the Integrated Digital Infrastructure Provider Certification (Tier 1), covering the provision of data centre services, cloud services, and integration services on an integrated basis.

"Internationally Recognised Certification" means a certification or standard recognised by the Agency as evidence of compliance with specified requirements under this Framework.

"Managed Service Provider (MSP)" means a provider responsible for managing, operating, monitoring, or supporting digital infrastructure or cloud services on behalf of another entity, certified under this Framework in accordance with Section 7.5.

"National Assurance Baseline" means the body of Nigerian regulatory assurance requirements established by this Framework and consolidated in Schedule 2, with which NDIAF Assurance Certification certifies conformity, and which applies alongside and is evidenced separately from the internationally recognised technical certifications recognised under Part 16.

"National Register of Certified Providers" means the register established and maintained by the Agency under Section 9.1, recording all valid NDIAF Assurance Certifications, their Certification Classes, workload assurance endorsements, conditions, and status.

"NDIAF Assurance Certification" means the certification granted by the Agency under this Framework, being the Agency's formal confirmation that the holder conforms with the requirements of this Framework including the regulatory, governance, sovereignty, localisation, resilience, and public interest requirements applicable to the relevant Certification Class and is subject to the Agency's continuous regulatory oversight, subject to the conditions endorsed on the certification.

"Nigerian Regulatory Assurance Requirements" means the Nigeria-specific assurance requirements consolidated in Schedule 2 to this Framework, covering digital sovereignty, data residency and localisation, governance and accountability, operational resilience and continuity, regulatory reporting and transparency, national security interfaces, public interest and customer protection, and participation in continuous assurance.

"Provider" means any person or organisation subject to this Framework.

"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.

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

"Regulated Sector Workloads" means workloads, systems, data, applications, or services within a designated Regulated Sector that are subject to the oversight of

the relevant sector regulator, classified in accordance with the Data Classification Framework.

"Risk-Based Assessment" means an assessment approach that applies requirements proportionate to the risks, criticality, and nature of the services being provided.

"Sensitive Workloads" means systems, applications, data, or digital services that process, store, or transmit information requiring enhanced confidentiality, integrity, availability, or regulatory protection due to their potential impact on operations, citizen privacy, public trust, or national interests.

"Service Integrator (SI)" means a provider responsible for integrating, deploying, or managing digital infrastructure or cloud services on behalf of another entity, operating as a partner of, or under authorisation from, one or more Cloud Service Providers holding an NDIAF Assurance Certification.

"Sovereign Compute" means computing infrastructure designed, deployed, and operated in a manner that preserves Nigerian jurisdictional control, security, resilience, and governance requirements for sensitive, critical, artificial intelligence, high-performance computing, or strategically important workloads.

"Sovereign Compute Provider" means a provider of computing infrastructure specifically designed, designated, or authorised to support sovereign, sensitive, critical, artificial intelligence, high-performance computing, or other strategically important workloads, certified under this Framework in accordance with Section 7.5.

"Sovereign Infrastructure" means digital infrastructure that satisfies prescribed requirements relating to Nigerian jurisdictional control, data residency, operational and administrative control, security, resilience, auditability, and compliance with applicable laws, regulations, standards, and national interests.

"Sovereign Workload Assurance (SWA)" means a workload assurance endorsement issued by the Agency and endorsed on an NDIAF Assurance Certification, confirming that a Certified Provider has demonstrated compliance with the enhanced requirements prescribed for hosting, processing, or supporting critical and strategic workloads and digital services.

"Strategic Workloads" means systems, applications, data, or digital services designated by the Federal Government as being of strategic importance to national

development, economic security, technological sovereignty, or public service delivery. For the purposes of this Framework, Critical Workloads correspond to Level 4, and Sensitive Workloads correspond to Levels 3 and 2 of the Data Classification Framework. Strategic Workloads constitute a designation applied by the Federal Government across classification levels.

"Workload" means an application, system, dataset, service, or computing process hosted or executed on digital infrastructure.

"Workload Assurance Endorsement" means an Enhanced Workload Assurance (EWA) endorsement or a Sovereign Workload Assurance (SWA) endorsement issued under Part 14 and endorsed on an NDIAF Assurance Certification.

9. The NDIAF Assurance Certification Framework

9.1 Establishment and Administration

a. The Agency shall establish and administer NDIAF Assurance Certification, together with the conformity assessment, workload assurance, continuous assurance, and compliance monitoring mechanisms of this Framework, for the certification and supervision of digital infrastructure and cloud service providers within its scope.

b. The Agency shall establish and maintain a National Register of Certified Providers.

c. NDIAF Assurance Certification constitutes Nigeria's national digital infrastructure assurance baseline and the recognised assurance pathway for providers serving Public Institutions, regulated sectors, operators of Critical Information Infrastructure, and other designated organisations, and is the assurance mechanism contemplated under the National Cloud Computing Guideline and the National Cloud Technical Guideline.

d. In accordance with Sections 7.2 and 7.3, and subject to the transitional provisions of this Framework, a provider shall not provide data centre services, cloud services, or integration services to a Public Institution, to a Regulated Sector entity in respect of Regulated Sector Workloads where sector-specific instruments so require, to an operator of Critical Information Infrastructure where certification is required under applicable critical infrastructure protection requirements, or to an organisation designated under Section

7.2(d), except while holding a valid NDIAF Assurance Certification of the appropriate class issued under this Framework.

e. The NDIAF Assurance Certification:

   i. confirms conformity with the national assurance requirements of this Framework applicable to the relevant Certification Class, including the Nigerian Regulatory Assurance Requirements consolidated in Schedule 2;

   ii. confirms the Certified Provider's participation in the continuous assurance regime established under Section 9.14;

   iii. confers recognition as a trusted provider through listing on the National Register of Certified Providers and the Digital Regulatory Platform, with publicly verifiable certification status;

   iv. establishes eligibility to serve Public Institutions in accordance with Section 7.2(a), and constitutes the recognised national assurance baseline for adoption within Regulated Sectors and for Critical Information Infrastructure in accordance with Sections 7.2(b) and 7.2(c);

   v. streamlines procurement by enabling Public Institutions and regulated entities to verify certification status and workload assurance endorsements directly through the Digital Regulatory Platform, in place of transaction-by-transaction due diligence; and

   vi. carries with it the recognition of international assurance under Part 16, so that a Certified Provider is not re-assessed on matters already adequately evidenced by recognised international certifications.

f. The requirements prescribed under this Framework constitute the national minimum requirements for the provision of digital infrastructure and cloud services within its scope, and shall not be construed as precluding, limiting, or displacing additional or more stringent requirements prescribed by a competent sector regulator for workloads, services, or entities within its regulatory purview.

g. The requirements of this Framework shall be proportionate to:

   i. the class of NDIAF Assurance Certification sought or held;

   ii. the nature of the services provided;

   iii. the classification of workloads to be hosted;

iv. the criticality of the infrastructure; and

v. the risks associated with the services being provided.

h. In applying this Framework, the Agency shall prescribe simplified requirements, extended compliance timelines, reduced fees, or adjusted financial requirements for small providers, start-ups, indigenous providers, or providers serving lower-risk workloads, consistent with the risk-based approach of this Framework, including through the sub-classes and reliefs set out in Schedule 1. Regulatory assurance under this Framework shall not unnecessarily inhibit innovation or market entry.

9.2 Classes of NDIAF Certifications

The Agency shall grant NDIAF Assurance Certification in the following Certification Classes:

a. Integrated Digital Infrastructure Provider Certification (Tier 1), covering the provision of data centre services, cloud services, and integration services on an integrated basis;

b. Cloud Infrastructure Provider Certification, covering the establishment and operation of data centres and related physical digital infrastructure;

c. Cloud Service Provider Certification, covering the provision of cloud services from one or more approved Deployment Regions or Availability Zones within Nigeria; and

d. Service Integration Provider Certification, covering the provision of integration services as a partner of, or under authorisation from, one or more Cloud Service Providers holding an NDIAF Assurance Certification.

The Agency may, by regulation or guideline, establish additional Certification Classes, sub-classes, or endorsements where necessary for the effective administration of this Framework, including the Cloud Service Provider Certification (Restricted) sub-class established under Schedule 1.

NDIAF Assurance Certification class summary:

Certification Class	Scope of Certification
Tier 1 — Integrated Digital Infrastructure Provider Certification	Data centre services, cloud services, and integration services (integrated coverage across all three domains).
Cloud Infrastructure Provider Certification	Data centres and related physical digital infrastructure, including colocation, hosting, power, cooling, and intra-facility connectivity.
Cloud Service Provider Certification	Cloud services (IaaS, PaaS, SaaS, and related services) delivered from approved Deployment Regions or Availability Zones within Nigeria.
Service Integration Provider Certification	Integration, deployment, and management of cloud and digital infrastructure services, subject to CSP partnership or authorisation.

9.3 Application Requirements

a. Applications for an NDIAF Assurance Certification shall be submitted to the Agency in the form and manner prescribed, accompanied by the prescribed fee and such supporting documentation as the Agency may require.

b. An applicant shall, at a minimum, submit:

   i. evidence of incorporation and registration in Nigeria, or in such other jurisdiction as the Agency may approve, together with evidence of a registered place of business in Nigeria;

   ii. particulars of ownership, control, and ultimate beneficial ownership;

   iii. a description of the services proposed, the infrastructure and facilities to be used, and, for Cloud Service Provider Certification applicants, the proposed Deployment Regions and Availability Zones where required under Section 12.2;

   iv. evidence of technical, financial, and human resource capacity appropriate to the Certification Class sought;

   v. governance, information security, business continuity, and risk management documentation; and

vi. such other information as the Agency may prescribe.

c. The Agency may request clarification or additional information, and the period for determination of an application shall be suspended pending the applicant's response.

d. The Agency may refuse an application that is incomplete, contains false or misleading information, or fails to satisfy the requirements applicable to the Certification Class sought, and shall communicate the grounds of refusal to the applicant in writing.

9.4 Integrity and Good Standing

a. The Agency shall verify the integrity and good standing of an applicant or Certified Provider, having regard to:

   i. the integrity and honesty of the applicant and its beneficial owners;

   ii. the ownership and control structure of the applicant, including ultimate beneficial ownership;

   iii. the jurisdiction of incorporation and the regulatory environment applicable to the applicant and its beneficial owners;

   iv. any history of regulatory sanctions, criminal convictions, or material legal proceedings involving the applicant or its beneficial owners; and

   v. such other considerations as the Agency may prescribe.

b. Applicants shall submit accurate and complete beneficial ownership information at the time of application and shall notify the Agency of any material change in ownership or control structure within thirty (30) days of such change.

c. The Agency may verify information submitted by an applicant through documentary evidence, independent data sources, corporate registries, regulatory authorities, or other lawful verification mechanisms as it considers appropriate. Any material misrepresentation, false statement, omission, or failure to provide accurate information may constitute grounds for refusal, suspension, or withdrawal of an NDIAF Assurance Certification.

d. The Agency may prescribe additional integrity and good standing requirements applicable to applicants for the Tier 1 Certification, applicants

seeking a Sovereign Workload Assurance, or Certified Providers hosting Critical Workloads.

9.5 Certification Timelines

The Agency shall prescribe and publish timelines governing the certification process, consistently with the service-timeline, transparency, and default-approval provisions of the Business Facilitation (Miscellaneous Provisions) Act, 2023 including:

a. the period within which the Agency shall acknowledge receipt of a complete application;

b. the period within which an assessment shall be completed following receipt of a complete application;

c. the period within which the Agency shall issue a certification decision following completion of assessment;

d. the validity period applicable to each class of NDIAF Assurance Certification;

e. the period within which a renewal application shall be submitted prior to the expiry of an existing NDIAF Assurance Certification; and

f. such other timelines as may be necessary for the orderly administration of this Framework.

9.6 Default Timelines

Until the Agency prescribes specific timelines, the following default timelines shall apply:

a. acknowledgement of application within ten (10) working days of receipt of a complete application;

b. completion of assessment within sixty (60) working days of acknowledgement, subject to the complexity of the assessment and the cooperation of the applicant;

c. certification decision within twenty (20) working days of completion of assessment;

d. validity of each class of NDIAF Assurance Certification is three (3) years, unless otherwise endorsed on the certification; and

e. renewal application should be submitted not less than ninety (90) days prior to expiry.

9.7 Certification Conditions, Variation, and Non-Transferability

a. Each NDIAF Assurance Certification shall define the scope of certification, and the Agency may attach to it such conditions or scope limitations as are necessary to reflect the conformity demonstrated, varying them upon notice to the Certified Provider where the underlying conformity position changes.

b. A Certified Provider may apply to the Agency to vary the scope of its NDIAF Assurance Certification, including the addition of Deployment Regions, Availability Zones, facilities, or service categories, in the form and manner prescribed.

c. An NDIAF Assurance Certification is personal to the Certified Provider and shall not be assigned, transferred, or otherwise disposed of. A successor entity shall apply for its own certification, and the Agency may prescribe an expedited conformity confirmation where the certified operations, facilities, and management systems continue materially unchanged.

d. A change in the control of a Certified Provider, whether by acquisition, merger, or otherwise, shall be notified to the Agency in writing not less than thirty (30) days in advance, or as soon as reasonably practicable where advance notice is not lawfully possible, and shall be subject to the integrity and good standing requirements of this Framework.

e. A Certified Provider shall notify the Agency within seven (7) days of the commencement of any insolvency, receivership, administration, winding-up, or analogous proceeding affecting it, or of any other event that materially impairs its ability to continue certified operations.

f. Upon the occurrence of any such corporate event, the Agency may impose conditions, require the implementation of customer transition arrangements, or suspend or withdraw the NDIAF Assurance Certification, having regard to the continuity of services and the protection of customers.

9.8 Assessment Methodology: Technical Assurance and Regulatory Oversight

a. Assessments under this Framework may include:

i. documentation review;

ii. self-assessment;

iii. technical assessment;

iv. site inspection;

v. security assessment;

vi. operational assessment;

vii. surveillance assessment; and

viii. such other activities as may be prescribed by the Agency.

b. All regulatory decisions under this Framework including the grant, refusal, renewal, variation, suspension, and withdrawal of NDIAF Assurance Certifications and workload assurance endorsements, the determination of compliance status, and the taking of enforcement action shall be exercised exclusively by the Agency through its authorised officers or assigned entities.

c. In discharging its assessment functions, the Agency shall rely on technical assurance in accordance with Part 16, accepting valid, current, and applicable internationally recognised certifications and independent conformity assessment reports as evidence of compliance with corresponding technical requirements, and shall focus its own assessment on Nigeria-specific regulatory obligations.

d. The Agency may engage accredited independent assessors or conformity assessment bodies to support routine surveillance, technical verification, and monitoring activities, acting under the Agency's direction and subject to conditions the Agency prescribes; all resulting regulatory decisions shall remain with the Agency in accordance with paragraph (b).

e. The Agency may undertake independent verification and risk-based inspections at any stage of the assessment process and may coordinate joint assessments with other competent authorities where regulatory responsibilities overlap.

9.9 Operational Manual

Detailed technical requirements, assessment methodologies, scoring criteria, evidence requirements, and operational procedures shall be prescribed through the Operational Manual, issued as Schedule 4 to this Framework and published by the Agency, so that this Framework states the core minimum requirements while implementation detail is elaborated in the Operational Manual. The Operational Manual shall include a process map illustrating the application-to-certification journey and the indicative timelines applicable to each stage and shall not impose obligations inconsistent with this Framework. The Operational Manual is confined to implementation detail: the principles of recognition, proportionality, assessment philosophy, and the risk model are established by this Framework and shall not be varied by the Operational Manual. Wherever this Framework empowers the Agency to prescribe requirements, criteria, thresholds, or procedures, the Agency shall do so through published instruments containing objective criteria and measurable thresholds and shall apply them consistently as between providers in comparable circumstances.

9.10 Digital Regulatory Platform (DRP)

a. The Digital Regulatory Platform (DRP) established under the National Cloud Computing Guideline shall serve as the operational backbone of this Framework and the authoritative repository of Certified Providers that have satisfied the requirements prescribed under this Framework.

b. The DRP shall support:

   i. certification applications and renewals;

   ii. regulatory reporting and annual returns;

   iii. surveillance and compliance monitoring;

   iv. incident reporting;

   v. public verification of Certified Providers and their certification status;

   vi. publication of Enhanced Workload Assurance (EWA) endorsements and Sovereign Workload Assurance (SWA) endorsements;

   vii. implementation guidance; and

   viii. trusted provider discovery by Public Institutions, regulated sectors, and other customers.

c. Listing on the DRP shall be subject to the continued validity of the Certified Provider's NDIAF Assurance Certification.

d. Listing on the DRP shall automatically lapse where the underlying NDIAF Assurance Certification:

   i. expires;

   ii. is suspended;

   iii. is withdrawn; or

   iv. otherwise ceases to be valid.

e. The Agency may prescribe additional onboarding, operational, and reporting requirements for participation on the DRP.

9.11 Surrender of Certification and Market Exit

a. A Certified Provider may surrender its NDIAF Assurance Certification, in whole or in part, by giving the Agency not less than ninety (90) days' written notice, or such other period as may be endorsed on the certification.

b. A surrender takes effect on the date stated in the notice or, if later, upon completion of the exit obligations in this Section, and the Agency shall record the surrender on the National Register of Certified Providers and the Digital Regulatory Platform.

c. Before ceasing certified operations, a Certified Provider shall submit to the Agency, and implement, a customer transition plan providing for:

   i. advance notice to affected customers;

   ii. reasonable migration support;

   iii. return of customer data in a commonly used, machine-readable format;

   iv. secure deletion of customer data following migration, in accordance with applicable law; and

   v. continuity arrangements for critical services during the transition.

d. Surrender or market exit shall not discharge any liability or obligation accrued prior to the effective date of surrender.

e. The obligations of this Section shall apply, so far as applicable, where an NDIAF Assurance Certification expires without renewal or is withdrawn.

9.12 Financial Capacity, Capital, and Financial Assurance

a. The Agency may prescribe, for each class of NDIAF Assurance Certification, minimum financial capacity requirements, professional indemnity and cyber liability insurance levels, and, where applicable under paragraph (d), Financial Assurance requirements, through a schedule published as a subsidiary instrument to this Framework. Schedule 1 to this Framework sets out the requirements applicable at commencement.

b. The purpose of the financial requirements prescribed under this Section is to provide evidence that a provider possesses sufficient financial capacity and operational sustainability to sustain critical digital infrastructure operations and to meet its obligations including its customer protection, service continuity, and market exit obligations throughout the certification lifecycle. The financial requirements are not intended to create barriers to market entry and shall be applied proportionately. The Agency does not conduct prudential supervision under this Framework: it does not supervise solvency, does not monitor capital adequacy on a continuing basis, and does not assess financial performance. Financial capacity is assessed at certification and renewal solely as evidence of a provider's ability to sustain certified operations, to discharge its service continuity, customer transition, and market exit obligations, and to protect the continuity of Government and regulated sector services and sovereign workloads and, for Sovereign Workload Assurance holders and systemically significant providers, to support the Financial Assurance required under paragraph (d). No financial requirement under this Framework serves any purpose beyond these.

c. For every Certification Class, the financial requirements shall comprise evidence of financial capacity appropriate to the Certification Class; professional indemnity insurance; cyber liability insurance; demonstrated business continuity capability; and financial sustainability appropriate to the scale and criticality of the services provided.

d. In addition to the requirements of paragraph (c), a Certified Provider holding or seeking a Sovereign Workload Assurance endorsement or designated by the Agency as providing systemically significant services, shall maintain Financial Assurance in the amount prescribed in Schedule 1, in the form of an irrevocable on-demand bank guarantee or a performance bond issued by a

qualifying institution specified in Schedule 1. No other instrument shall satisfy the Financial Assurance requirement.

e. The Agency may call upon Financial Assurance maintained under this Section, in accordance with the procedure set out in Schedule 1, to satisfy unmet customer transition, data migration, or market exit obligations under Sections 9.11 and 19, outstanding financial obligations to the Agency, or amounts payable to affected customers pursuant to a determination of the Agency. Affected customers may submit claims against the Financial Assurance in accordance with the prescribed procedure without prejudice to the jurisdiction of the courts or to any contractual remedy available to the customer.

f. Minimum financial capacity may be evidenced by audited financial statements; by a current audited or independently reviewed statement of paid-up capital; by a parent company guarantee supported by group audited financial statements; or by a banker's confirmation of capital injection, so that newly incorporated entities, greenfield ventures, and funded start-ups with demonstrable capital are not excluded by the absence of a multi-year audit history.

g. The Agency shall review the financial requirements prescribed under this Section at least once every two (2) years, and may adjust them to reflect macroeconomic conditions, inflation, exchange rate movements, and market developments, through republication of the schedule without requiring amendment of this Framework.

h. The Agency may grant proportionate relief from the financial requirements including reduced amounts, extended build-up periods, or adjusted instruments for small providers, start-ups, indigenous providers, and providers operating facilities in underserved geopolitical zones, in accordance with Schedule 1.

9.13 Certification Process Overview

The certification journey comprises the following stages, the detailed process map and timelines for which shall be set out in the Operational Manual:

Stage	Description
1. Application	Submission of the application, prescribed documentation, and fee, through the Digital Regulatory Platform or such other channel as the Agency may prescribe.
2. Assessment	Documentation review and technical, security, and operational assessment, leveraging recognised technical assurance in accordance with Part 16.
3. Inspection	Site inspection of relevant facilities by the Agency's authorised officers, where applicable.
4. Decision	Grant or refusal of the NDIAF Assurance Certification, with written grounds communicated to the applicant.
5. Certification Grant and Onboarding	Issuance of the NDIAF Assurance Certification, endorsement of any workload assurance endorsements, and listing on the Digital Regulatory Platform.
6. Surveillance	Ongoing reporting, annual returns, attestations, audits, and risk-based inspections proportionate to the Certified Provider's risk profile.
7. Renewal	Renewal application not less than ninety (90) days before expiry, with reassessment as required.

9.14 Continuous Assurance Lifecycle

Certification under this Framework is not a one-time assessment. Each NDIAF Assurance Certification is granted, maintained, and supervised through a continuous assurance lifecycle comprising:

a. initial certification;

b. annual surveillance;

c. periodic reassessment, including at renewal;

d. incident reporting in accordance with Part 18;

e. compliance monitoring and regulatory reporting;

f. notification of material changes;

g. risk-based inspections;

h. corrective action plans;

i. suspension of certification, where warranted; and

j. withdrawal of certification, where necessary.

The obligations of the continuous assurance lifecycle apply throughout the validity of each NDIAF Assurance Certification, and conformity is assessed on a continuing basis rather than solely at the point of grant or renewal. The intensity of the lifecycle is proportionate, not uniform: surveillance frequency, reporting obligations, evidence requirements, and audit intensity differ by Certification Class and risk profile, in accordance with Section 18.3 and the Operational Manual.

9.15 The Three-Stage Assurance Model

Assurance under this Framework proceeds in three stages, which together define the assessment philosophy of the NDIAF:

Stage	What Happens	Where Prescribed
Stage 1: Recognition	Internationally recognised certifications and independent conformity assessments are verified and mapped, and the requirements they adequately evidence are accepted without reassessment.	Part 16; Schedule 3
Stage 2: Nigerian Conformity Assessment	The Agency assesses conformity with the Nigerian Regulatory Assurance Requirements the matters international certifications do not assess.	Schedule 2; Section 16.3
Stage 3: Continuous Assurance	The Certified Provider remains within the continuous assurance lifecycle, at the surveillance intensity applicable to its Certification Class and risk profile.	Sections 9.14, 18.3

The three stages apply, with necessary modifications, at initial certification, at renewal, and in surveillance. Nothing assessed and accepted at Stage 1 is reassessed at Stage 2 or Stage 3, except where there is reasonable cause or material risk.

10. Integrated Digital Infrastructure Provider Certification — Tier 1

10.1 Scope of Certification

a. The Integrated Digital Infrastructure Provider Certification is the Tier 1, omnibus NDIAF Assurance Certification under this Framework, certifying the Certified Provider for the provision of data centre services, cloud services, and integration services on an integrated basis within Nigeria.

b. A Tier 1 Certified Provider shall be subject to the requirements applicable to the Cloud Infrastructure Provider Certification, the Cloud Service Provider Certification, and the Service Integration Provider Certification in respect of each corresponding domain of its operations, in addition to the requirements set out in this Part.

c. A Tier 1 Certified Provider shall not be required to hold a separate Cloud Infrastructure Provider Certification, Cloud Service Provider Certification, or Service Integration Provider Certification in respect of activities covered by its Tier 1 Certification. The Tier 1 Certification provides a single consolidated assessment, a single certification relationship with the Agency, and consolidated fees for providers operating across all three domains.

10.2 Eligibility Criteria

An applicant for the Tier 1 Certification shall:

a. be duly incorporated in Nigeria, or in such other jurisdiction as the Agency may approve, and maintain a registered place of business in Nigeria;

b. demonstrates established technical, operational, and financial capacity to operate concurrently across the data centre, cloud services, and integration services domains;

c. owns, operate, or have secured enforceable rights over data centre facilities and cloud infrastructure within Nigeria sufficient to support the services proposed;

d. demonstrates a track record of operating digital infrastructure or cloud services at scale, or such equivalent evidence of capability as the Agency may accept;

e. satisfies the integrity and good standing requirements of this Framework, including in respect of ultimate beneficial ownership; and

f. satisfies the minimum capitalisation, Financial Assurance, and professional indemnity and cyber liability insurance requirements prescribed for the Tier 1 Certification under Section 9.12 and Schedule 1.

10.3 Technical Standards

A Tier 1 Certified Provider shall:

a. comply with the physical infrastructure, security, and resilience standards applicable to Cloud Infrastructure Providers under Part 11 in respect of each data centre facility it operates;

b. comply with the deployment, data residency, availability, and interoperability requirements applicable to Cloud Service Providers under Part 12 in respect of each cloud service it provides;

c. comply with the integration, interoperability, and security requirements applicable to Service Integration Providers under Part 13 in respect of each integration service it provides;

d. implement and maintain an information security management system aligned with internationally recognised standards, covering all certified domains of its operations;

e. maintain segregation of environments, access controls, and audit logging across its data centre, cloud, and integration operations; and

f. comply with the National Cloud Technical Guideline and such other technical standards as the Agency may prescribe.

10.4 Operational Compliance

A Tier 1 Certified Provider shall:

a. maintain documented operational procedures, service management processes, and business continuity and disaster recovery arrangements covering all certified domains;

b. meet the energy resilience and Power Usage Effectiveness benchmarks prescribed under the National Cloud Technical Guideline in respect of its data centre operations;

c. maintain incident management arrangements and report significant incidents to the Agency within prescribed timelines;

d. publish and honour service level commitments appropriate to the services provided; and

e. maintain records sufficient to demonstrate continued compliance with this Framework across all certified domains.

10.5 Governance Obligations

A Tier 1 Certified Provider shall:

a. maintain a governance structure with clear accountability for regulatory compliance across each certified domain, including a designated senior officer responsible for compliance with this Framework;

b. establish and maintain enterprise risk management, conflict of interest management, and supply chain risk management arrangements;

c. disclose and document all third-party dependencies, sub-processors, and sub-infrastructure arrangements material to its certified operations;

d. notify the Agency of any material change affecting its NDIAF Assurance Certification, including changes in ownership, control, infrastructure location, architecture, data residency arrangements, or third-party dependencies; and

e. comply with applicable data protection, cybersecurity, and sector-specific regulatory obligations.

10.6 Audit and Inspection

a. The Agency shall have the right, exercisable through its authorised officers, to audit, inspect, and verify the compliance of a Tier 1 Certified Provider with this Framework, including through scheduled audits, surveillance assessments, and unannounced risk-based inspections of any facility, system, or record within the scope of the certification.

b. A Tier 1 Certified Provider shall grant the Agency's authorised officers access to its facilities, systems, records, and personnel for the purposes of any audit or inspection and shall cooperate fully with such activities.

10.7 Renewal, Suspension, and Withdrawal

a. The Tier 1 Certification shall be valid for the period prescribed under Part 9 and shall be renewable upon application, payment of the prescribed fee, and demonstration of continued compliance with this Framework.

b. The Agency may suspend or withdraw the Tier 1 Certification, in whole or in respect of one or more certified domains, in accordance with Part 18 of this Framework.

c. Where the Tier 1 Certification is suspended or withdrawn in respect of one domain only, the Certified Provider's certification in respect of the remaining domains shall continue, subject to such conditions as the Agency may impose.

11. Cloud Infrastructure Assurance Certification

11.1 Scope of Certification

a. The Cloud Infrastructure Provider Certification confirms that the Certified Provider has demonstrated conformity with the requirements of this Framework applicable to the establishment and operation of data centre facilities and related physical digital infrastructure within Nigeria, including colocation, hosting, power, cooling, intra-facility connectivity, and supporting infrastructure services.

b. Connectivity within the scope of this certification is limited to intra-facility interconnection and cross-connection within a certified facility. Nothing in this Part requires an NDIAF Assurance Certification for, or extends the Agency's authority to, communications services or network facilities licensable under the Nigerian Communications Act, 2003, and the Agency shall pursue mutual recognition arrangements with the Nigerian Communications Commission in respect of facilities subject to both regimes.

11.2 Eligibility Criteria

An applicant for the Cloud Infrastructure Provider Certification shall:

a. be duly incorporated in Nigeria, or in such other jurisdiction as the Agency may approve, and maintain a registered place of business in Nigeria;

b. own, operate, or have secured enforceable rights over the data centre facilities to be covered by the certification;

c. demonstrate technical and financial capacity to construct, operate, and maintain data centre infrastructure to the standards prescribed under this Framework, including the financial requirements prescribed under Section 9.12 and Schedule 1;

d. employ or engage qualified personnel with demonstrated expertise in data centre operations, physical security, and facilities management;

e. maintain professional indemnity and cyber liability insurance at the minimum levels prescribed under Schedule 1; and

f. satisfy the integrity and good standing requirements of this Framework.

11.3 Design Assurance Review (Pre-Deployment Conformity Review)

a. An applicant or Certified Provider proposing to establish new data centre infrastructure shall, prior to the commencement of construction or deployment, undergo a Design Assurance Review by the Agency. The purpose of the review is to assess whether the proposed facility or infrastructure is capable of achieving NDIAF Assurance Certification, and to support certification readiness.

b. A Design Assurance Review may be completed, and a confirmation of design conformity issued, on the basis of:

   i. design specifications;

   ii. proposed operational arrangements;

   iii. security architecture;

   iv. business continuity planning;

   v. governance arrangements; and

   vi. siting criteria covering power, connectivity, physical security, environmental risk, and proximity to demand.

c. A Design Assurance Review does not constitute planning approval or authorisation to commence operations; it does not replace any environmental, telecommunications, energy, or construction approval required under other applicable laws; and it does not guarantee that an NDIAF Assurance Certification will be granted.

11.4 Technical Standards: Physical Infrastructure, Security, and Resilience

A Cloud Infrastructure Provider shall, in respect of each certified facility:

a. satisfy baseline physical infrastructure standards, including redundancy of power, cooling, and connectivity appropriate to the facility's designated resilience tier;

b. implement physical security controls, including perimeter security, access control, surveillance, and visitor management;

c. implement environmental controls and fire detection and suppression systems consistent with internationally recognised data centre standards;

d. meet the energy resilience and Power Usage Effectiveness benchmarks prescribed under the National Cloud Technical Guideline;

e. implement an information security management system aligned with internationally recognised standards; and

f. comply with the National Cloud Technical Guideline and such other technical standards as the Agency may prescribe.

11.5 Operational Compliance

A Cloud Infrastructure Provider shall:

a. maintain documented operational procedures, maintenance schedules, and capacity management arrangements for each certified facility;

b. maintain business continuity and disaster recovery arrangements, including tested recovery procedures;

c. maintain incident management arrangements and report significant incidents affecting the confidentiality, integrity, availability, or resilience of certified infrastructure to the Agency within prescribed timelines;

d. publish and honour service level commitments to customers hosted within its facilities; and

e. maintain records of operations, maintenance, incidents, and access sufficient to demonstrate continued compliance.

11.6 Governance Obligations

A Cloud Infrastructure Provider shall:

a. maintain a governance structure with a designated senior officer responsible for compliance with this Framework;

b. establish and maintain risk management and supply chain risk management arrangements, including in respect of critical equipment and vendors;

c. disclose and document all third-party dependencies material to the operation of certified facilities;

d. notify the Agency of any material change affecting its NDIAF Assurance Certification, including changes in ownership, control, facility location, or infrastructure architecture; and

e. comply with applicable environmental, building, safety, energy, data protection, and cybersecurity requirements administered by other competent authorities.

11.7 Audit and Inspection

a. The Agency shall have the right, exercisable through its authorised officers, to audit and inspect any certified facility, system, or record of a Cloud Infrastructure Provider, including through scheduled audits, surveillance assessments, and unannounced risk-based inspections.

b. A Cloud Infrastructure Provider shall grant the Agency's authorised officers access to its facilities, systems, records, and personnel for the purposes of any audit or inspection, and shall cooperate fully with such activities.

11.8 Renewal, Suspension, and Withdrawal

a. The Cloud Infrastructure Provider Certification shall be valid for the period prescribed under Part 9 and shall be renewable upon application, payment of

the prescribed fee, and demonstration of continued compliance with this Framework.

b. The Agency may suspend or withdraw the Cloud Infrastructure Provider Certification, in whole or in respect of one or more facilities, in accordance with Part 18 of this Framework.

12. Cloud Service Provider Certification

12.1 Scope of Certification

a. The Cloud Service Provider Certification confirms that the Certified Provider has demonstrated conformity with the requirements of this Framework applicable to the provision of cloud computing services within Nigeria, including infrastructure, platform, software, storage, and related cloud-based services.

b. Where the Certified Provider hosts Government Workloads, Regulated Sector Workloads, or workloads of Critical Information Infrastructure operators or designated organisations, the Cloud Service Provider Certification shall specify, within its certified scope, the Deployment Region or Regions, and the Availability Zone or Zones within each Deployment Region, from which those services are delivered.

c. A Cloud Service Provider shall not deliver cloud services to Public Institutions or regulated sectors from any facility outside its approved Deployment Regions and Availability Zones, except as expressly approved by the Agency.

d. A Cloud Service Provider may deliver its services from facilities it owns or from facilities operated by a Cloud Infrastructure Provider or a Tier 1 Certified Provider and shall disclose all such hosting arrangements to the Agency.

12.2 Eligibility Criteria

An applicant for the Cloud Service Provider Certification shall:

a. be duly incorporated in Nigeria, or in such other jurisdiction as the Agency may approve, and maintain a registered place of business in Nigeria;

b. where the applicant proposes to host Government Workloads, Regulated Sector Workloads, or workloads of Critical Information Infrastructure

operators or designated organisations, or seeks an Enhanced Workload Assurance or Sovereign Workload Assurance, identify at least one proposed Deployment Region within Nigeria, comprising one or more Availability Zones, from which those services will be delivered;

c. demonstrate technical and financial capacity to deliver cloud services at the scale and availability levels proposed, including the financial requirements prescribed under Section 9.12 and Schedule 1;

d. where paragraph (b) applies, demonstrate that the physical infrastructure underlying each proposed Deployment Region is provided by the applicant under a Cloud Infrastructure or Tier 1 Certification, or by a Cloud Infrastructure Provider or Tier 1 Certified Provider under a disclosed hosting arrangement, including a provider holding provisional status under Section 21.4 during the transitional period;

e. employ or engage qualified personnel with demonstrated expertise in cloud operations, security, and service management;

f. maintain professional indemnity and cyber liability insurance at the minimum levels prescribed under Schedule 1; and

g. satisfy the integrity and good standing requirements of this Framework.

12.3 Deployment Regions and Availability Zones

a. Each Deployment Region and Availability Zone shall be identified within the scope of the certification. A Certified Provider shall notify the Agency of any proposed addition, relocation, or decommissioning of a Deployment Region or Availability Zone not less than thirty (30) days in advance. An addition or relocation takes effect within the certified scope upon notification, subject to conformity assessment where the change materially affects conformity with this Framework; workloads covered by an Enhanced Workload Assurance or Sovereign Workload Assurance shall not be migrated to a new or relocated Availability Zone until its inclusion in the certified scope is confirmed.

b. Each Availability Zone shall consist of one or more discrete facilities with independent power, cooling, and networking, engineered such that the failure of one Availability Zone does not cause the failure of another within the same Deployment Region.

c. A Cloud Service Provider seeking an Enhanced Workload Assurance or Sovereign Workload Assurance shall maintain at least two Availability Zones within Nigeria, or such other resilience configuration as the Agency may approve.

d. A Cloud Service Provider shall maintain and provide to the Agency, upon request, an accurate and current inventory of the facilities constituting each Deployment Region and Availability Zone.

12.4 Data Residency Requirements

A Cloud Service Provider shall, where applicable to the workloads it hosts:

a. host government and regulated sector workloads primarily within the territory of the Federal Republic of Nigeria, in accordance with Part 15 of this Framework;

b. establish and maintain documented data residency arrangements that identify the physical location of all government and regulated sector workloads at all times;

c. obtain the approvals required under Part 15 before any cross-border transfer of government or regulated sector workloads, and comply with applicable data protection and cybersecurity requirements, including the Nigeria Data Protection Act, 2023, in respect of any such transfer; and

d. notify the Agency of any change in data residency arrangements, third-party dependencies, or jurisdictional arrangements that may affect the residency or sovereignty status of hosted workloads.

12.5 Service Availability and Continuity

A Cloud Service Provider shall:

a. publish service level commitments for each cloud service offered, including availability targets, and report service performance to the Agency in the form and at the intervals prescribed;

b. maintain business continuity and disaster recovery arrangements, including tested failover between Availability Zones where more than one Availability Zone is maintained;

c. maintain exit and portability arrangements enabling customers, including Public Institutions and regulated sector entities, to migrate workloads to alternative providers in a timely and non-disruptive manner; and

d. notify affected customers and the Agency of significant service disruptions within prescribed timelines.

12.6 Technical Standards and Compliance

A Cloud Service Provider shall, where applicable:

a. implement and maintain an information security management system aligned with internationally recognised standards;

b. implement tenant isolation, encryption, identity and access management, logging, and monitoring controls appropriate to the services provided and the classification of workloads hosted;

c. comply with the interoperability and portability requirements of the National Cloud Technical Guideline and the Nigerian e-Government Interoperability Framework, where applicable;

d. comply with applicable data protection, cybersecurity, and sector-specific regulatory obligations in respect of the workloads it hosts; and

e. comply with such other technical standards as the Agency may prescribe.

12.7 Governance Obligations

A Cloud Service Provider shall:

a. maintain a governance structure with a designated senior officer responsible for compliance with this Framework;

b. disclose and document all third-party dependencies, sub-processors, and sub-infrastructure arrangements that may affect the sovereignty, residency, security, or availability of hosted workloads;

c. maintain a register of Service Integrators operating as its partners or under its authorisation, and notify the Agency of additions to or removals from that register;

d. notify the Agency of any material change affecting its NDIAF Assurance Certification, including changes in ownership, control, Deployment Regions, Availability Zones, architecture, or hosting arrangements; and

e. establish and maintain supply chain risk management arrangements.

12.8 Audit and Inspection

a. The Agency shall have the right, exercisable through its authorised officers, to audit, inspect, and verify the compliance of a Cloud Service Provider with this Framework, including the facilities constituting its Deployment Regions and Availability Zones, whether such facilities are operated by the Certified Provider or by a Cloud Infrastructure Provider on its behalf.

b. A Cloud Service Provider shall grant, and shall procure that its hosting providers grant, the Agency's authorised officers access to relevant facilities, systems, records, and personnel for the purposes of any audit or inspection and shall cooperate fully with such activities.

12.9 Renewal, Suspension, and Withdrawal

a. The Cloud Service Provider Certification shall be valid for the period prescribed under Part 9 and shall be renewable upon application, payment of the prescribed fee, and demonstration of continued compliance with this Framework.

b. The Agency may suspend or withdraw the Cloud Service Provider Certification, in whole or in respect of one or more Deployment Regions, Availability Zones, or service categories, in accordance with Part 18 of this Framework.

13. Service Integration Provider Certification

13.1 Scope of Certification

a. The Service Integration Provider Certification confirms that the Certified Provider has demonstrated conformity with the requirements of this Framework applicable to the integration, deployment, configuration, migration, and management of cloud and digital infrastructure services on behalf of another entity within Nigeria.

b. A Service Integration Provider shall operate only as a partner of, or under authorisation or licence from, one or more Cloud Service Providers or a Tier 1 Certified Provider, in respect of the cloud services it integrates.

c. The Service Integration Provider Certification shall be required only for entities undertaking the integration, deployment, configuration, migration, or ongoing management of cloud environments for Public Institutions, regulated sectors, operators of Critical Information Infrastructure, or designated organisations, and shall not be required for routine ICT implementation, software development, or professional services that do not involve such activities. Managed Service Providers undertaking such activities shall hold this certification in accordance with Section 7.5. The Agency may issue guidance delineating the activities for which this certification is required.

13.2 Eligibility Criteria

An applicant for the Service Integration Provider Certification shall:

a. be duly incorporated in Nigeria, or in such other jurisdiction as the Agency may approve, and maintain a registered place of business in Nigeria;

b. submit evidence of a valid partnership, authorisation, or licensing arrangement with at least one Cloud Service Provider or Tier 1 Certified Provider, including the scope of services covered by that arrangement;

c. demonstrate technical capacity and qualified personnel with demonstrated expertise in the integration, deployment, and management of the cloud services covered by its partnership arrangements;

d. maintain appropriate professional indemnity insurance at the minimum level prescribed under Schedule 1; and

e. satisfy the integrity and good standing requirements of this Framework.

13.3 Partnership and Authorisation Requirements

a. A Service Integration Provider shall maintain, throughout the validity of its certification, at least one valid partnership, authorisation, or licensing arrangement with a Cloud Service Provider or Tier 1 Certified Provider.

b. A Service Integration Provider shall notify the Agency within thirty (30) days of the commencement, variation, suspension, or termination of any such partnership or authorisation arrangement.

c. Where a Service Integration Provider ceases to hold any valid partnership or authorisation arrangement, its certification shall be deemed suspended until a qualifying arrangement is restored and notified to the Agency, or until the Agency otherwise determines.

d. A Service Integration Provider shall not integrate, deploy, or manage cloud services on behalf of a Public Institution or a regulated sector entity except in respect of services provided by a Certified Provider under this Framework.

13.4 Technical Standards and Operational Compliance

A Service Integration Provider shall:

a. comply with the technical, security, and configuration standards of the Cloud Service Providers whose services it integrates, and with the National Cloud Technical Guideline where applicable;

b. implement secure integration practices, including secure handling of credentials, secrets, and customer data, and the application of least-privilege access in all customer environments;

c. maintain documented project delivery, change management, and quality assurance processes;

d. report to the Agency and to the affected Cloud Service Provider any significant incident arising from its integration activities within prescribed timelines; and

e. maintain records of integration engagements sufficient to demonstrate continued compliance.

13.5 Governance Obligations

A Service Integration Provider shall:

a. maintain a governance structure with a designated officer responsible for compliance with this Framework;

b. maintain confidentiality, conflict of interest, and data protection arrangements in respect of customer engagements;

c. notify the Agency of any material change affecting its certification, including changes in ownership, control, or partnership arrangements; and

d. comply with applicable data protection, cybersecurity, and sector-specific regulatory obligations.

13.6 Audit and Inspection

a. The Agency shall have the right, exercisable through its authorised officers, to audit, inspect, and verify the compliance of a Service Integration Provider with this Framework, including its integration practices, records, and customer engagement documentation.

b. A Service Integration Provider shall grant the Agency's authorised officers access to relevant systems, records, and personnel for the purposes of any audit or inspection and shall cooperate fully with such activities.

13.7 Renewal, Suspension, and Withdrawal

a. The Service Integration Provider Certification shall be valid for the period prescribed under Part 9 and shall be renewable upon application, payment of the prescribed fee, evidence of a subsisting qualifying partnership or authorisation arrangement, and demonstration of continued compliance with this Framework.

b. The Agency may suspend or withdraw the Service Integration Provider Certification in accordance with Part 18 of this Framework.

14. Workload Assurance Endorsements and Classification Mapping

14.1 Enhanced Workload Assurance (EWA)

a. A Certified Provider seeking to provide digital infrastructure or cloud services to Public Institutions, or to host Sensitive Workloads or Regulated Sector Workloads at Levels 2 and 3 of the Data Classification Framework, shall obtain an Enhanced Workload Assurance endorsed on its NDIAF Assurance Certification.

b. The Agency shall prescribe the requirements for the Enhanced Workload Assurance, including:

   i. enhanced security controls;

ii. data sovereignty arrangements;

iii. government workload handling requirements;

iv. personnel security; and

v. supply chain risk management.

c. Requirements applicable to the hosting of Regulated Sector Workloads under an Enhanced Workload Assurance shall be developed and prescribed in consultation with the relevant sector regulator, so that they reflect the supervisory requirements of the sector concerned and avoid duplication of sector-specific obligations.

14.2 Sovereign Workload Assurance (SWA)

a. A Certified Provider seeking to host critical or strategic government or regulated sector workloads shall obtain a Sovereign Workload Assurance endorsed on its NDIAF Assurance Certification.

b. An Enhanced Workload Assurance shall be a prerequisite for the Sovereign Workload Assurance.

c. The Agency shall prescribe the requirements for the Sovereign Workload Assurance, including:

i. critical workload isolation;

ii. enhanced access controls;

iii. jurisdictional arrangements;

iv. sovereign operational requirements;

v. alignment with the protection obligations applicable to designated Critical Information Infrastructure under the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, as amended, in coordination with the Office of the National Security Adviser; and

vi. such other requirements as the Agency may prescribe for critical and strategic workloads.

14.3 Workload Classification and Assurance Mapping

NDIAF Assurance Certifications and workload assurance endorsements issued under this Framework shall correspond to the classification of workloads a Certified Provider

is certified to host, determined in accordance with the Data Classification Framework, as set out below:

Assurance Level	**Corresponding Workload Classification**
NDIAF Assurance Certification (without workload assurance endorsement)	Public and General Workloads (Level 1), including government and regulated sector workloads classified at Level 1
NDIAF Assurance Certification with Enhanced Workload Assurance (EWA)	Sensitive Workloads (Levels 2 and 3), including Government Workloads and Regulated Sector Workloads at those levels
NDIAF Assurance Certification with Sovereign Workload Assurance (SWA)	Critical Workloads (Level 4) and Strategic Workloads

a. A Certified Provider shall not process, store, or host a workload above the classification tier corresponding to its valid NDIAF Assurance Certification and workload assurance endorsements.

b. Public Institutions shall determine the classification of a workload in accordance with the Data Classification Framework prior to procurement and shall procure digital infrastructure and cloud services only from Certified Providers holding an NDIAF Assurance Certification and workload assurance endorsement at or above the tier applicable to that classification.

c. Entities operating within Regulated Sectors shall, in collaboration with the relevant sector regulator, determine the classification of Regulated Sector Workloads in accordance with the Data Classification Framework, and shall procure or utilise digital infrastructure and cloud services only from Certified Providers holding an NDIAF Assurance Certification and workload assurance endorsement at or above the tier applicable to that classification. Regulated Sector Workloads classified at Level 1 require only the base NDIAF Assurance Certification, so that requirements remain proportionate to the sensitivity of the workload rather than the identity of the customer.

d. The Agency may, by directive or guidance issued under this Framework, revise the mapping set out in this Section to reflect updates to the Data Classification Framework.

15. Data Sovereignty and Localisation Requirements

a. A Certified Provider holding an Enhanced Workload Assurance or Sovereign Workload Assurance shall satisfy the following data sovereignty requirements:

   i. primary hosting of government and regulated sector workloads shall be within the territory of the Federal Republic of Nigeria;

   ii. backup and disaster recovery facilities for government and regulated sector workloads shall be located within the territory of the Federal Republic of Nigeria, unless the Agency expressly approves alternative arrangements;

   iii. the Certified Provider shall establish and maintain documented data residency arrangements that identify the physical location of all government and regulated sector workloads at all times;

   iv. cross-border transfer of Government Workloads shall require the prior written approval of the Agency and the relevant Public Institution; cross-border transfer of Regulated Sector Workloads shall require the prior written approval of the Agency, granted in coordination with the relevant sector regulator; and any such transfer shall comply with applicable data protection and cybersecurity requirements, including, in respect of personal data, the cross-border transfer provisions of the Nigeria Data Protection Act, 2023;

   v. the Certified Provider shall maintain exit and portability arrangements enabling Public Institutions and regulated sector entities to migrate workloads to alternative providers in a timely and non-disruptive manner; and

   vi. the Certified Provider shall disclose and document all third-party dependencies, sub-processors, and sub-infrastructure arrangements that may affect the sovereignty, residency, or security of government and regulated sector workloads.

b. A Certified Provider shall notify the Agency of any change in data residency arrangements, third-party dependencies, or jurisdictional arrangements that may affect the data sovereignty status of government and regulated sector workloads.

c. The Agency may prescribe additional data sovereignty requirements for Certified Providers hosting Critical Workloads or Sensitive Workloads, consistent with the National Cloud Computing Guideline and other applicable national policies and instruments. Residency obligations under this Section shall be applied by reference to the classification levels of the Data Classification Framework. For Level 4 and Level 3 workloads, the recovery copy required under the National Coud Technical Guideline shall be maintained at a facility geographically separated from the primary site, in a different geopolitical zone or at such distance as ensures continuity in the event of localised disruption.

d. The Agency shall establish coordination and mutual-reliance arrangements with the Nigeria Data Protection Commission in respect of cross-border transfers involving personal data, so that approvals under this Section and under the Nigeria Data Protection Act, 2023, are administered in a coordinated manner and, where arrangements allow, through a single application. Nothing in this Section shall be construed as limiting the application of applicable data protection laws, including the Nigeria Data Protection Act, 2023.

e. Nothing in this Framework shall be construed as limiting or replacing any data localisation obligation imposed by a sector regulator, including the Central Bank of Nigeria, with respect to payment systems, financial market infrastructures, regulated financial institutions, or payment transaction data. This Framework supports the implementation of such sector-specific localisation requirements by providing an assured national infrastructure base on which they can be met.

f. The localisation requirements of this Section are confined to government, regulated sector, and critical workloads, and are administered as proportionate public-interest measures consistent with Nigeria’s continental and regional commitments on trusted cross-border data flows, including the African Union Data Policy Framework, the ECOWAS Supplementary Act on Personal Data Protection, and Nigeria’s commitments under the AfCFTA Protocol on Digital Trade.

16. Technical Assurance and Recognition of International Certifications

16.1 Technical Assurance and Regulatory Oversight

a. This Framework distinguishes between technical assurance and regulatory oversight. Technical assurance comprises internationally recognised certifications, independent conformity assessments, and technical audits, which verify conformance with technical standards. Regulatory oversight comprises the NDIAF Assurance Certification, compliance monitoring, surveillance, reporting, and enforcement, which this Framework vests in the Agency.

b. Internationally recognised certifications, standards, and independent conformity assessments may be relied upon by applicants and Certified Providers, and shall be accepted by the Agency, as evidence of compliance with the corresponding technical requirements of this Framework. The Agency's assessment shall focus primarily on Nigerian regulatory obligations including digital sovereignty, data residency and localisation, governance, operational resilience, reporting, national security, and other public interest obligations rather than re-assessing matters already independently verified through recognised international assurance mechanisms.

16.2 Recognised Standards and Certifications

a. The Agency may recognise internationally accepted standards and certifications as evidence of compliance with specified requirements under this Framework.

b. Such certifications may include:

   i. Uptime Institute certifications;

   ii. ANSI/TIA-942 certifications;

   iii. ISO/IEC 27001;

   iv. ISO/IEC 27701;

   v. ISO/IEC 22301;

   vi. ISO/IEC 20000;

   vii. PCI DSS;

viii. SOC 2 Type II;

ix. ISO/IEC 42001, as evidence of AI governance and management capability for Certified Providers offering AI infrastructure, sovereign compute services, or AI-enabled cloud services, or hosting government or regulated sector AI workloads; and

x. such other standards and certifications as may be recognised by the Agency.

c. Recognition of an international certification shall not automatically confer an NDIAF Assurance Certification or workload assurance endorsement under this Framework.

d. The Agency shall leverage, and shall not replicate, internationally recognised certifications. Where an applicant or Certified Provider holds a valid, current, and applicable certification recognised in the Recognition and Mapping Schedule, the Agency shall accept it as evidence of compliance with the corresponding technical and operational requirements of this Framework and shall not re-assess matters adequately evidenced by that certification, save for verification of its validity, scope, and applicability.

e. Registration, filing, and audit obligations discharged under the Nigeria Data Protection Act, 2023 including data protection compliance audit filings accepted by the Nigeria Data Protection Commission shall be accepted by the Agency as evidence of compliance with the corresponding data protection requirements of this Framework, and the Agency shall not require duplicative filings in respect of matters adequately evidenced by them.

f. An NDIAF Assurance Certification certifies conformity with the national assurance requirements of this Framework and confers the recognition described in Section 9.1(e). Internationally recognised technical certification schemes retain their own distinct function, and the two operate together in the manner set out in this Part.

g. Recognition of an international certification shall not exempt a Certified Provider from compliance with Nigerian laws, sector-specific regulatory obligations, data sovereignty requirements, or additional assurance requirements prescribed by the Agency.

16.3 Conformity Assessment Workflow

An application for an NDIAF Assurance Certification is assessed through the following workflow, which gives effect to the three-stage assurance model in Section 9.15 and is elaborated in the Operational Manual:

a. the applicant submits its internationally recognised certifications, independent conformity assessment reports, and audit evidence together with its application;

b. the Agency verifies the validity, currency, scope, and applicability of each certification, including, where necessary, with the issuing certification or accreditation body;

c. the Agency maps the verified certifications to the corresponding requirements of this Framework using the Recognition and Mapping Schedule (Schedule 3), and treats the mapped requirements as evidenced without reassessment;

d. a gap assessment is conducted, confined to those requirements of this Framework that are not adequately evidenced by the mapped certifications;

e. the Agency assesses conformity with the Nigerian Regulatory Assurance Requirements consolidated in Schedule 2, which are not addressed by international technical certifications; and

f. upon satisfactory completion, the Agency grants the NDIAF Assurance Certification, recording the recognised certifications relied upon within the certification record.

g. Where internationally recognised certifications adequately demonstrate compliance with corresponding technical requirements, the Agency shall not require reassessment of those requirements, except where there is reasonable cause or material risk. The same workflow applies, with necessary modifications, to surveillance and renewal.

16.4 Recognition and Mapping Schedule

a. The Recognition and Mapping Schedule are issued as Schedule 3 to this Framework. It specifies:

   i. the internationally recognised certifications and standards accepted under this Framework;

ii. the Certification Classes, authorisations, and assessment domains to which each recognised certification or standard applies;

iii. the degree to which each recognised certification or standard satisfies specific assessment requirements, including whether full, partial, or supplementary assessment is required; and

iv. any additional national requirements that must be satisfied notwithstanding the existence of internationally recognised certifications.

b. The Agency shall maintain the Recognition and Mapping Schedule current and may review and republish it in accordance with Schedule 3 without requiring amendment of the main body of this Framework.

c. Nothing in this Framework shall be construed as extending the Agency's authority to matters falling under the statutory jurisdiction of another competent authority.

17. Roles and Responsibilities

17.1 The Agency (NITDA)

The Agency shall:

a. administer and oversee the implementation of this Framework;

b. establish and administer the NDIAF Assurance Certification regime, including the four classes of NDIAF Assurance Certification and the workload assurance endorsements established under this Framework;

c. prescribe application, assessment, authorisation, and surveillance requirements;

d. establish and maintain the National Register of Certified Providers;

e. administer the onboarding of Certified Providers onto the Digital Regulatory Platform (DRP);

f. grant, renew, vary, suspend, and withdraw NDIAF Assurance Certifications and workload assurance endorsements under this Framework;

g. conduct audits, risk-based inspections, surveillance activities, and compliance assessments in accordance with Section 9.8;

h. recognise internationally accepted standards, certifications, and conformity assessments for the purposes of this Framework;

i. prescribe technical, operational, and administrative requirements necessary for the implementation of this Framework;

j. issue operational manuals, directives, advisories, and guidance notes as may be necessary;

k. promote regulatory cooperation, information sharing, and mutual recognition arrangements with competent sector regulators and other relevant authorities including the Nigerian Communications Commission, the Nigeria Data Protection Commission, the Central Bank of Nigeria, and the Office of the National Security Adviser including through memoranda of understanding, joint prescription of regulated sector requirements, coordinated assessments and inspections, and harmonised reporting arrangements; and

l. perform such other functions as may be necessary for the effective implementation of this Framework.

17.2 Certified Providers

Certified Providers shall:

a. comply with the requirements of this Framework, the conditions of their NDIAF Assurance Certifications, and any directives issued by the Agency;

b. maintain the conditions upon which their NDIAF Assurance Certifications and workload assurance endorsements were granted;

c. provide accurate and complete information during application, assessment, and supervision processes;

d. cooperate with the Agency during audits, inspections, and assessments;

e. notify the Agency of any material change affecting their certification or endorsement status;

f. report incidents and significant service disruptions in accordance with applicable requirements;

g. undertake periodic reassessments and surveillance activities as may be prescribed by the Agency;

h. maintain records necessary to demonstrate continued compliance; and

i. comply with such other requirements as may be prescribed by the Agency.

17.3 Public Institutions

Public Institutions shall:

a. procure digital infrastructure and cloud services only from Certified Providers that satisfy the requirements of this Framework, subject to applicable procurement laws and regulations;

b. utilise the Digital Regulatory Platform (DRP) as the primary reference for identifying Certified Providers;

c. ensure that digital infrastructure and cloud deployments comply with applicable NITDA regulatory instruments;

d. cooperate with the Agency in monitoring and compliance activities;

e. ensure that cloud and digital infrastructure projects submitted for IT Project Clearance comply with this Framework; and

f. comply with such other requirements as may be prescribed by the Agency.

17.4 Other Competent Authorities and Regulatory Coordination

a. Nothing in this Framework limits or replaces the statutory responsibilities of sector regulators or any other competent authority.

b. Where a Certified Provider supports regulated sectors, including financial services, payment systems, telecommunications, health, energy, or other designated critical sectors, compliance with the applicable regulatory requirements issued by the relevant sector regulator shall constitute an additional condition of the NDIAF Assurance Certification.

c. The requirements of this Framework constitute the national minimum requirements. Sector regulators retain full independence, in accordance with their respective statutory mandates, to prescribe, administer, and enforce additional or more stringent requirements applicable to workloads, services, or entities within their regulatory purview. Where such requirements materially affect the implementation of this Framework or the national digital infrastructure assurance baseline, the relevant sector regulator should notify and engage the Agency to promote regulatory coordination, consistency, and mutual recognition, as appropriate.

d. Where a sector regulator prescribes additional or more stringent requirements, a Certified Provider shall comply with both the requirements of this Framework and the applicable sector-specific requirements, and, in the event of an overlap, the more stringent requirement shall apply in respect of the workloads within that sector.

e. The Agency shall promote regulatory cooperation, information sharing, and mutual recognition arrangements with other competent authorities, including those responsible for:

   i. financial services;

   ii. telecommunications;

   iii. cybersecurity and national security;

   iv. data protection and privacy;

   v. electricity and energy;

   vi. environmental protection;

   vii. building and safety standards;

   viii. public procurement; and

   ix. such other matters relevant to the implementation of this Framework.

f. Such cooperation may include memoranda of understanding, mutual recognition of assessments and approvals, information sharing, coordinated inspections, joint assessments, harmonised or single-window reporting arrangements, referrals, and other arrangements necessary to facilitate the effective and non-duplicative implementation of this Framework.

g. The Agency shall collaborate with relevant sector regulators to promote regulatory coordination, minimise unnecessary duplication of assurance activities, and facilitate recognition of equivalent assurance outcomes where appropriate, consistent with the respective statutory mandates of the participating authorities.

18. Compliance, Monitoring, Enforcement, and Sanctions

18.1 General Compliance Requirements

a. Certified Providers shall comply with all applicable application, assessment, authorisation, surveillance, and reporting requirements prescribed by the Agency.

b. Public Institutions shall procure digital infrastructure and cloud services in accordance with the requirements of this Framework and other applicable NITDA regulatory instruments.

c. The Agency may issue directives, advisories, and implementation guidance for the effective administration of this Framework.

d. Certified Providers shall notify the Agency of significant incidents affecting the confidentiality, integrity, availability, or resilience of certified infrastructure or services within the timelines prescribed by the Agency and, until such timelines are prescribed, shall provide initial notification of a major incident or significant service disruption within twenty-four (24) hours of becoming aware of it, and a detailed incident report within five (5) working days.

e. The Agency shall establish harmonised incident reporting arrangements with the Nigeria Data Protection Commission and relevant sector regulators, including single-window reporting where agreed, so that a single notification may satisfy corresponding reporting obligations across regimes. Notification under this Framework shall not displace any separate obligation to notify a breach of personal data under the Nigeria Data Protection Act, 2023, or any sector-specific reporting obligation, until such harmonised arrangements are in place.

f. Certified Providers shall notify the Agency of any material change affecting their certification or endorsement status, including changes in ownership, control, infrastructure location, architecture, data residency arrangements, third-party dependencies, international certifications, partnership arrangements, or major security incidents.

g. Certified Providers shall submit to the Agency an annual regulatory compliance return, in the form and manner prescribed by the Agency, not later than ninety (90) days after the end of each calendar year. The return shall include

information on compliance status, material organisational or operational changes, significant incidents, service performance, existing infrastructure capacity, utilisation, planned expansion or upgrade programmes, projected capacity growth, and such other regulatory, operational, or statistical information as the Agency may reasonably require for the administration of this Framework, national digital infrastructure planning, policy development, investment promotion, and ecosystem monitoring.

h. Nothing in this Framework shall prejudice the statutory powers of competent sector regulators. Where regulatory responsibilities overlap, the Agency may coordinate assessments, inspections, reporting, and enforcement actions with the relevant authorities.

18.2 Compliance Status

a. The Agency may classify the compliance status of a Certified Provider as:
   i. Compliant;
   ii. Partially Compliant;
   iii. Materially Non-Compliant; or
   iv. Critically Non-Compliant.

b. The Agency may prescribe the criteria, remediation requirements, and timelines applicable to each compliance status.

c. Compliance obligations under this Framework shall apply to all Certified Providers and shall not be limited to Certified Providers serving Public Institutions and regulated sector.

18.3 Risk-Based Monitoring and Surveillance

a. The Agency shall undertake monitoring and surveillance on a risk-based supervisory model. Certified Providers supporting Government, regulated sectors, Critical Information Infrastructure, or other nationally significant services shall receive enhanced supervisory attention, while lower-risk Certified Providers shall be subject to proportionate regulatory oversight.

b. Surveillance intensity shall differ visibly by Certification Class. Unless the Agency's published supervisory plan prescribes otherwise for a specific Certified Provider on risk grounds:

i. Tier 1 Certified Providers shall undergo an annual surveillance assessment;

ii. Cloud Infrastructure Providers shall undergo a surveillance assessment at least once every eighteen (18) months;

iii. Cloud Service Providers shall be supervised on a risk-based cycle prescribed in the supervisory plan, with at least one surveillance assessment per certification cycle;

iv. holders of the Cloud Service Provider Certification (Restricted) and the Service Integration Provider Certification shall submit an annual self-attestation of continuing conformity and shall be subject to sample-based and for-cause audits rather than routine inspection; and

v. holders of a Sovereign Workload Assurance endorsement shall in all cases receive enhanced surveillance as prescribed for that endorsement.

c. Reporting frequency, evidence requirements, and audit intensity shall likewise be differentiated by Certification Class and risk profile in the Operational Manual, so that the obligations borne by a small or lower-risk Certified Provider are visibly lighter than those borne by a Tier 1 or sovereign-workload provider. The default supervisory profiles are:

Provider Profile	**Surveillance**	**Reporting**	**Audit and Evidence Intensity**
Restricted sub-class and Service Integration (small and SME providers)	Annual self-attestation; sample-based and for-cause audits only	Simplified annual return	Simplified documentary evidence; no routine inspection
Cloud Service and Cloud Infrastructure (standard providers)	Risk-based cycle; at least one surveillance assessment per certification cycle (Cloud Infrastructure: at	Annual return and compliance attestation	Recognised certifications accepted; assessment confined to gaps and Schedule 2

	least every 18 months)		
Providers holding EWA or SWA endorsements (sovereign and endorsed workloads)	Enhanced surveillance as prescribed for the endorsement	Annual return plus endorsement-specific reporting	Enhanced evidence for sovereignty, isolation, and resilience controls
Tier 1 (integrated providers)	Annual surveillance assessment	Consolidated annual return across all three domains	Single consolidated assessment relationship

d. Monitoring activities may include:
   i. periodic reporting;
   ii. annual compliance attestations;
   iii. document reviews;
   iv. surveillance assessments;
   v. site inspections;
   vi. technical assessments;
   vii. incident reporting reviews; and
   viii. such other activities as the Agency may prescribe.

18.4 Audits and Risk-Based Inspections

a. The Agency shall have the right to conduct scheduled and unannounced audits and inspections of any Certified Provider, in accordance with Section 9.8.
b. The Agency may undertake risk-based inspections where:
   i. significant non-conformities are identified;
   ii. material incidents have occurred;
   iii. there is evidence of non-compliance;
   iv. complaints or reports have been received;

v. certification renewal is being considered; or

vi. such other circumstances as the Agency may determine.

c. Certified Providers shall cooperate fully with audits and inspections conducted under this Framework and shall grant the Agency's authorised officers access to relevant facilities, systems, records, and personnel.

18.5 Remediation Measures

a. Where non-conformities are identified, the Agency may require a Certified Provider to:

i. implement corrective actions;

ii. submit a remediation plan;

iii. undertake additional assessments;

iv. implement specified safeguards;

v. suspend certain services or activities; or

vi. take such other measures as may be directed by the Agency.

b. The Agency may prescribe remediation timelines based on the nature and severity of the non-conformity.

18.6 Enforcement Measures

Enforcement under this Framework addresses conformity with national assurance requirements. It does not withdraw or restrict any person's right to conduct business under licences, permits, or approvals issued by other competent authorities. Without prejudice to any other applicable law, enforcement shall proceed through progressive regulatory intervention proportionate to the nature, severity, and persistence of the non-conformity. The Agency may take one or more of the following actions where a Certified Provider fails to conform with this Framework:

a. issue an advisory notice or warning;

b. require a corrective action plan;

c. place the Certified Provider under enhanced monitoring;

d. issue an improvement notice or a directive requiring remedial action;

e. impose conditions on the continued validity of an NDIAF Assurance Certification or workload assurance endorsement;

f. restrict the Certified Provider from supporting specified workload categories, or from onboarding additional workloads or customers, including government or regulated sector workloads;

g. publish the Certified Provider's certification and compliance status;

h. suspend an NDIAF Assurance Certification or workload assurance endorsement, in whole or in part;

i. remove the Certified Provider from the National Register of Certified Providers and the Digital Regulatory Platform (DRP);

j. notify affected Public Institutions or the relevant sector regulators, where appropriate;

k. apply such administrative measures as are lawfully available to the Agency under the NITDA Act, 2007, and applicable regulations, including drawing upon Financial Assurance maintained under Section 9.12, where applicable, in accordance with Schedule 1, and refer contraventions for prosecution as offences under Sections 17 and 18 of the NITDA Act, 2007; or

l. withdraw an NDIAF Assurance Certification or workload assurance endorsement.

k. Immediate suspension or withdrawal of certification shall be reserved for serious misconduct, systemic failures, or significant risks to national interests, to users of digital services, or to the continuity of government or regulated sector services.

18.7 Grounds for Suspension and Withdrawal

The Agency may suspend or withdraw an NDIAF Assurance Certification or workload assurance endorsement where a Certified Provider:

a. no longer satisfies the applicable eligibility, technical, operational, financial, or governance requirements;

b. provides false or misleading information;

c. fails to address identified non-conformities within prescribed timelines;

d. fails to comply with the requirements of this Framework or the conditions of its certification;

e. in the case of a Service Integrator, ceases to maintain a qualifying partnership or authorisation arrangement with a Cloud Service Provider or Tier 1 Certified Provider;

f. poses significant risks to the national digital economy, to users of digital services, or to national interests, including government or regulated sector services; or

g. commits any other act that materially undermines the objectives of this Framework.

18.8 Consequences of Suspension or Withdrawal

a. A Certified Provider whose NDIAF Assurance Certification has been suspended or withdrawn shall cease to represent itself as authorised under this Framework in respect of the affected scope and shall cease to onboard new customers within that scope.

b. Where an NDIAF Assurance Certification is suspended or withdrawn, the Certified Provider's listing on the Digital Regulatory Platform (DRP) shall automatically lapse in respect of the affected scope.

c. The Agency may direct a Certified Provider whose NDIAF Assurance Certification has been suspended or withdrawn to implement orderly migration and exit arrangements for affected customers, including Public Institutions, and may apply any Financial Assurance maintained by the Certified Provider under Section 9.12 toward the discharge of unmet migration and exit obligations.

d. The Agency may prescribe conditions for reinstatement following suspension.

18.9 Procurement Restrictions

a. Following the expiration of the transition period prescribed by the Agency, Public Institutions and regulated sector entities shall procure digital infrastructure and cloud services only from providers that:

   i. hold a valid NDIAF Assurance Certification under this Framework;

   ii. are listed on the Digital Regulatory Platform (DRP); and

iii. hold an NDIAF Assurance Certification and workload assurance endorsement at the tier applicable to the classification of the workload to be hosted or processed, in accordance with Section 14.3.

b. The Agency may approve exceptions in circumstances involving:

i. emergency requirements;

ii. pilot initiatives;

iii. the absence of suitable Certified Providers;

iv. national security considerations; or

v. such other circumstances as the Agency may determine.

c. Procurement restrictions applicable to entities within a Regulated Sector shall be administered in coordination with the relevant sector regulator, and nothing in this Section limits the supervisory or directive powers of that regulator over procurement by entities within its purview.

d. NDIAF Assurance Certification constitutes the national assurance baseline for procurement of digital infrastructure and cloud services, without prejudice to any additional procurement requirements prescribed under applicable procurement laws, including the Public Procurement Act, 2007, and nothing in this Framework displaces the functions of the Bureau of Public Procurement or any procurement authority. The procurement obligations of this Section shall be given effect through applicable procurement rules and circulars and through the IT Projects Clearance process applicable to Public Institutions.

18.10 Appeals

a. Any person aggrieved by a decision made under this Framework including a refusal to issue or renew an NDIAF Assurance Certification or workload assurance endorsement, the imposition or variation of certification conditions, or the suspension or withdrawal of an NDIAF Assurance Certification or workload assurance endorsement may submit an appeal to the Agency in writing within thirty (30) days of the date of the decision being appealed, setting out:

i. the decision being appealed;

ii. the grounds of appeal; and

iii. the remedy sought.

b. The Agency shall acknowledge receipt of an appeal within ten (10) working days.

c. Appeals shall be considered by a designated Appeals Panel constituted by the Agency, which shall include at least two independent members who are not officers of the Agency, and which shall not include any officer directly involved in the original decision.

d. The Agency shall issue a written determination on an appeal within sixty (60) working days of acknowledgement, or such extended period as the Agency may notify the appellant in writing.

e. The submission of an appeal shall not automatically suspend any enforcement action unless otherwise determined by the Agency or the Appeals Panel.

f. The Agency may prescribe further procedural requirements for the conduct of appeals, including requirements for oral hearings, the submission of evidence, and representation.

g. Nothing in this Framework limits the right of any person to seek judicial review or other judicial recourse in accordance with applicable law, and nothing precludes the Agency from taking any other action available to it under applicable laws and regulations.

19. Customer Protection and Service Continuity

a. Certified Providers shall provide certified services to customers with due skill, care, and diligence, and on terms that are fair, clear, and transparent.

b. Certified Providers shall publish accurate descriptions of their certified services, applicable service levels, and material terms, and shall not make false or misleading representations regarding their certification status or the nature of their services.

c. Certified Providers shall establish and maintain accessible complaints-handling mechanisms, resolve complaints within reasonable timelines, and maintain records of complaints and their resolution, which shall be made available to the Agency upon request.

d. A Certified Provider proposing to discontinue a certified service shall:

i. provide affected customers and the Agency with not less than ninety (90) days' written notice, or such other period as the Agency may prescribe;

ii. provide reasonable migration support to affected customers;

iii. return or make available customer data in a commonly used, machine-readable format; and

iv. securely delete customer data following migration, in accordance with applicable law and contractual arrangements.

e. A Certified Provider shall not suspend or terminate services to a customer in a manner that is arbitrary or inconsistent with its published terms and shall maintain the exit and portability arrangements required under this Framework.

f. The Agency may prescribe additional customer protection requirements, and nothing in this Section shall limit the application of the Federal Competition and Consumer Protection Act, 2018, the Nigeria Data Protection Act, 2023, or other applicable consumer protection laws.

20. Capacity Development and Awareness

a. The Agency shall promote awareness, sensitisation, and capacity-building programmes for Certified Providers, Public Institutions, and ecosystem participants to support the effective implementation of this Framework.

b. Capacity development under this Framework shall be treated as a strategic national imperative to strengthen Nigeria's digital infrastructure ecosystem, improve compliance capabilities, and promote the development of indigenous expertise in digital infrastructure assurance and supervision.

c. The Agency may undertake or facilitate activities including:

i. stakeholder sensitisation and awareness programmes;

ii. publication of implementation guidance, advisories, and technical notes;

iii. training and capacity-building programmes for public and private sector stakeholders;

iv. competency development programmes for the Agency's supervisory and inspection personnel;

v. promotion of internationally recognised standards and best practices;

vi. industry engagement and collaboration initiatives;

vii. support for knowledge transfer and skills development; and

viii. such other activities as may be necessary for the effective implementation of this Framework.

d. The Agency may collaborate with educational institutions, professional bodies, industry associations, development partners, and technology providers to strengthen national capabilities in digital infrastructure assurance and supervision.

e. The Agency shall promote awareness of the Digital Regulatory Platform (DRP) and encourage the adoption of trusted digital infrastructure services provided by Certified Providers among Public Institutions, regulated sectors, businesses, and other stakeholders across the national digital economy.

f. Certified Providers may be required to support knowledge transfer and capacity development initiatives as may be prescribed by the Agency.

21. Review and Transitional Provisions

21.1 Periodic Review

The Agency shall review this Framework periodically, and in any event not less than once every three (3) years from the date of commencement, or as may be necessary to reflect:

a. technological developments;

b. emerging risks;

c. changes in applicable laws and policies;

d. international standards and best practices;

e. implementation experience and stakeholder feedback; and

f. opportunities to consolidate obligations common to the Certification Classes into general requirements and to streamline the drafting of this Framework.

21.2 Directives and Guidance

The Agency may issue directives, advisories, operational manuals, and guidance documents to support the implementation of this Framework.

21.3 Transitional Period and Phased Implementation

a. Existing providers within the mandatory scope of this Framework shall obtain the applicable NDIAF Assurance Certification in accordance with the phased timelines set out in this Section, or within such other period as may be prescribed by the Agency.

b. The following provisions shall apply with effect from the commencement of this Framework:

   i. the Enhanced Workload Assurance and Sovereign Workload Assurance requirements, in respect of new procurements by Public Institutions;

   ii. the Design Assurance Review requirement, in respect of new data centre construction and deployment;

   iii. the incident reporting requirements of Part 18; and

   iv. onboarding onto the Digital Regulatory Platform for providers already serving Public Institutions.

c. Existing data centre operators shall obtain the Cloud Infrastructure Provider Certification (or Tier 1 Certification, as applicable) within twelve (12) months of commencement, through the conversion pathway established under Section 21.4.

d. Existing providers of cloud services and integration services to Public Institutions, regulated sectors, operators of Critical Information Infrastructure, or designated organisations shall obtain the Cloud Service Provider Certification or Service Integration Provider Certification, as applicable, within twenty-four (24) months of commencement.

e. The financial requirements prescribed under Section 9.12 and Schedule 1 shall apply to new applicants from commencement. Existing providers shall satisfy the applicable financial capacity and, where applicable, Financial Assurance requirements progressively over a build-up period of twenty-four (24) months from commencement, in accordance with Schedule 1.

f. The Agency shall publish a transition schedule specifying application windows, migration timelines, and phased compliance dates for each class of NDIAF Assurance Certification and may abridge or extend the timelines in this Section where necessary to give effect to national priorities, including the operationalisation of the National Sovereign Cloud Initiative and the implementation of sector-specific localisation requirements.

g. The procurement obligations of Sections 7.2(a) and 18.9 shall be activated for each Certification Class only on the compliance date specified for that class in the published transition schedule. Before activating them, the Agency shall satisfy itself, and publish its conclusion on the Digital Regulatory Platform, that a sufficient number and diversity of Certified Providers exist in the relevant class to sustain competitive procurement. Until activation, and thereafter where capacity is insufficient, Public Institutions may procure from provisional Certified Providers under Section 21.4(a) and under the exceptions in Section 18.9(b), so that procurement is not stalled by the pace of certification.

21.4 Continuation During Transition

During the transitional period, existing providers may continue to provide services to Public Institutions, subject to such conditions as the Agency may prescribe.

21.5 Existing Contracts

Nothing in this Framework shall invalidate contractual arrangements entered into before the commencement of this Framework, provided that such arrangements are brought into compliance within the transitional period prescribed by the Agency.

21.6 Additional Transitional Arrangements

The Agency may prescribe additional transitional arrangements where necessary to facilitate the orderly implementation of this Framework.

22. Fees and Financial Requirements

a. The Agency shall prescribe administrative fees for certification applications, assessments, grant of certification, renewals, variations, workload assurance

endorsements, surveillance activities, and other services provided under this Framework.

b. Such fees shall be:

   i. published in advance and made publicly available;

   ii. proportionate to the class of NDIAF Assurance Certification and the nature of the assessment or service;

   iii. reviewed periodically to reflect operational costs and market conditions; and

   iv. prescribed by the Agency through Schedule 1 to this Framework, or a successor fee schedule published as a subsidiary instrument.

c. Schedule 1, including the fees, financial capacity, Financial Assurance, and insurance requirements it prescribes, may be reviewed and republished by the Agency from time to time in accordance with Section 9.12(g) without requiring amendment of this Framework.

Schedule 1 — NDIAF Assurance Certification Categorisation, Financial Capacity, and Fee Requirements

Issued pursuant to Sections 9.12 and 22 of this Framework.

S1.1 Purpose

This Schedule prescribes the minimum financial capacity, insurance, and fee requirements applicable to each Certification Class, together with the Financial Assurance requirements applicable to Certified Providers holding Sovereign Workload Assurance endorsements or designated as systemically significant, and the conditions, reliefs, and transitional arrangements governing their application. The certification categorisation, eligibility, technical, operational, and governance requirements for each class are set out in Parts 9 to 13 of the Framework, and this Schedule is to be read together with them.

S1.2 Basis of the Financial Requirements

The financial requirements in this Schedule serve a single regulatory purpose: to provide evidence that a Certified Provider possesses the financial capacity and operational sustainability to sustain critical digital infrastructure operations and to meet its customer protection, service continuity, and market exit obligations throughout the certification lifecycle. They are calibrated against comparable regimes including Saudi Arabia's CST Cloud Computing Regulatory Framework, India's MeitY cloud empanelment regime, and the Nigerian Communications Commission's infrastructure licensing practice, each of which relies principally on certification, audit, and case-by-case financial capability assessment and they adapt that benchmark to this Framework's scope by combining recognised technical assurance under Part 16 with class-differentiated financial capacity benchmarks, insurance, and demonstrated business continuity capability. Financial capacity benchmarks are set materially higher for infrastructure classes, where facility investment is inherently capital-intensive, and materially lower for service and integration classes, whose risk is addressed principally through insurance and continuing supervision. Financial Assurance is not a general requirement: it applies only to Certified Providers holding Sovereign Workload Assurance endorsements or designated as systemically significant, and where it applies it is set at twenty per cent (20%) of the financial capacity benchmark of the relevant Certification Class.

S1.3 Financial Capacity and Insurance Requirements

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

All amounts are denominated in Naira. Financial capacity evidenced through paid-up capital shall be unimpaired by losses at the time of application, save that the Agency may accept fresh equity injections as curing prior planned losses for early-stage infrastructure businesses that remain solvent. Each applicant and Certified Provider shall additionally demonstrate business continuity capability and financial sustainability appropriate to its Certification Class, in accordance with Section 9.12(c) of the Framework.

S1.4 Evidence of Financial Capacity

Minimum financial capacity may be evidenced by any of the following, in accordance with Section 9.12(f) of the Framework:

a. audited financial statements for the preceding three (3) years, where available;

b. a current audited or independently reviewed statement of paid-up capital;

c. a parent company guarantee supported by the group's audited financial statements; or

d. a banker's confirmation of capital injection issued by a Deposit Money Bank licensed by the Central Bank of Nigeria.

S1.5 Financial Assurance: Sovereign Workload Assurance Holders and Systemically Significant Providers

a. Financial Assurance is required only of a Certified Provider that holds or seeks a Sovereign Workload Assurance endorsement, or that is designated by the Agency as providing systemically significant services, in accordance with Section 9.12(d) of the Framework. The prescribed amounts are: ₦200,000,000 for the Tier 1 Integrated Digital Infrastructure Provider Certification; ₦100,000,000 for the Cloud Infrastructure Provider Certification; and ₦20,000,000 for the Cloud Service Provider Certification.

b. Financial Assurance shall be maintained in the name of the Certified Provider and shall take the form of an irrevocable on-demand bank guarantee or a performance bond, and no other instrument. The instrument shall be issued by a Deposit Money Bank licensed by the Central Bank of Nigeria, or an insurer licensed by the National Insurance Commission, carrying a minimum long-term national-scale rating of A- (or equivalent) from a recognised credit rating agency, and not itself an affiliate or related party of the Certified Provider.

c. Financial Assurance shall remain in force throughout the validity of the Sovereign Workload Assurance endorsement and the underlying NDIAF Assurance Certification, and for six (6) months after expiry, surrender, or withdrawal, or until all customer transition, data migration, and exit obligations have been discharged, whichever is later.

d. The Agency may call upon the Financial Assurance, by written demand stating the grounds, to satisfy unmet customer transition, data migration, or market exit obligations under Sections 9.11 and 19 of the Framework; administrative sanctions imposed under Part 18; or outstanding financial obligations to the Agency. An affected customer may submit a claim to the Agency for payment out of the Financial Assurance in respect of unmet transition or migration obligations, and the Agency shall assess the claim and may direct payment in accordance with the procedure prescribed in the Operational Manual, which shall provide for notice to the Certified Provider, an opportunity to make representations, and a written, reasoned determination, and which shall be without prejudice to the jurisdiction of the courts.

e. Where any amount is drawn, the Certified Provider shall restore the Financial Assurance to the prescribed amount within thirty (30) days of the drawing.

f. Upon surrender, expiry without renewal, or withdrawal of the Sovereign Workload Assurance endorsement or the underlying NDIAF Assurance Certification, the instrument shall be discharged, net of amounts applied under paragraph (d), once the Agency confirms that all obligations to the Agency and to affected customers have been discharged.

S1.6 Fees

Certification Class / Endorsement	**Application Fee (non-refundable)**	**Certification Fee (payable before grant)**	**Renewal Fee**
Tier 1: Integrated Digital Infrastructure Provider Certification	₦1,000,000	₦15,000,000	50% of the Certification Fee
Cloud Infrastructure Provider Certification	₦1,000,000	₦10,000,000	50% of the Certification Fee
Cloud Service Provider Certification	₦1,000,000	₦10,000,000	50% of the Certification Fee
Cloud Service Provider Certification (Restricted)	₦250,000	₦3,000,000	50% of the Certification Fee
Service Integration Provider Certification	₦100,000	₦5,000,000	50% of the Certification Fee
Enhanced Workload Assurance (EWA)	₦500,000	₦5,000,000 (assessment and endorsement)	Renewed with the underlying certification
Sovereign Workload Assurance (SWA)	₦500,000	₦5,000,000 (assessment and endorsement)	Renewed with the underlying certification

The consolidated Tier 1 fee structure reflects a single application, a single consolidated assessment, and a single certification relationship in place of three separate ones and is priced below the aggregate cost of the three constituent

certifications. Fees under this Schedule are administrative fees for assessment, grant, surveillance, and related regulatory services; they are not licence fees.

S1.7 Cloud Service Provider Certification (Restricted)

The Cloud Service Provider Certification (Restricted) is a sub-class established under Section 9.2 of the Framework for small providers, start-ups, and indigenous providers serving lower-risk workloads within the scope of the Framework, and for voluntary applicants. A Restricted certification covers the hosting of Public and General Workloads (Level 1) only, does not qualify for an Enhanced Workload Assurance or Sovereign Workload Assurance, and is subject to simplified documentary requirements and extended compliance timelines as prescribed in the Operational Manual. A Restricted certification holder may apply at any time to upgrade to the full Cloud Service Provider Certification.

S1.8 Underserved Zone Incentives

To align the economics of this Framework with the objective of nationally distributed digital infrastructure, the following reliefs apply to facilities sited in geopolitical zones designated by the Agency as underserved:

a. a reduction of up to fifty per cent (50%) of the applicable Application Fee and Certification Fee in respect of the relevant facility;

b. extended compliance timelines for the relevant facility, as prescribed in the transition schedule; and

c. adjusted Financial Assurance arrangements, including phased build-up, in respect of the relevant facility.

S1.9 Review, Indexation, and Transition

a. The amounts in this Schedule shall be reviewed at least once every two (2) years in accordance with Section 9.12(g) of the Framework, and may be adjusted to reflect inflation, exchange rate movements, and market conditions through republication of this Schedule.

b. The financial requirements apply to new applicants from the commencement of the Framework. Existing providers within the mandatory scope shall attain not less than fifty per cent (50%) of the applicable financial capacity and, where applicable, Financial Assurance requirements within twelve (12) months

of commencement, and full compliance within twenty-four (24) months, in accordance with Section 21.3(e) of the Framework.

c. This Schedule takes effect upon approval and publication by the Agency, alongside Schedule 3 (Recognition and Mapping Schedule) and Schedule 4 (Operational Manual).

Schedule 2 — Nigerian Regulatory Assurance Requirements

Issued pursuant to Parts 9 and 16 of this Framework.

S2.1 Purpose

This Schedule is the centrepiece of the certification regime. It consolidates the Nigeria-specific assurance requirements with which NDIAF Assurance Certification certifies conformity, and together they constitute the National Assurance Baseline. The division of labour is deliberate and simple: international standards assess technical controls; this Schedule contains Nigeria's additional regulatory assurance requirements; and NDIAF Assurance Certification certifies conformity with this Schedule while recognising existing international assurance under Part 16. The two are complementary and nothing is assessed twice.

S2.2 The Requirements

Domain	Requirement	Framework Anchor
Digital sovereignty and jurisdictional control	Workloads within scope remain subject to Nigerian jurisdiction and control arrangements, including sovereign operational requirements, workload isolation, and jurisdictional safeguards for endorsed workloads.	Parts 14 and 15
Data residency and localisation	Data within scope is hosted, processed, and stored in accordance with the Data Classification Framework and applicable localisation requirements, from certified Deployment Regions and Availability Zones within Nigeria where required.	Parts 12 and 15
Governance and accountability in Nigeria	The provider maintains a registered presence, accountable management, designated	Sections 9.3, 9.4; Parts 10–13

	compliance responsibility, and verified beneficial ownership transparency.	
Operational resilience and continuity	The provider maintains availability, redundancy, continuity, and disaster recovery arrangements proportionate to the workloads served, including multi-Availability-Zone resilience for endorsed workloads.	Sections 12.3, 12.5; Part 19
Regulatory reporting and transparency	The provider files annual returns and compliance attestations, reports incidents within prescribed timelines, notifies material changes, and maintains a publicly verifiable certification status.	Section 9.14; Part 18
National security interfaces	Endorsed workloads align with Critical National Information Infrastructure protection obligations, in coordination with the Office of the National Security Adviser and other competent authorities.	Section 14.2; Part 17
Public interest and customer protection	The provider meets service continuity, complaints handling, data return and deletion, migration support, and market exit obligations.	Section 9.11; Part 19
Continuous assurance participation	The provider remains within the continuous assurance lifecycle, including surveillance, reassessment, and corrective action, at the intensity applicable to its Certification Class.	Sections 9.14, 18.3

S2.3 What NDIAF Assesses That International Certifications Do Not

Assurance Mechanism	What It Assesses
International assurance (ISO/IEC 27001, ISO/IEC 22301, ISO/IEC 27701, SOC 2, CSA STAR, Uptime, ANSI/TIA-942, PCI DSS)	Technical conformity, information security management, business continuity, privacy management, operational controls, cloud control frameworks, physical resilience, and payment data security
NDIAF Assurance Certification	Nigerian sovereignty and regulatory conformity, jurisdictional control, data residency and localisation, governance and accountability in Nigeria, reporting to the Agency, national security interfaces, public interest and customer protection, and participation in continuous national assurance

S2.4 Relationship with International Certifications

The requirements in this Schedule are not addressed by internationally recognised technical certifications and are assessed by the Agency in every case. Technical and operational requirements outside this Schedule are, wherever adequately evidenced by certifications recognised in the Recognition and Mapping Schedule, accepted without reassessment in accordance with Section 16.3.

S2.5 Status and Maintenance

a. This Schedule is the definitive statement of the National Assurance Baseline. Every assessment criterion applied under this Framework in respect of Nigerian regulatory conformity shall trace to a domain in this Schedule, and no instrument issued under this Framework — including Schedule 4 (Operational Manual) — may add to, subtract from, or vary the requirements of this Schedule.

b. This Schedule may be amended only through the periodic review process established under Section 21.1, following stakeholder consultation, and not by administrative republication.

Schedule 3 — Recognition and Mapping Schedule

Issued pursuant to Part 16 of this Framework.

S3.1 Purpose

This Schedule gives effect to Stage 1 of the three-stage assurance model in Section 9.15. It specifies the internationally recognised certifications and standards accepted under this Framework, what each is recognised for, and the Nigerian gap assessment that remains. Requirements mapped in this Schedule are accepted as evidenced without reassessment, in accordance with Sections 16.2(d) and 16.3.

S3.2 Recognition Mapping Matrix

International Certification / Standard	**Recognised For**	**Nigerian Gap Assessment (Schedule 2 domains)**
ISO/IEC 27001	Information security management (ISMS)	Governance and accountability; digital sovereignty; regulatory reporting
ISO/IEC 22301	Business continuity management	Operational resilience specifics; continuity of Government services
ISO/IEC 27701	Privacy information management	NDPA alignment, verified through NDPC mutual reliance
Uptime Institute Tier / ANSI/TIA-942	Physical and facility resilience	Public interest obligations; localisation of facilities
SOC 2 Type II	Operational and trust services controls	Localisation; DRP integration; regulatory reporting
CSA STAR	Cloud control framework	Sovereignty requirements; jurisdictional control

PCI DSS	Payment card data security	Sector requirements administered with the Central Bank of Nigeria
ISO/IEC 42001	AI management systems	AI and sovereign compute endorsement requirements

S3.3 Requirement-Level Mapping and Maintenance

a. The Agency shall maintain, as part of this Schedule, a requirement-level mapping specifying, for each recognised certification or standard: the Certification Classes and endorsements to which it applies; the requirements of this Framework it evidences in full; the requirements it evidences in part, and the supplementary evidence required; and the Schedule 2 domains that remain for Nigerian conformity assessment.

b. The Agency shall review this Schedule at least annually and republish it — including to add newly recognised certifications, successor versions of recognised standards, and equivalence determinations agreed with sector regulators — without requiring amendment of the main body of this Framework. Removal of a recognised certification shall apply prospectively and shall not invalidate an assessment already relied upon.

c. Where a Certified Provider's recognised certification is suspended, withdrawn, or expires, the Certified Provider shall notify the Agency within fourteen (14) days, and the Agency shall determine what supplementary assessment, if any, is required to maintain the mapped evidence.

Schedule 4 — Operational Manual

Issued pursuant to Section 9.9 of this Framework.

S4.1 Status

a. The Operational Manual is issued as this Schedule 4 and forms part of this Framework. It is confined to implementation detail: the principles of recognition, proportionality, assessment philosophy, and the risk model are established by the main body of this Framework and by Schedule 2, and nothing in the Operational Manual may vary them or impose obligations inconsistent with this Framework.

b. The Agency shall publish the first edition of the Operational Manual before the first application window under the transition schedule opens and may review and republish it from time to time without requiring amendment of the main body of this Framework. Each edition shall state its effective date, and assessments in progress shall be completed under the edition in force when the application was submitted, unless the applicant elects otherwise.

S4.2 Mandatory Contents

The Operational Manual shall contain, at minimum:

a. the assessment methodology and scoring model for each Certification Class, giving effect to the three-stage assurance model in Section 9.15;

b. evidence requirements for each Certification Class and workload assurance endorsement, differentiated in accordance with the supervisory profiles in Section 18.3;

c. the process map of the application-to-certification journey and the indicative timelines applicable to each stage, in accordance with Section 9.5;

d. application forms, submission requirements, and documentary checklists;

e. surveillance, self-attestation, and renewal procedures for each supervisory profile;

f. the Design Assurance Review procedure under Section 11.3;

g. assessment procedures for the Enhanced Workload Assurance and Sovereign Workload Assurance endorsements;

h. the Financial Assurance draw-down and claims determination procedure under Schedule 1;

i. complaints-handling and appeals procedures, elaborating Part 18;

j. transition, conversion, and provisional-status procedures under Part 21; and

k. guidance for accredited assessors and conformity assessment bodies engaged under Section 9.8, including the conditions of their engagement.

S4.3 Interpretation

In the event of any inconsistency between the Operational Manual and the main body of this Framework, Schedule 1, Schedule 2, or Schedule 3, the latter shall prevail to the extent of the inconsistency.

This Instrument was signed this 4th Day of August, 2026.

Kashifu Inuwa Abdullahi, *CCIE*

Director-General/CEO

National Information Technology Development Agency