Technical Standards for Deployment of Nigeria's Digital Public Infrastructure (DPI)

Document Version	1.3
Last Updated	March 17, 2025
Status	DRAFT

Table of Contents

1. INTRODUCTION

1.0 Background

Nigeria is transforming its digital landscape to enhance public services and boost economic growth through technology. Digital Public Infrastructure (DPI) is central to this effort, ensuring efficient and accessible services for citizens and businesses. Consequently, on the 4th of March 2025, the Federal Ministry of Communications, Innovation and Digital Economy (FMCIDE) issued a National Digital Public Infrastructure (DPI) Framework, articulating a broad plan for the development and implementation of Digital Public Infrastructure (DPI) in Nigeria.

Therefore, strong technical standards are necessary to implement the framework of the Federal Ministry of Communication, Innovation, and Digital Economy and to keep pace with rapid technological changes. These standards promote interoperability, security, and quality across digital platforms, creating efficient, reliable, and inclusive systems. They will address key issues like data privacy, cybersecurity, and user experience, fostering trust in digital services. As Nigeria progresses in its digital economy, these standards will ensure a secure and user-friendly environment.

Since 2001, when the Federal Government of Nigeria issued the National Information Technology Policy, successive governments' visions of government digital services have progressively led to the creation of several platforms to deliver those services. However, the full potential of government digital services cannot be achieved due to the siloed approach based on existing legal frameworks.

To address this issue, the National Information Technology Development Agency, under the policy directives of the Federal Ministry of Communications Innovation and Digital Economy, has identified the need to develop a uniform standard for integrating government digital services in a manner that would harness the vast resources of

government in delivering cost-effective and functional services across all government agencies and platforms through the Digital Public Infrastructure (DPI) Programme.

Developing robust Digital Public Infrastructure (DPI) in Nigeria is intrinsically linked to establishing and adhering to comprehensive technical standards. In a nation undergoing rapid digital transformation, the need for interoperability, security, and efficiency within its digital systems is paramount. Nigeria's journey towards a thriving digital economy necessitates standards that ensure seamless integration of various digital services, from identity management to financial transactions, through an exchange platform that harnesses the potential of data sharing through common standards. The goal is to create a secure and reliable digital ecosystem that can support the nation's economic growth and improve the lives of its citizens.

1.1 Purpose

These technical standards provide a structured framework for developing, developing, and deploying Nigeria's Digital Public Infrastructure (DPI). They define the essential technical requirements and best practices to ensure interoperability, security, and efficiency across digital services. By establishing clear guidelines, these standards support the seamless integration of DPI components, fostering a secure, scalable, and resilient digital ecosystem.

The standards will:

1. **Enhance Interoperability**: Ensure seamless communication across platforms, agencies, and services
2. **Ensure Data Security and Privacy**: Protect sensitive information while complying with local and international regulations
3. **Promote Accessibility and Usability**: Create inclusive systems that are easy to navigate and cater to all citizens, including marginalised groups.

4. **Define Performance Benchmarks**: Establish metrics to ensure systems are reliable, scalable, and efficient.
5. **Foster Governance and Compliance**: Provide clear accountability, transparency, and regulatory alignment rules
6. **Encourage Innovation**: Facilitate the adoption of open-source technologies while adhering to proper usage guidelines.
7. **Standardise Testing Practices**: Ensure consistent validation of systems to meet defined technical and user requirements

Requirement 1.1.1: All service providers, government agencies, and other stakeholders participating in Nigeria's DPI ecosystem must comply with these standards.

1.2 Scope

These standards encompass all technical aspects of DPI implementation, including but not limited to:

a) System architecture and design
b) Data exchange and management
c) Security and privacy controls
d) Performance and scalability requirements
e) Integration and interoperability specifications
f) Testing and quality assurance procedures

1.3 Application and Target Audience

This document is intended for:

1. **Government Agencies and Departments**:
    - Federal ministries and agencies implementing DPI components
    - State and local government bodies integrating with DPI

- Regulatory bodies overseeing digital services

2. **Service Providers**:
    - Public sector organisations delivering digital services
    - Private sector entities integrating with government systems
3. **Developers and System Integrators**:
    - Software engineers and architects building and maintaining DPI solutions
    - Integration specialists ensuring cross-platform interoperability
4. **Vendors and Solution Providers**:
    - Technology companies providing software, hardware, and cloud services
5. **Private Sector Partners**:
    - Financial institutions, tech hubs, and innovators collaborating with the government
6. **Civil Society and Advocacy Groups**:
    - Organisations ensuring inclusivity, transparency, and public interest
7. **Academia and Research Institutions**:
    - Providing technical expertise and fostering innovation

1.4 Document Updates

These standards may be updated from time to time based on emerging technologies, evolving security threats, changes in regulatory requirements, feedback from stakeholders, and lessons learned from operational experience.

2. CORE PRINCIPLES

2.0 Introduction

This document outlines the core principles guiding the development and implementation of a technical standard for data exchange within Nigeria's Digital Public Infrastructure (DPI). These principles are fundamental to ensuring a robust, secure, and equitable data ecosystem that serves all citizens.

2.1 Interoperability

Interoperability is fundamental to Nigeria's DPI ecosystem. It enables seamless communication and data exchange between diverse systems, platforms, and stakeholders.

Requirement 2.1.1: Service providers must implement standardised APIs and data exchange protocols that conform to the specifications detailed in Section 9 of this document.

Requirement 2.1.2: Interoperability Requirements

Services must demonstrate:
a) Technical interoperability through standardised protocols
b) Semantic interoperability through common data models
c) Organisational interoperability through aligned business processes.

Requirement 2.1.3: Service providers shall:

1. Maintain backward compatibility for at least one year when implementing updates or changes to their APIs
2. Facilitate unified operations and streamline processes across governmental tiers

3. Enable efficient service delivery across governmental tiers, private entities, and citizen-facing services
4. Break down data silos and promote a "whole-of-government" approach

2.2 Security and Privacy

Public trust is built upon strong privacy and data security practices. Citizens shall be made to believe their data is secure and their privacy is respected. Privacy and data security are mutually reinforcing. Strong security measures are essential for protecting privacy, and privacy principles guide the implementation of security controls.

Requirement 2.2.1: All service providers must implement comprehensive security controls specified in Section 5 of this document.

Requirement 2.2.2: Service providers shall comply with:
a) Nigeria Data Protection Act (NDPA)
b) ISO/IEC 27001 Information Security Management Standards
c) NIST Cybersecurity Framework guidelines

Requirement 2.2.3: Service providers shall:

1. Embed robust security measures to protect sensitive data from unauthorised access, use, or disclosure
2. Adhere to all relevant Nigerian data protection laws and international standards
3. Ensure transparency and accountability in data handling practices
4. Foster public confidence in the DPI and encourage widespread adoption

2.3 Scalability

This refers to the data exchange's ability to handle a growing volume of data and increase user demands without compromising performance, reliability, or security. Essentially, it means ensuring the system can "scale up" or "scale out" to meet future needs.

Requirement 2.3.1: All DPI components must be capable of handling:

a) Minimum of 1,000 requests per second under normal conditions
b) Scaling to 10,000 requests per second during peak loads
c) Response times of ≤300ms for 95% of requests

Requirement 2.3.2: Service providers shall:

1. Support systems capable of handling Nigeria's large and growing population
2. Ensure data exchange can scale efficiently without system failures
3. Design systems to handle increasing data volume and transaction loads
4. Implement auto-scaling capabilities as detailed in Section 7.3

2.4 Inclusivity

This means ensuring that all individuals and groups, regardless of their background, abilities, or circumstances, have equitable access to and can effectively participate in the data exchange ecosystem. It shall go beyond making data available; it must actively remove barriers and design systems that cater to diverse needs.

Requirement 2.4.1: All user interfaces must follow Web Content Accessibility Guidelines (WCAG) 2.1 Level AA standards.

Requirement 2.4.2: Service providers shall:
a) Support English as the primary language
b) Provide the capability to support additional languages, including but not limited to Hausa, Yoruba, and Igbo, based on regional requirements and demographics
c) Support various access devices (desktop, mobile, feature phones)

d) Accommodate different connectivity levels (including low-bandwidth scenarios)
e) Implement region-specific formatting for:

- Currency display in Naira (₦)
- Date format (dd/mm/yyyy)
- Time format (configurable 24-hour or AM/PM)

Requirement 2.4.3: Service providers shall:

1. Prioritise accessibility for all citizens, including those in rural communities
2. Support people with disabilities and individuals with diverse languages
3. Promote equitable access to digital services
4. Bridge the digital divide through inclusive design
5. Maintain offline capabilities where technically feasible

---

3. SERVICE PROCESS AND ARCHITECTURE STANDARDS

3.0 Introduction

This chapter outlines the essential components of the Nigerian Data Exchange (NGDX). Through digital channels, this mandated infrastructure enables streamlined and secure interactions between citizens, service providers, and government entities. The following sections detail the elements and standards governing the NGDX, ensuring efficiency, security, and transparency in public service delivery.

3.1 Data Transaction Process

3.1.1 Service Consumer (NGDX Member)

Service Consumers are defined as entities or platforms that directly interact with citizens, providing various services through digital interfaces as stipulated by NGDX standards.

Requirement 3.1.1.1: Service Consumers must implement the following mandatory platforms:

a) **Web Portals**: Required for facilitating applications for services such as driving licences, tax returns, and government subsidies

b) **Mobile Applications**: Must provide access to critical services like social benefit payments and healthcare records

3.1.2 Consumer Security Server

Requirement 3.1.2.1: The Consumer Security Server, managed by Service Consumer agencies, must:

a) Securely transmit and sign all outgoing requests

b) Maintain the integrity and confidentiality of data exchanges

c) Adhere to NGDX security protocols

3.1.3 NGDX Operator

Requirement 3.1.3.1: Galaxy Backbone Limited (GBB) is designated as the government agency responsible for:

a) Management and maintenance of the technical infrastructure supporting the DPI

b) Ensuring infrastructure availability and reliability

c) Implementing and maintaining disaster recovery capabilities

d) Providing secure hosting and connectivity services

Requirement 3.1.3.2: Trust Services must:

a) Be managed by GBB or a designated trusted third-party

b) Validate all certificates within the NGDX ecosystem
c) Implement mandatory timestamping of every transaction

3.1.4 Service Provider (NGDX Member)

Requirement 3.1.4.1: Service Providers must implement and maintain the following:
a) Backend services and data necessary for public service functions
b) Provider Security Server as the security gateway
c) Comprehensive data management systems

Requirement 3.1.4.2: Examples of mandatory service implementations include:
a) WAEC: Management of examination results database
b) Nigerian Federal Road Safety Corps: Maintenance of driver and vehicle registration records
c) E-Governance Services: Digital service delivery by various ministries

3.1.5 Data Layer

Requirement 3.1.5.1: The Data Layer must include the following centralised repositories:
a) **Citizen Database**: Managed by NIMC for personal and demographic information
b) **Transaction Database**: Managed by NIBSS for transactional data
c) **National Data Exchange**: Platform for secure inter-agency data sharing

3.2 Data Exchange Architecture

Requirement 3.2.1: The data exchange architecture shall comprise three distinct layers:

a) **National Layer**

- Operated by: Galaxy Backbone Infrastructure
- Scope: Federal agencies and cross-state communications

- Services: Security, authentication, and trust management

b) **Sub-National Layer**

- Operated by: State governments
- Scope: State-level agencies and local government areas
- Integration: Must connect to the national NGDX system

c) **Sectoral Layer**

- Operated by: Sector regulatory bodies
- Scope: Industry-specific ecosystems (healthcare, finance, etc.)
- Compliance: Must adhere to sector-specific regulations

3.3 Service Provider Architecture Standards

Requirement 3.3.1: Service providers must implement the following architectural components:

a) **NGDX Interface Layer**

- Must handle request/response management
- Shall implement security protocols as specified in Section 5
- Must maintain transaction logs

b) **Security Server**

- Must verify all incoming requests
- Shall implement comprehensive logging
- Must sign all outgoing responses

c) **Core Service Systems**

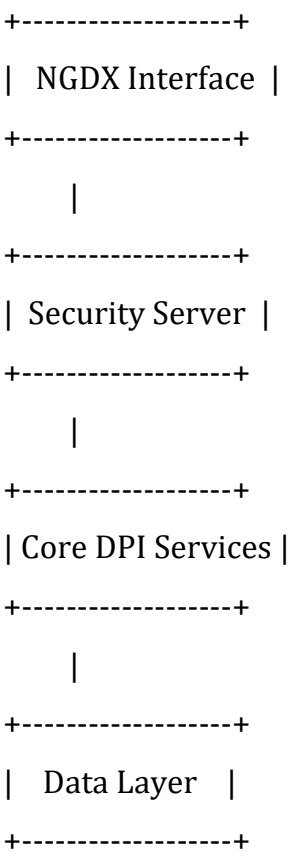
- Must implement modular design
- Shall support horizontal scaling

- Must maintain service isolation

Requirement 3.3.2: Data Layer Implementation

Service providers must implement a data layer that:
a) Uses centralised data repositories
b) Implements proper data segregation
c) Maintains data integrity controls

Figure 3.1: Service Provider Architecture



Requirement 3.3.3: Security Mapping

Service providers must implement security controls at each architectural layer:
a) Transport Layer Security (TLS 1.3) for communications

b) Mutual TLS (mTLS) for service authentication
c) End-to-end encryption for sensitive data

---

4. DATA STANDARDS

4.1 Data Exchange Standards

All data exchanges within the DPI ecosystem must follow standardised formats and protocols to ensure interoperability and consistency.

Requirement 4.1.1: Data Format Standards

Service providers must:
a) Use JSON as the standard format for all data exchanges
b) Implement UTF-8 character encoding
c) Follow ISO 8601 for date and time formats

Requirement 4.1.2: API Standards

All APIs must:
a) Follow RESTful architecture principles
b) Implement versioning using semantic versioning (e.g., v1, v2)
c) Include standardised error handling and status codes

4.2 Metadata Format

Requirement 4.2.1: Mandatory Metadata Fields

All data records must include the following metadata:

Field	Description	Format	Required
created_at	Creation timestamp	ISO 8601	Yes
modified_at	Last modification time	ISO 8601	Yes
created_by	Creator identifier	String	Yes
sensitivity	Data classification	Enum	Yes
version	Record version	Semantic	Yes

Requirement 4.2.2: Metadata Structure

Service providers must implement metadata in the following JSON format:

```
{
 "metadata": {
  "created_at": "2024-03-01T10:00:00Z",
  "modified_at": "2024-03-01T10:00:00Z",
  "created_by": "system_id",
  "sensitivity": "confidential",
  "version": "1.0.0"
 },

}
```

4.3 Data Lifecycle Management

Requirement 4.3.1: Data Retention

Service providers must implement the following retention periods:
a) Public Data: A stipulated in relevant policy or regulation issued under the Nigerian National Archives Act 2004, NITDA Act 2007 and the Nigerian Data Protection Act 2003.
b) Confidential Data: As issued under any policy or regulation issued under NITDA Ac 2007
c) Restricted Data: As issued under the NITDA Act 2007 or the Offical States Secrets Act

Requirement 4.3.2: Data Versioning

Service providers shall:
a) Maintain version history for all critical data
b) Implement audit trails for data modifications
c) Support data rollback capabilities

Requirement 4.3.3: Secure Deletion

When deleting data, service providers must:
a) Use secure deletion methods (e.g., cryptographic erasure)
b) Maintain deletion logs
c) Verify complete removal of data and associated metadata

4.4 Security and Governance

Requirement 4.4.1: Access Control

Service providers must implement:
a) Role-Based Access Control (RBAC)

b) Attribute-Based Access Control (ABAC) where necessary
c) Regular access review procedures

Requirement 4.4.2: Data Classification

All data must be classified according to the following sensitivity levels:

Level	Description	Examples
Public	No restrictions	Public notices
Confidential	Limited access	Personal data
Restricted	Strictly controlled	Financial records

Requirement 4.4.3: Audit Requirements

Service providers must maintain:
a) Immutable audit logs
b) Access logs for all data operations
c) Regular audit reports for compliance verification

---

5. SECURITY STANDARDS

5.1 Authentication and Authorisation

Requirement 5.1.1: Authentication Framework

All services must implement:
a) Multi-factor authentication for sensitive operations
b) Role-based access control (RBAC)
c) Session management with secure token handling

Requirement 5.1.2: Authorisation Framework

The following authorisation controls must be implemented:
a) Attribute-based access control (ABAC)
b) Fine-grained permission management
c) Regular access reviews

Table 5.1: Authentication Methods and Use Cases

Method	Use Case	Minimum Requirements
Password	User login	Min. 12 chars, complexity rules
MFA	Admin access	Two independent factors
Certificates	Service auth	X.509, 2048-bit minimum

5.2 Encryption

Requirement 5.2.1: Data in Transit

All data in transit must be encrypted using:
a) TLS 1.3 or higher for all communications

b) Perfect Forward Secrecy (PFS) for key exchange
c) Strong cipher suites as approved by NIST

Requirement 5.2.2: Data at Rest

Service providers must implement:
a) AES-256 encryption or better for stored data
b) Secure key management using Hardware Security Modules (HSM)
c) Regular key rotation procedures

5.3 API Security

Requirement 5.3.1: API Protection

All APIs must implement:
a) Rate limiting and throttling
b) Input validation and sanitisation
c) Output encoding
d) CORS policies

Requirement 5.3.2: API Authentication

APIs must use:
a) OAuth 2.0 with OpenID Connect
b) JWT tokens with appropriate expiration
c) API keys for service-to-service communication

5.4 Identity Management

Requirement 5.4.1: Identity Standards

Service providers must:
a) Use the National Identity Number (NIN) as the primary identifier
b) Implement identity federation where appropriate
c) Support identity verification through NIMC

Requirement 5.4.2: Identity Data Protection

Identity data must be:
a) Encrypted at rest and in transit
b) Stored in secure, access-controlled locations
c) Regularly backed up and protected

5.5 Incident Response

Requirement 5.5.1: Incident Management

Service providers must establish:
a) Incident response teams and procedures
b) 24/7 security monitoring
c) Incident classification and escalation protocols

Table 5.2: Incident Response Timelines

Severity	Initial Response	Resolution Target
Critical	1 hour	4 hours
High	4 hours	24 hours

Medium	12 hours	72 hours
Low	24 hours	1 week

Requirement 5.5.2: Security Monitoring

Implement continuous monitoring of:
a) System and application logs
b) Network traffic and anomalies
c) Security events and alerts

Requirement 5.5.3: Vulnerability Management

Service providers must:
a) Conduct quarterly (minimum) vulnerability assessments
b) Perform annual penetration testing
c) Maintain a vulnerability management program

5.6 Compliance and Reporting

Requirement 5.6.1: Security Compliance

Service providers must comply with:
a) Nigeria Data Protection Act (NDPA)
b) ISO/IEC 27001 standards
c) Cloud Cybersecurity Framework

---

6. ACCESSIBILITY AND USABILITY STANDARDS

6.1 User Interface Guidelines

Requirement 6.1.1: WCAG Compliance

All user interfaces must:
a) Comply with WCAG 2.1 Level AA standards
b) Support keyboard navigation
c) Provide text alternatives for non-text content
d) Ensure sufficient color contrast ratios

Requirement 6.1.2: Screen Reader Compatibility

Service providers must ensure:
a) Compatibility with common screen readers (NVDA, JAWS, VoiceOver)
b) Proper semantic HTML structure
c) ARIA labels where necessary

Table 6.1: Accessibility Requirements

Feature	Requirement	Standard
Color Contrast	Minimum 4.5:1	WCAG 2.1
Text Sizing	Scalable to 200%	WCAG 2.1
Keyboard Navigation	Full access	WCAG 2.1

Screen Reader	Full support	WCAG 2.1

6.2 Language and Localisation

Requirement 6.2.1: Language Support

All user interfaces must:
a) Support English (primary)
b) Provide capability to support additional languages, including but not limited to Hausa, Yoruba, and Igbo, based on regional requirements and demographics
c) Implement localised date and time formats
d) Support customisation based on user preferences

Requirement 6.2.2: Content Localisation

Service providers must implement:
a) Language selection options
b) Localised date and time formats
c) Currency formatting (₦)
d) Region-specific content where applicable

Requirement 6.2.3: Translation Management

Implement a centralised translation service that:
a) Maintains consistent terminology
b) Supports regular content updates
c) Ensures quality of translations

6.3 Mobile Accessibility

Requirement 6.3.1: Responsive Design

All interfaces must:

a) Adapt to different screen sizes

b) Support touch interactions

c) Maintain functionality across devices

Requirement 6.3.2: Mobile optimisation

Service providers must implement:

a) Compressed images and media

b) Minimal bandwidth usage

c) Offline capabilities where feasible

Table 6.2: Mobile Performance Requirements

Metric	Target	Maximum
Page Load	< 3 seconds	5 seconds
Total Size	< 2 MB	5 MB
First Paint	< 1 second	2 seconds

6.4 Testing and Validation

Requirement 6.4.1: Accessibility Testing

Service providers must conduct:

a) Automated accessibility testing

b) Manual screen reader testing

c) Keyboard navigation testing

d) Color contrast verification

Requirement 6.4.2: Usability Testing

Perform regular testing with:

a) Different user groups

b) Various devices and platforms

c) Different network conditions

Requirement 6.4.3: Performance Testing

Regular testing must verify:

a) Load times across devices

b) Responsiveness of UI elements

c) Bandwidth usage optimisation

6.5 Documentation and Support

Requirement 6.5.1: User Documentation

Provide accessible documentation including:

a) User guides in multiple languages

b) Accessibility features documentation

c) Alternative format availability

Requirement 6.5.2: Support Channels

Maintain accessible support through:

a) Web-based help systems

b) Phone support
c) Email support
d) Chat assistance

---

7. PERFORMANCE AND SCALABILITY STANDARDS

7.1 Benchmarking

Requirement 7.1.1: Key Performance Indicators (KPIs)

Service providers must meet the following performance metrics:
a) Response Time: ≤300ms for 95% of API requests under normal conditions
b) Throughput: Minimum 1,000 requests per second (RPS)
c) Error Rate: ≤0.1% under normal conditions
d) System Availability: 99.99% for critical systems, 99.65% minimum for all services

Requirement 7.1.2: Performance Monitoring

Service providers must implement:
a) Real-time performance dashboards
b) Automated alerting for KPI violations
c) Historical performance trend analysis

Table 7.1: Performance Benchmarks

Metric	Normal Conditions	Peak Load

Response Time	≤300ms	≤500ms
Throughput	1,000 RPS	10,000 RPS
Error Rate	≤0.1%	≤1%
CPU Utilisation	≤70%	≤90%

Requirement 7.1.3: Resource Monitoring

Monitor and report on:
a) CPU utilisation: ≤70% under normal load
b) Memory utilisation: ≤75% under normal load
c) Network latency: ≤50ms within data centre
d) Storage utilisation: ≤80% capacity

7.2 Load Testing

Requirement 7.2.1: Load Testing Requirements

Service providers must:
a) Conduct monthly load tests simulating peak conditions
b) Test with production-like data volumes
c) Validate all KPIs under stress conditions

Requirement 7.2.2: Testing Scenarios

Implement the following test scenarios:
a) Normal operational load
b) Peak load (200% of normal)
c) Sustained high load (150% for 24 hours)
d) Disaster recovery scenarios

Requirement 7.2.3: Testing Tools

Use industry-standard tools for load testing:
a) JMeter or equivalent for API testing
b) Browser-based tools for UI testing
c) Specialised tools for specific protocols

7.3 Elastic Scaling

Requirement 7.3.1: Auto-scaling Triggers

Implement auto-scaling based on:
a) CPU Utilisation: Scale up at >70%, down at <30%
b) Memory Usage: Scale up at >75% utilisation
c) Request Queue Size: Scale if queue exceeds 50% capacity
d) Custom metrics as appropriate for the service

Requirement 7.3.2: Scaling Mechanisms

Service providers must implement:
a) Horizontal scaling for stateless services
b) Vertical scaling where horizontal scaling is not feasible
c) Region-based scaling for improved latency
d) Cost optimisation during non-peak periods

Table 7.2: Scaling Thresholds

Metric	Scale Up	Scale Down
CPU	>70%	<30%
Memory	>75%	<40%
Queue Size	>50%	<20%
Error Rate	>0.1%	N/A

7.4 Real-Time Monitoring

Requirement 7.4.1: Monitoring Requirements

Implement continuous monitoring of:
a) Infrastructure metrics (CPU, memory, disk, network)
b) Application metrics (response times, error rates, throughput)
c) Business metrics (transaction volumes, user activity)
d) Security metrics (failed logins, suspicious activities)

Requirement 7.4.2: Alerting Framework

Establish an alerting system that:
a) Provides real-time notifications for KPI violations
b) Implements different severity levels
c) Includes escalation procedures
d) Maintains alert history for analysis

Requirement 7.4.3: Monitoring Tools

Deploy industry-standard monitoring tools:
a) Infrastructure monitoring (e.g., Prometheus, Grafana)
b) Application Performance Monitoring (APM)
c) Log aggregation and analysis
d) Custom monitoring for specific requirements

---

8. GOVERNANCE AND COMPLIANCE STANDARDS

8.1 Regulatory Alignment

Requirement 8.1.1: Regulatory Compliance

Service providers must comply with:
a) Nigeria Data Protection Act (NDPA)
b) ISO/IEC 27001 Information Security Management Standards
c) NIST Cybersecurity Framework

8.2 Audit and Monitoring

Requirement 8.2.1: Training Programme Requirements

Service providers must:
a) Establish standardised training programmes
b) Implement certification programmes for technical staff
c) Maintain a knowledge centre for documentation
d) Conduct regular skill assessments

8.3 Roles and Responsibilities

Requirement 8.3.1: Governance Structure

Service providers must establish:
a) Clear governance structure
b) Roles and responsibilities for all stakeholders
c) Decision-making processes

---

9. INTEROPERABILITY STANDARDS

9.1 Integration Protocols

Requirement 9.1.1: Performance Optimisation

Services must implement:
a) Caching strategies
b) Load balancing
c) Resource optimisation
d) Database query optimisation

9.2 Common Identifiers

Requirement 9.2.1: Common Identifier Standards

Service providers must implement:
a) Unique identifiers for all DPI components
b) Consistent naming conventions
c) Integration with existing systems

9.3 Monitoring and Governance

Requirement 9.3.1: Monitoring and Governance

Service providers must implement:

a) Monitoring frameworks

b) Governance structures

c) Reporting and compliance mechanisms

---

10. TESTING AND QUALITY ASSURANCE STANDARDS

10.1 Unit Testing

Requirement 10.1.1: Testing Standards

Implement the following:

a) Standardised test procedures

b) Automated test suites

c) Performance optimisation measures

d) Security vulnerability assessments

Requirement 10.1.2: Testing Framework

Implement unit testing using:

a) Industry-standard testing frameworks

b) Automated test runners

c) Continuous Integration (CI) pipeline integration

d) Mock and stub frameworks for dependencies

Table 10.1: Code Coverage Requirements

Component Type	Minimum Coverage	Target Coverage
Critical Systems	100%	100%
New Code	80%	90%
Legacy Code	70%	80%
Infrastructure Code	75%	85%

10.2 Integration Testing

Requirement 10.2.1: Integration Test Scope

Integration tests must cover:
a) All service-to-service interactions
b) Database operations
c) External API integrations
d) Message queue operations

Requirement 10.2.2: Test Environment

Maintain the following environments:
a) Development environment
b) Integration test environment
c) Staging environment
d) Production-like test environment

Requirement 10.2.3: Data Management

For integration testing:

a) Use anonymised production-like data

b) Implement data cleanup procedures

c) Maintain test data versioning

d) Ensure data isolation between tests

10.3 Performance Testing

Requirement 10.3.1: Performance Test Types

Implement the following performance tests:

a) Load testing under normal conditions

b) Stress testing at 200% capacity

c) Endurance testing for 24+ hours

d) Spike testing for sudden load increases

Requirement 10.3.2: Performance Metrics

Monitor and report:

a) Response times (average, 95th percentile, 99th percentile)

b) Throughput (requests per second)

c) Error rates and types

d) Resource utilisation (CPU, memory, disk, network)

10.4 Security Testing

Requirement 10.4.1: VAPT Requirements

Conduct regular security testing:

a) Monthly automated vulnerability scans

b) Quarterly penetration testing

c) Annual comprehensive security audit

d) Ad-hoc testing after major changes

Requirement 10.4.2: Security Test Coverage

Security testing must include:

a) OWASP Top 10 vulnerabilities

b) API security testing

c) Authentication and authorisation testing

d) Encryption and key management validation

Table 10.2: Security Testing Schedule

Test Type	Frequency	Minimum Duration
Automated Scans	Monthly	24 hours
Penetration Testing	Quarterly	1 week
Security Audit	Annual	2 weeks
Code Review	Continuous	N/A

Requirement 10.4.3: Security Testing Tools

Use industry-standard security testing tools:

a) Static Application Security Testing (SAST)

b) Dynamic Application Security Testing (DAST)

c) Interactive Application Security Testing (IAST)

d) Software Composition Analysis (SCA)

10.5 Test Automation

Requirement 10.5.1: Automation Framework

Implement test automation for:
a) Unit tests in CI/CD pipeline
b) Integration tests in deployment pipeline
c) Security scans in release process
d) Performance tests in staging environment

Requirement 10.5.2: Test Reporting

Generate automated reports for:
a) Test execution results
b) Code coverage metrics
c) Performance test results
d) Security scan findings

10.6 Quality Gates

Requirement 10.6.1: Release Criteria

Define quality gates for:
a) Code coverage thresholds
b) Performance benchmarks
c) Security vulnerability limits
d) Test pass rates

Requirement 10.6.2: Quality Metrics

Track and report quality metrics:
a) Defect density

b) Test coverage trends
c) Technical debt metrics
d) Security vulnerability trends

---

11. DEPLOYMENT AND OPERATIONS STANDARDS

11.1 Infrastructure Requirements

Requirement 11.1.1: Infrastructure Specifications

Service providers must maintain:
a) High-availability infrastructure with 99.99% uptime
b) Geo-redundant deployments across multiple zones
c) Scalable compute resources (CPU, memory, storage)
d) Network capacity for peak loads

Requirement 11.1.2: Disaster Recovery

Implement disaster recovery with:
a) Recovery Time Objective (RTO) ≤4 hours
b) Recovery Point Objective (RPO) ≤15 minutes
c) Regular DR testing (minimum quarterly)
d) Documented recovery procedures

Table 11.1: Infrastructure SLAs

Component	Availability	Redundancy

Core Services	99.99%	Multi-zone
Data Storage	99.999%	Multi-region
Network	99.99%	Redundant paths
Security Systems	99.999%	Active-active

11.2 CI/CD Pipelines

Requirement 11.2.1: Pipeline Components

Implement CI/CD pipelines with:
a) Source code version control
b) Automated build processes
c) Test automation integration
d) Deployment automation

Requirement 11.2.2: Deployment Processes

Establish deployment procedures for:
a) Blue-green deployments
b) Canary releases
c) Rollback capabilities
d) Feature flags management

Requirement 11.2.3: Infrastructure as Code

Implement IaC practices using:
a) Version-controlled infrastructure definitions

b) Automated provisioning
c) Configuration management
d) Environment parity

11.3 Monitoring and Alerts

Requirement 11.3.1: Monitoring Coverage

Monitor the following aspects:
a) Infrastructure health and performance
b) Application metrics and logs
c) Security events and alerts
d) Business KPIs

Requirement 11.3.2: Alert Management

Implement alerting with:
a) Severity-based classification
b) Automated escalation procedures
c) On-call rotation schedules
d) Incident tracking and resolution

Table 11.2: Alert Response SLAs

Severity	Response Time	Resolution Time
Critical	15 minutes	2 hours
High	30 minutes	4 hours

Mediu m	2 hours	8 hours
Low	8 hours	24 hours

11.4 Backup and Recovery

Requirement 11.4.1: Backup Requirements

Implement backup procedures for:
a) Database backups (hourly)
b) Configuration backups (daily)
c) System state backups (weekly)
d) Archive storage (monthly)

Requirement 11.4.2: Data Retention

Maintain data retention periods for a minimum of:
a) Operational data: 90 days
b) Business records: 7 years
c) Audit logs: 3 years
d) System backups: 30 days

11.5 Change Management

Requirement 11.5.1: Change Control

Implement change management procedures:
a) Change request documentation
b) Impact assessment

c) Approval workflows
d) Post-implementation review

Requirement 11.5.2: Release Management

Establish release procedures for:
a) Version control and tagging
b) Release notes generation
c) Deployment scheduling
d) Stakeholder communication

---

12. TRAINING AND CAPACITY BUILDING STANDARDS

12.1 Developer Documentation

Requirement 12.1.1: Developer Documentation

Service providers must provide:
a) Detailed technical documentation
b) API documentation
c) Deployment and configuration guides

12.2 End-User Training

Requirement 12.2.1: End-User Training

Service providers must implement:
a) Training programmes for all users

b) Certification and accreditation processes
c) User acceptance testing

12.3 Community Engagement

Requirement 12.3.1: Community Engagement

Service providers must engage with:
a) Local communities
b) Industry associations
c) Technical forums

---

13. FUTURE-PROOFING STANDARDS

13.1 Emerging Technologies

Requirement 13.1.1: Emerging Technologies

Service providers must:
a) Identify emerging technologies
b) Assess their potential impact
c) Plan for integration

13.2 Implementation Strategies

Requirement 13.2.1: Implementation Strategies

Service providers must implement:
a) Strategic deployment plans

b) Pilot projects

c) Scalable architectures

13.3 Upgradability

Requirement 13.3.1: Upgradability

Service providers must implement:

a) Flexible upgrade paths

b) Version control mechanisms

c) Continuous integration and deployment

ANNEXURES

Annexure A: Glossary

Annexure A: Glossary

Term	Definition
ABAC	Attribute-Based Access Control - A security model that authorises access based on attributes
AES	Advanced Encryption Standard
API	Application Programming Interface - A set of rules for building and integrating software applications
APM	Application Performance Monitoring
ARIA	Accessible Rich Internet Applications
BVN	Bank Verification Number
CBN	Central Bank of Nigeria

CI/CD	Continuous Integration/Continuous Deployment
CORS	Cross-Origin Resource Sharing
CPU	Central Processing Unit
CSA	Cloud Security Alliance
DAST	Dynamic Application Security Testing
DPI	Digital Public Infrastructure - Core digital systems serving as public utilities
DR	Disaster Recovery
GBB	Galaxy Backbone Limited
HSM	Hardware Security Module - Physical device that safeguards digital keys
IAST	Interactive Application Security Testing
IaC	Infrastructure as Code
ISO	International Organization for Standardization
JWT	JSON Web Token - Compact, URL-safe means of representing claims between parties
KPI	Key Performance Indicator
MFA	Multi-Factor Authentication - Authentication using two or more verification factors
mTLS	Mutual Transport Layer Security
NCC	Nigerian Communications Commission
NDPA	Nigeria Data Protection Act
NGDX	Nigerian Data Exchange
NIBSS	Nigeria Inter-Bank Settlement System
NIMC	National Identity Management Commission - Nigeria's identity management authority

NIN	National Identification Number - Unique identifier for Nigerian citizens
NIST	National Institute of Standards and Technology
NITDA	National Information Technology Development Agency
NVDA	NonVisual Desktop Access
OWASP	Open Web Application Security Project
PFS	Perfect Forward Secrecy
RBC	Role-Based Access Control - Access control based on user roles
RPO	Recovery Point Objective
RPS	Requests Per Second
RTO	Recovery Time Objective
SAST	Static Application Security Testing
SCA	Software Composition Analysis
SLA	Service Level Agreement
TLS	Transport Layer Security - Cryptographic protocol for secure communications
VAPT	Vulnerability Assessment and Penetration Testing - Security testing methodology
WAEC	West African Examinations Council
WAT	West Africa Time
WCAG	Web Content Accessibility Guidelines - Web accessibility standards

Annexure B: Reference Documents

B.1 Technical Standards

1. ISO/IEC 27001:2013 - Information Security Management

2. NIST Special Publication 800-53 - Security Controls
3. WCAG 2.1 - Web Content Accessibility Guidelines
4. OAuth 2.0 and OpenID Connect Specifications

B.2 National Regulations

1. Nigeria Data Protection Act (NDPA) 2023
2. NITDA Guidelines for Digital Public Infrastructure
3. National Cybersecurity Policy
4. NGDX Standards and Architecture Documents

Annexure C: Global Standards and Frameworks

C.1 Security Frameworks

1. NIST Cybersecurity Framework
2. ISO/IEC 27001 Information Security Management
3. OWASP Security Standards
4. Cloud Security Alliance (CSA) Guidelines

C.2 Interoperability Standards

1. REST API Design Standards
2. JSON Data Exchange Format
3. X-Road Specifications
4. OpenAPI (Swagger) Specification

Annexure D: Local Standards and Policies

D.1 Nigerian Government Policies

1. National Digital Economy Policy
2. National Broadband Plan

3. e-Government Master Plan
4. National Cloud Computing Policy

D.2 Regulatory Guidelines

1. NITDA Regulations
2. CBN Financial Technology Guidelines
3. NCC Technical Standards
4. NIMC Identity Management Standards

Annexure E: Case Studies

E.1 Global Implementation Examples

1. Estonia's X-Road Implementation
2. India's Digital Public Infrastructure
3. Singapore's National Digital Identity
4. UK's Government Digital Service

E.2 Local Context

1. BVN Implementation
2. NIN Integration
3. Government Enterprise Architecture
4. Treasury Single Account Implementation

Annexure F: Standards Summary Matrix

Table F.1: Comprehensive Standards Summary

Section	Standard Category	Key Requirements	Compliance Level	Monitoring Frequency
Core Principles	Interoperability	- Standardised APIs - Common data models - Business process alignment	Mandatory	Quarterly
	Security & Privacy	- NDPA compliance - ISO 27001 - Privacy by Design	Mandatory	Monthly
	Scalability	- 1,000 RPS normal - 10,000 RPS peak - ≤300ms response time	Mandatory	Daily
	Inclusivity	- WCAG 2.1 Level AA - Multi-language support	Mandatory	Quarterly

		- Offline capabilities		
Service & Architecture	Data Transaction	- NGDX integration - Secure routing - Transaction logging	Mandatory	Daily
	Architecture	- 3-layer architecture - Security servers - Core service isolation	Mandatory	Monthly
Data Standards	Exchange Format	- JSON/UTF-8 - ISO 8601 dates - Standardised metadata	Mandatory	Weekly
	Lifecycle	- Version control - Retention policies - Secure deletion	Mandatory	Monthly

Security	Authentication	- Multi-factor authentication - Authorisation framework - Encryption standards	Mandatory	Daily
	Encryption	- TLS 1.3 - AES-256 - HSM key management	Mandatory	Daily
	API Security	- OAuth 2.0 - Rate limiting - Input validation	Mandatory	Daily
Accessibility	UI Standards	- WCAG 2.1 Level AA - Screen readers - Keyboard navigation	Mandatory	Monthly
	Language	- Multi-language UI - Translation management - Regional formats	Mandatory	Quarterly

	Mobile	- Responsive design - Offline support - Performance targets	Mandatory	Monthly
Performance	KPIs	- 99.99% uptime - ≤300ms response - ≤0.1% error rate	Mandatory	Daily
	Scaling	- Auto-scaling - Multi-region - Load balancing	Mandatory	Daily
	Monitoring	- Real-time metrics - Alerting - Trend analysis	Mandatory	Daily
Testing	Code Coverage	- 80% new code - 100% critical paths - Automated testing	Mandatory	Weekly

	Security Testing	- Monthly VAPT - Quarterly pentest - Annual audit	Mandatory	Monthly
	Performance Testing	- Load testing - Stress testing - Endurance testing	Mandatory	Monthly
Deployment	Infrastructure	- 99.99% uptime - Geo-redundancy - DR capabilities	Mandatory	Daily
	CI/CD	- Automated pipelines - Blue-green deployment - IaC practices	Mandatory	Weekly
	Monitoring	- 24/7 monitoring - SLA tracking - Incident response	Mandatory	Daily
Governance	Compliance	- NDPA - ISO 27001	Mandatory	Quarterly

		- NIST CSF		
	Auditing	- Security audits - Compliance checks - Risk assessments	Mandatory	Quarterly
Training	Documentation	- Technical docs - API references - User guides	Mandatory	Monthly
	Capacity Building	- Training programs - Certification - Knowledge base	Mandatory	Quarterly

Note: This matrix provides a high-level overview of the key standards. For detailed requirements, refer to the respective sections in the main document.

DOCUMENT END
