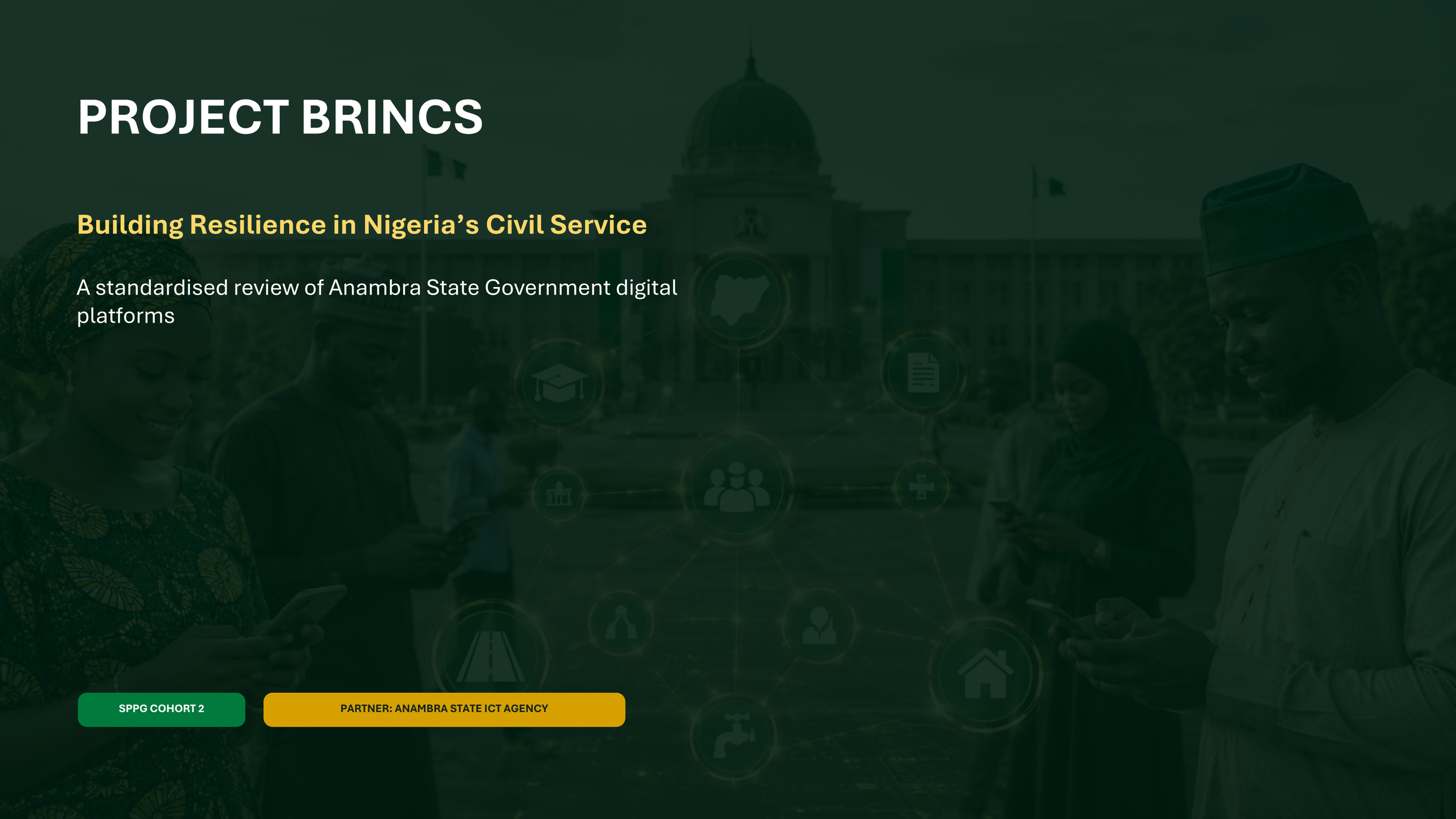
PROJECT BRINCS

Building Resilience in Nigeria’s Civil Service

A standardised review of Anambra State Government digital platforms



SPPG COHORT 2

PARTNER: ANAMBRA STATE ICT AGENCY

The BRINCS story

We began by asking what digital project we could build, but discovered that the deeper need was a system for government to continuously understand, govern and improve the digital services it already has.

17

platform reviews submitted

4

assessment categories

1

standard review manual

From one-off websites → to governed, evidence-based public services

Our name and what it means

BRINCS = Building Resilience in Nigeria’s Civil Service

B Building

R Resilience

I in

N Nigeria’s

C Civil

S Service

> **Resilience means services that continue to work despite leadership changes, technology failures, weak documentation, cybersecurity threats and changing citizen needs.**

Ownership

Standards

Evidence

Security

Feedback

Continuity

Our core belief

A government digital platform is not successful simply because it exists. It succeeds when citizens can find it, trust it, use it, complete a service and receive a response.

Find

Trust

Use

Complete

Response

BRINCS reviewed platforms from the citizen’s perspective, not only the developer’s perspective.

The problem we set out to solve

Can citizens locate and use the platform?

Can users complete the advertised service?

Are security and privacy controls visible?

Can citizens provide feedback or escalate?

Is ownership clear after leadership changes?

Are standards consistent across MDAs?

Without a uniform assessment framework, different government platforms can be built, maintained and evaluated using inconsistent standards.

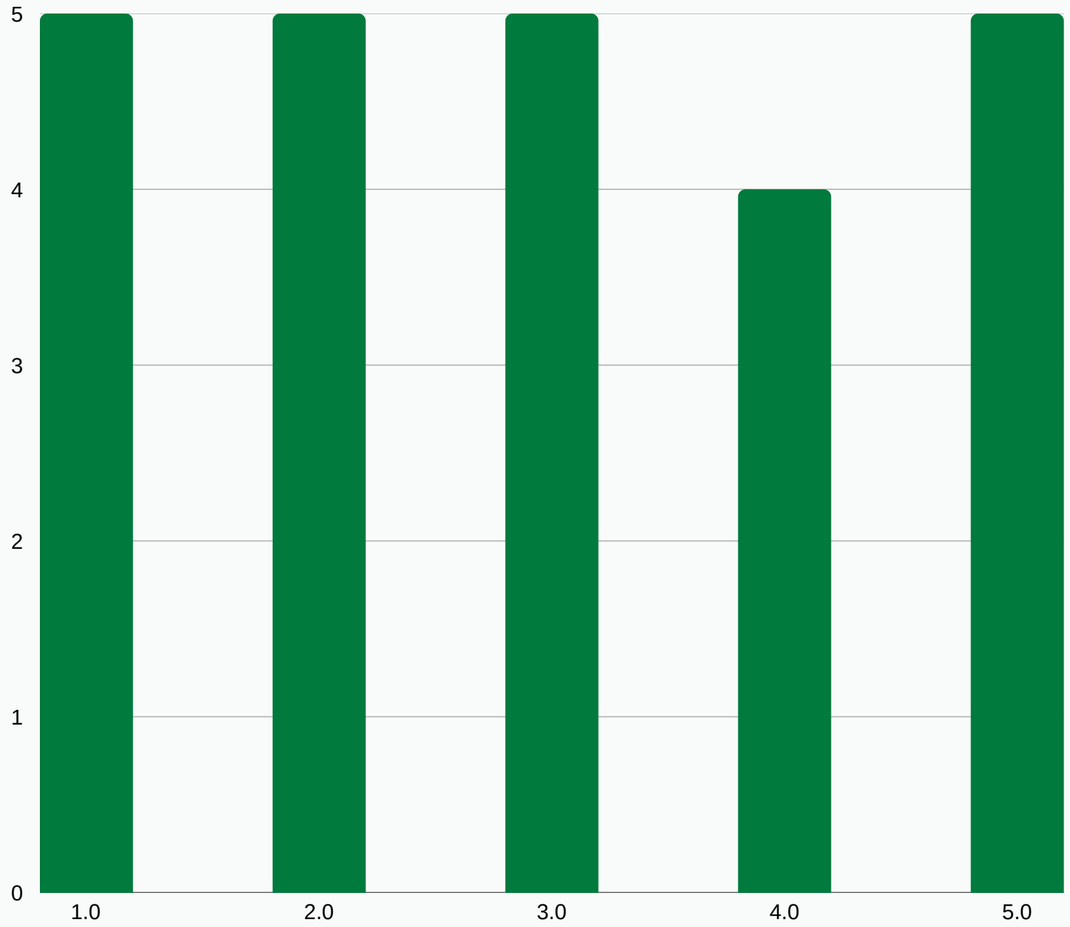
Why this matters for civil-service resilience

- Citizens unable to access essential services
- Public distrust in government technology
- Loss of institutional knowledge when officials change
- Exposure of personal or institutional data
- Abandoned digital assets and duplicated costs
- Exclusion of low-bandwidth or disabled users

understandable even when people and administrations

How we arrived at Anambra State

decision logic, not convenience



Anambra

Stronger partnership readiness, active digital ecosystem, existing ICT entry point and visible institutional impact.

Ekiti

Potential recruitment-digitisation opportunity, but with heavier infrastructure needs and an estimated ₦8m server/security requirement.

Decision principle: choose the state where the team could create measurable institutional value within the capstone timeline.

Partners and stakeholders

who the work touched

Principal institutional partner

Anambra State ICT Agency

SPPG / Capstone

BRINCS Team

Platform-owning MDAs

Citizens / Users

The ICT Agency served as the coordinating government entry point and potential owner of the review framework after the capstone.

The project team: roles and contributions

coordination + technical + documentation streams

Esther Ndife — coordination, ICT Agency engagement, platform inventory, consolidation

Tim Oladoyinbo — technical criteria, training, security guidance, minimum standards

Dorcas James — workflow proposal, process documentation, sustainability input

Lailah Gumbi — help-desk, FAQ, knowledge-transfer materials

Hanifa BabaSadiq — capstone alignment, meeting documentation, circulation

13

contributors listed in project records

2

review streams: technical + non-technical

1

shared mission: resilient digital services

Decision journey and project evolution

April–June 2026

13 Apr

State options compared

Anambra vs Ekiti

20 Apr

ICT Agency priorities understood

recruitment, testing, maintenance

27 Apr

Direction selected

hybrid review + workflow

4 May

Deliverables agreed

manual, report, continuity docs

11 May

Review model defined

technical + non-technical

25 May

Accountability reset

tasks, access, participation

1 Jun

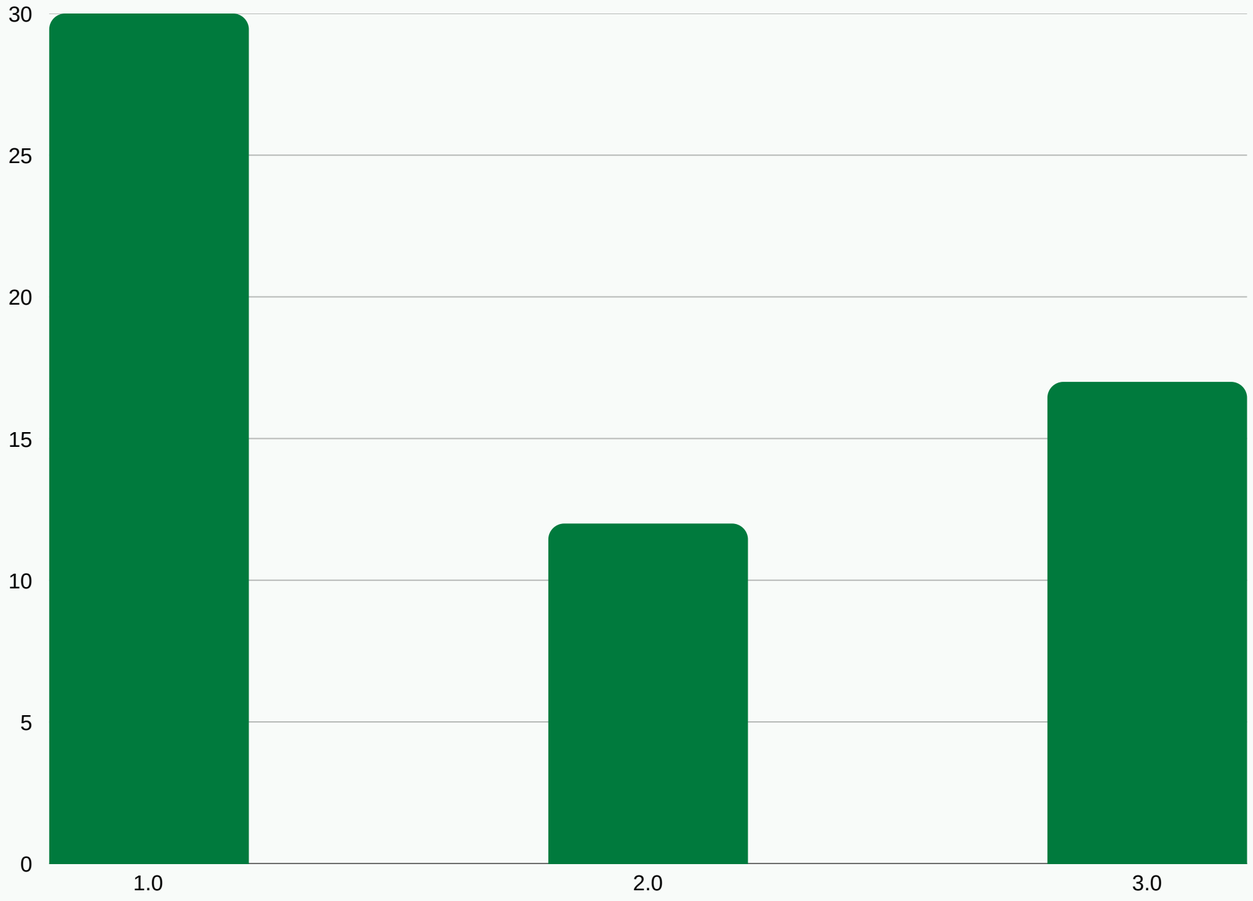
Government validation

evidence must be reproducible

Turning point: the ICT Agency asked for stronger, reproducible evidence that could support official MDA communications.

How the scope evolved

from wide scan to focused reviews



30+

government websites and online services initially considered

12

citizen-facing e-services first prioritised

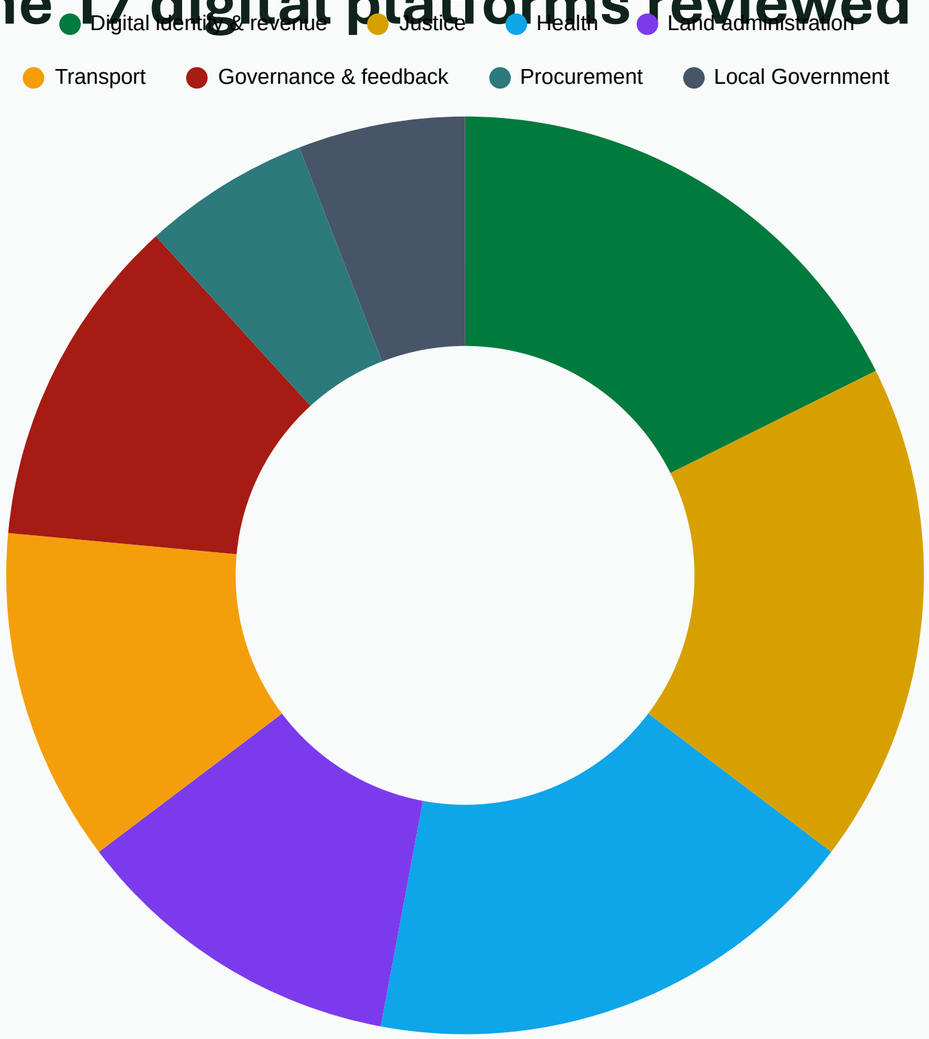
17

platform review documents submitted

The expansion from 12 to 17 shows the team’s increased coverage while keeping focus on high-impact public services.

The 17 digital platforms reviewed

across 8 service clusters



Digital identity & revenue

3 platforms

Transport

2 platforms

Justice

3 platforms

Governance & feedback

2 platforms

Health

3 platforms

Procurement

1 platform

Land administration

2 platforms

Local Government

1 platform

Data-quality note: 3 platform ownership entries still require formal MDA confirmation: GRM, IVAS and Local Government E-Services.

Platform coverage map

what was reviewed and who owns it

Electronic ID App
Anambra State ICT Agency

C of O Online Portal
Ministry of Lands

Ministry of Transport Services
Ministry of Transport

ASIN
Anambra Internal Revenue Service

ANAMGIS
Ministry of Lands

SolutionLens Platform
Anambra State ICT Agency

AIRS E-Tax Portal
Anambra Internal Revenue Service

Telemedicine Platform
Ministry of Health

GRM
TBC

E-Litigation Portal
Ministry of Justice

ASHEFAMU Portal
Ministry of Health

BBP E-Procurement Platform
Bureau of Public Procurement

E-Affidavit Platform
Ministry of Justice

HFWD
Ministry of Health

Local Government E-Services
TBC / Local Government Admin

Lis Pendens Anambra
Ministry of Justice

IVAS
TBC / likely Transport

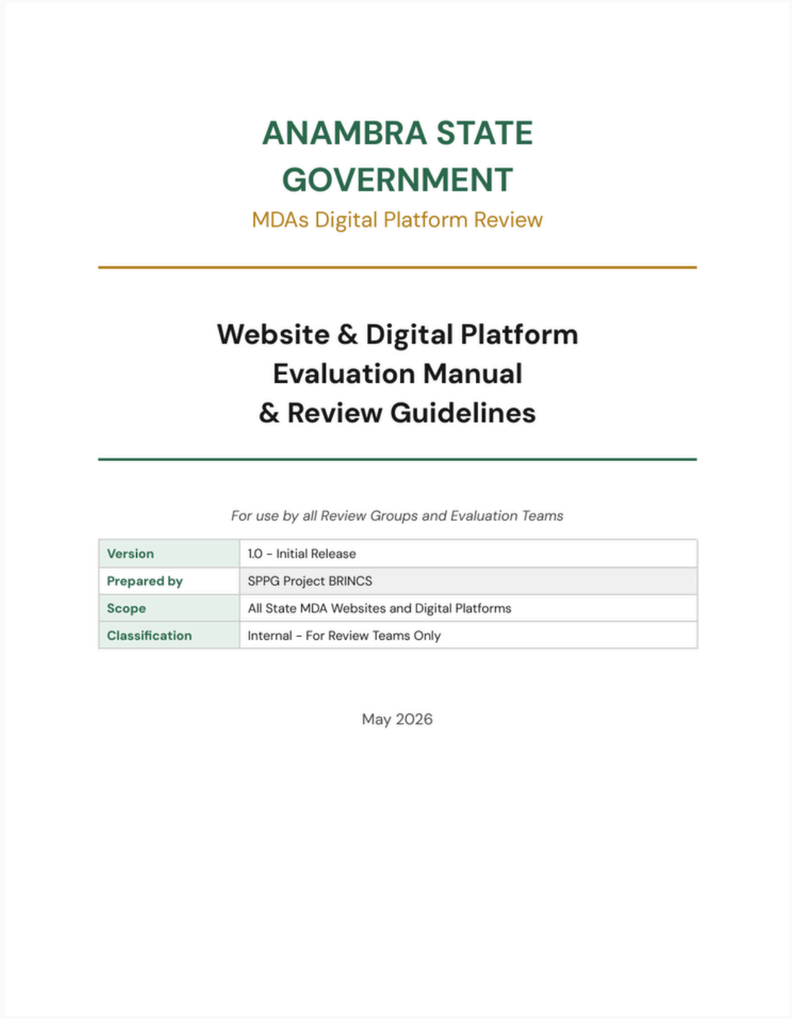
17 PLATFORMS

14 OWNERSHIP ENTRIES CONFIRMED

3 NEED FORMAL CONFIRMATION

The review framework we developed

the core institutional output



ANAMBRA STATE GOVERNMENT

MDAs Digital Platform Review

Website & Digital Platform Evaluation Manual & Review Guidelines

For use by all Review Groups and Evaluation Teams

Version	1.0 – Initial Release
Prepared by	SPPG Project BRINCS
Scope	All State MDA Websites and Digital Platforms
Classification	Internal – For Review Teams Only

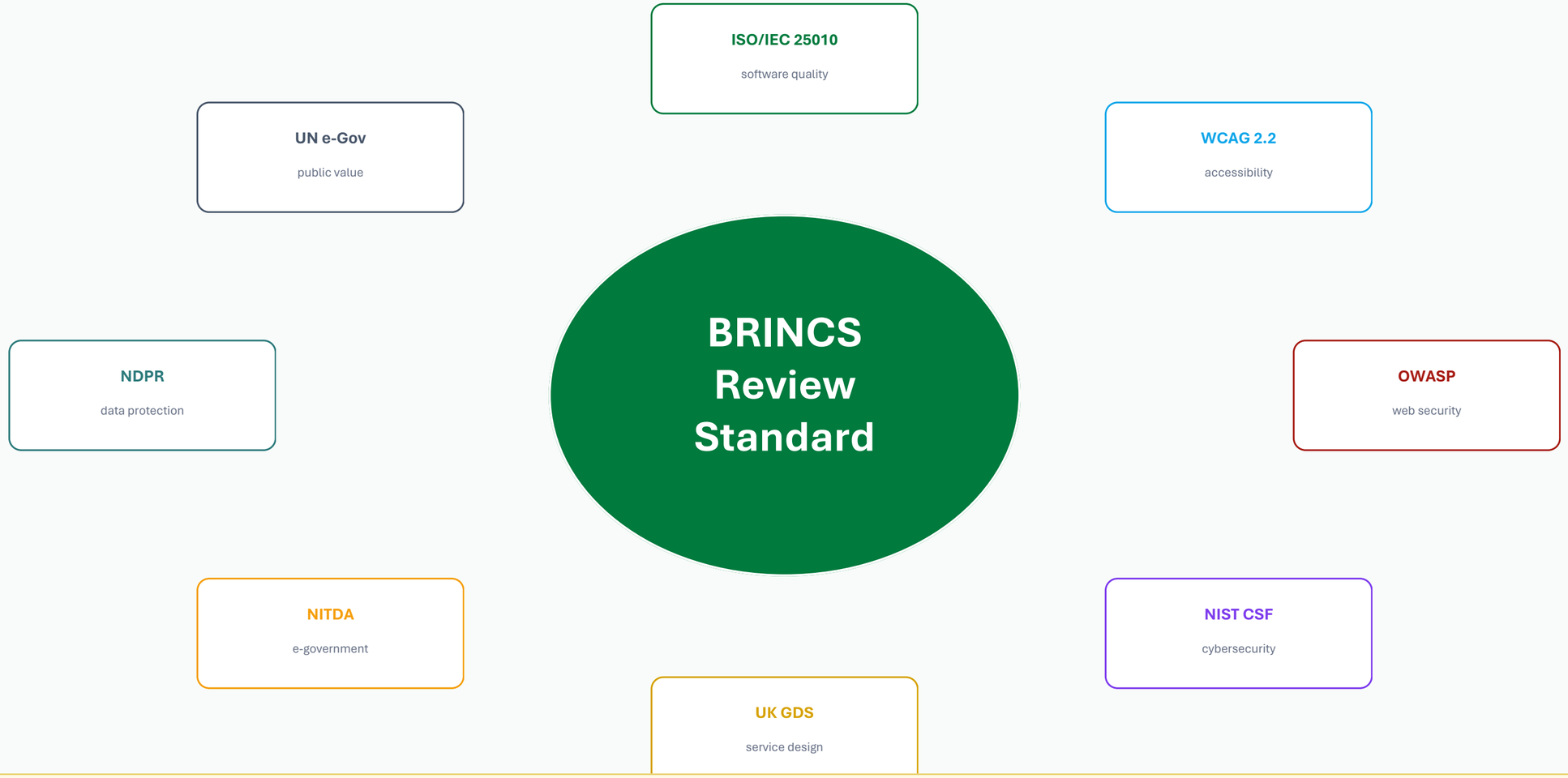
May 2026

- One review document per platform
- Every applicable criterion assessed
- Pass / Partial / Fail / N/A / Cannot Test
- Evidence: screenshots, URLs, error messages
- Severity classification and scorecard
- Submission to a review coordinator

The framework reduces subjectivity and makes findings comparable across MDAs.

Standards that guided the review

global standards adapted to Nigerian public-sector reality



The goal was not to copy foreign standards. The goal was to adapt recognised benchmarks to Anambra’s digital-service context.

The four assessment categories

100-point model

25%

User Experience

30%

Technical & Security

20%

Feedback & Improvement

25%

Purpose Validation

Category 4 asks the toughest question: does the platform actually deliver measurable value to citizens?

Rating and severity model

Pass

Partial

Fail

N/A

Cannot Test

	Critical	Immediate remediation
	High	Major functional/security issue
	Medium	Usability or trust impact
	Low	Minor content/cosmetic issue

scattered website observations into a prioritised

How the team worked

technical + non-technical streams

Inventory

mapped services and MDAs

Assign

split reviewers into workstreams

Test

mobile, desktop, links, forms

Document

screenshots and exact paths

Prioritise

severity and action guidance

Operating guardrail: no hacking, no exploitation; passive checks and citizen-journey validation only.

The evidence model

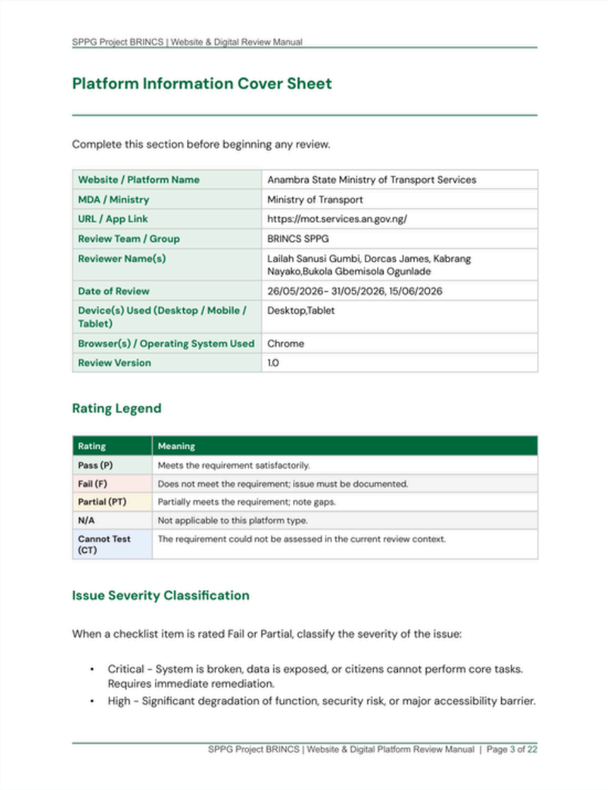
from opinion to reproducible findings

Path — Homepage → FAQ → question

Evidence — screenshot, URL, error text

Context — device, browser, date

Action — severity + recommendation



SPPG Project BRINCS | Website & Digital Review Manual

Platform Information Cover Sheet

Complete this section before beginning any review.

Website / Platform Name	Anambra State Ministry of Transport Services
MDA / Ministry	Ministry of Transport
URL / App Link	https://mot.services.an.gov.ng/
Review Team / Group	BRINCS SPPG
Reviewer Name(s)	Lailah Sanusi Gumbi, Dorcas James, Kabrang Nayako,Bukola Gbemisola Ogunlade
Date of Review	26/05/2026- 31/05/2026, 15/06/2026
Device(s) Used (Desktop / Mobile / Tablet)	Desktop,Tablet
Browser(s) / Operating System Used	Chrome
Review Version	1.0

Rating Legend

Rating	Meaning
Pass (P)	Meets the requirement satisfactorily.
Fail (F)	Does not meet the requirement; issue must be documented.
Partial (PT)	Partially meets the requirement; note gaps.
N/A	Not applicable to this platform type.
Cannot Test (CT)	The requirement could not be assessed in the current review context.

Issue Severity Classification

When a checklist item is rated Fail or Partial, classify the severity of the issue:

- Critical - System is broken, data is exposed, or citizens cannot perform core tasks. Requires immediate remediation.
- High - Significant degradation of function, security risk, or major accessibility barrier.

SPPG Project BRINCS | Website & Digital Platform Review Manual | Page 3 of 22

The ICT Agency requested that findings be reproducible so another officer can verify the same issue without asking the reviewer.

Work completed so far

not just analysis, but reusable government infrastructure

2
states assessed for partnership

17
platform review documents

8
service clusters covered

4
review categories

- Stakeholder engagement with ICT Agency
- Digital-platform inventory and MDA mapping
- Standard evaluation manual and scoring model
- Technical + non-technical review streams
- Issue evidence notes and screenshots
- Reusable roadmap, FAQ and sustainability recommendations

Impact signal: the ICT Agency indicated the findings could inform official letters or memos to MDA heads.

Challenges faced — and how the team adapted

Unclear project direction	hybrid review + workflow approach
Large platform ecosystem	prioritised citizen-facing services
Restricted platform access	front-end and passive checks + CT ratings
Unavailable or warning pages	documented errors and escalated access issues
Inconsistent early evidence	rework with paths, screenshots and notes
Participation constraints	task tracking and reassignment
Government transition	framed findings for new MDA heads

The challenges were not a side story. They shaped the final value of the project: clearer scope, stronger evidence and a repeatable framework.

Challenge 1: unclear initial direction

build, review, workflow — or all three?

Build a new system

Review existing platforms

Design MDA workflows

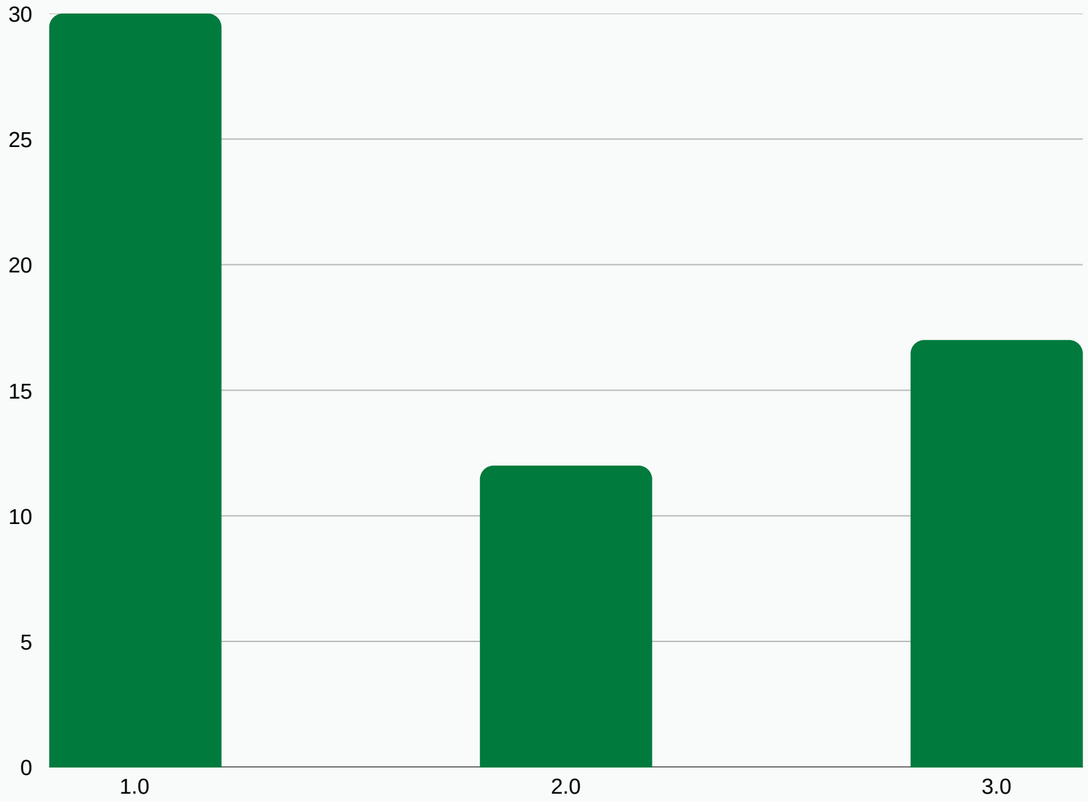
Resolution: a hybrid intervention — credible platform review + reusable standard + continuity documents + workflow thinking.

Why this mattered

- The capstone needed visible impact within a limited timeline.
- Technical fixes required access and government approvals.
- A reusable standard could outlive the project team.
- Workflow thinking supported long-term improvement.

Challenge 2: a very large digital ecosystem

too much to review deeply at once



- Prioritise direct e-services
- Assign checklist areas
- Separate technical/non-technical work
- Focus on high-impact user journeys

The work became focused enough to complete, but broad enough to reveal cross-platform patterns.

Challenge 3: restricted access to core journeys

login walls limited end-to-end validation

Login credentials

Authorised accounts

Demo access

Internal records

Response: front-end functional testing, passive security checks, “Cannot Test” ratings and access escalation through the ICT Agency.

The team explicitly avoided unauthorised backend testing, source-code review, database access or vulnerability exploitation.

Challenge 4: platforms down or difficult to reach

availability itself became a finding

404 errors

Browser warnings

Changed addresses

Inconsistent access

- Recorded exact URLs and error messages
- Separated “down” from browser/security warning
- Escalated inaccessible platforms
- Recommended uptime and certificate monitoring

Example: the Grievance Redress Portal returned a 404 during review, preventing meaningful assessment of its interface and service journey.

Challenge 5: inconsistent early evidence

Before

- Pass/Fail only
- brief comments
- no screenshot
- no navigation path

After

- exact path
- screenshot/URL
- device/browser/date
- severity + action

Homepage → scroll to FAQ → select question → observe template/dummy content

Challenge 6 & 7: people constraints and government tra

60%+

previous appointees replaced after state retreat

7

documented project challenges

3

ownership entries needing confirmation

1

answer: documentation over memory

- Weekly meetings reinforced
- Absences expected to be communicated early
- Named owners and technical contacts recommended
- Tasks tracked and reassigned when needed
- Findings framed for incoming MDA heads

This is why BRINCS focused on institutional memory: platforms must survive personnel and administration changes.

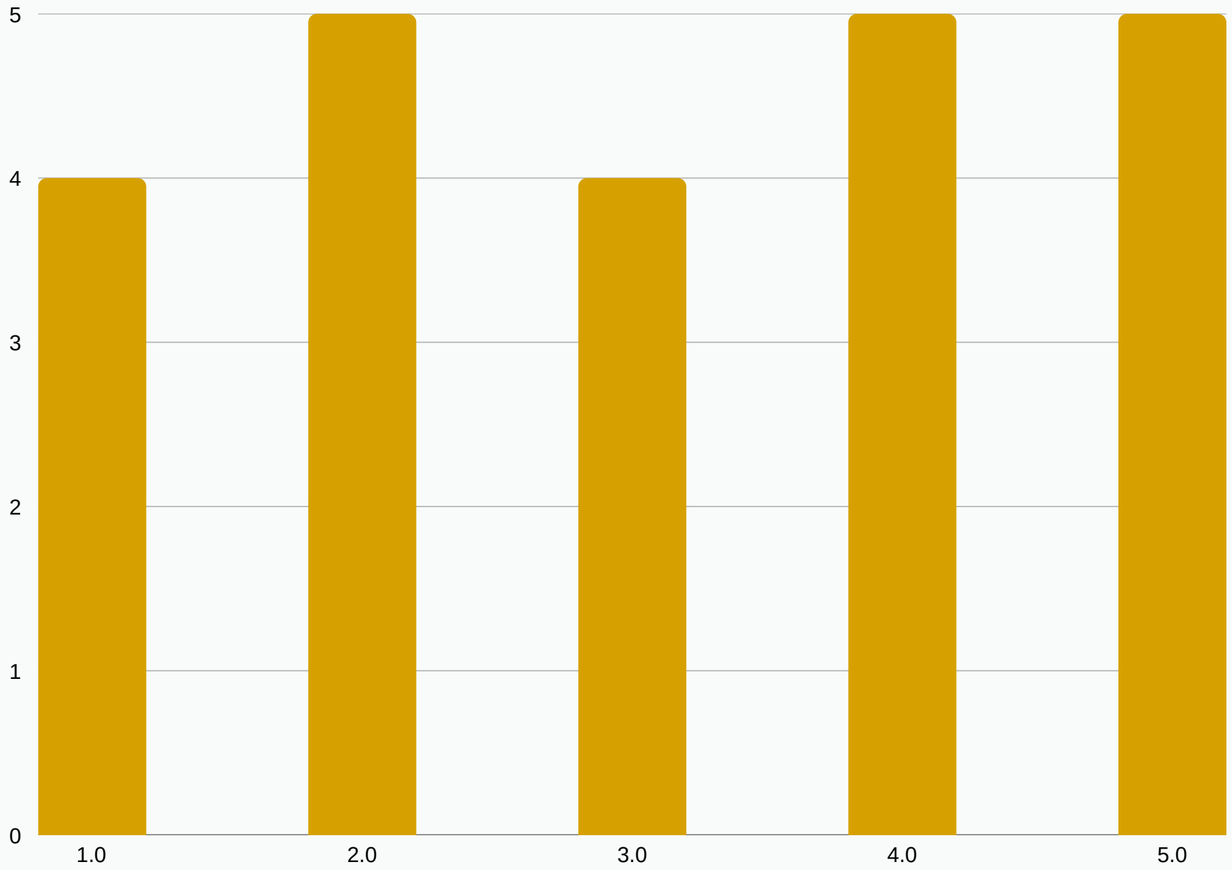
Cross-platform strengths

- Official government domains
- Citizen-facing service ambition
- Mobile-responsive signs
- Functioning forms on selected platforms
- State branding on several platforms
- Transactional e-service direction

The issue is not absence of digitisation. The issue is the need for stronger platform governance, security, feedback and continuous improvement.

Recurring user-experience gaps

where citizens may get stuck



- Long blocks of text instead of clear sections
- Public-facing typos and unclear instructions
- Login walls preventing access to basic information
- Inconsistent branding and trust signals

Example: the Ministry of Transport Services review found mobile content overlays, dummy FAQ material, missing alt text, template links and weak error handling.

Recurring security and privacy gaps

risk signals from passive checks

#	Check Item	Pass/Fail/ N.A.	Notes / Evidenc
1	Overall SecurityHeaders.com grade is C or above (target: A or B)	Fail	The review resulted in a grade of D
2	Content-Security-Policy (CSP) header is present	Fail	
3	X-Frame-Options or CSP frame-ancestors directive is set (prevents clickjacking)	Fail	
4	X-Content-Type-Options: nosniff header is present	Fail	
5	Referrer-Policy header is present	Fail	
6	Permissions-Policy header is present	Fail	
7	Server header does not expose the web server version (e.g., Apache/2.4.41)	Pass	
8	X-Powered-By header is not exposed (e.g., PHP/7.4)	Pass	

2.4 Information Exposure & Data Handling

#	Check Item	Pass/Fail/ N.A.	Notes / Evidenc
1	robots.txt file does not expose sensitive paths (e.g., /admin, /backup, /config)	Pass	
2	No directory listing is enabled on the server (test by appending /images/ or similar paths)	Pass	
3	Error messages do not expose file paths, database names, or stack traces	Pass	User-authenti ted images ma still need to be reviewed.
4	No sensitive files are publicly accessible (e.g., .env, .git, wp-config.php, database dumps)	Pass	
5	Source code comments do not contain credentials, API keys, or internal IP addresses (view page source)	Pass	
6	No personally identifiable information (PII) is exposed in page source or URLs without encryption	Pass	
7	Login or admin portals are not easily discoverable via common paths (/admin, /wp-admin, /login)	Pass	

2.5 Authentication & Access Controls (where applicable)

Only assess this section if the platform has a login or user portal.

- Missing CSP
- Missing clickjacking protection
- Missing nosniff header
- Missing Referrer Policy
- Missing Permissions Policy
- Unclear patch ownership

Security finding ≠ confirmed compromise. It means basic protective controls and evidence of security governance need strengthening.

Accessibility gaps

Image alt text	often missing or unclear
Keyboard navigation	requires deeper technical testing
WAVE testing	not fully completed in several reports
Accessible documents	PDF/HTML alternatives need review
Login-gated services	can exclude without guidance

Accessibility is not optional.

Recommendation: treat accessibility as a second-phase priority with WAVE, keyboard and screen-reader testing.

Feedback and support gaps

Contact form	often present
Confirmation	often weak / missing
Response time	often weak / missing
Escalation	often weak / missing
Improvement evidence	often weak / missing

> acknowledge, respond or escalate is not operating a

CATEGORY 3 **FEEDBACK & CONTINUOUS IMPROVEMENT**

Citizen Feedback · Support Channels · Update Cadence · Analytics Readiness

3.1 Overview & Purpose

A government digital platform is not a finished product; it must evolve based on cit
usage data. This category assesses whether mechanisms are in place for the p
problems, provide input, and for the MDA to demonstrably act on that input. An inter
with no feedback loop is a monologue, not a service.

*Framework references: UK GDS Service Standard Principle 10 (iterate and improve); ISO/
Maintainability; W3C QA Framework; NITDA e-Government Interoperability Framework (e*

3.2 Citizen Feedback Mechanisms

#	Check Item	Pass/Fail/ N.A.	No
1	A contact form or feedback form is accessible from all major pages	Pass	Co ava
2	The form functions correctly, and submission completes without errors	Pass	Fur pro
3	Submitter receives a confirmation message or email after submitting feedback	Fail	No em
4	An expected response timeframe is stated (e.g., 'We respond within 3 working days')	Fail	No
5	Multiple contact channels are available (e.g., phone, email, physical address, not just a web form)	Pass	All cha ava
6	Social media links in the footer/header are active and lead to verified accounts	Fail	The soc ico are
7	A complaint or escalation mechanism is described (e.g., who to contact if unsatisfied with a response)	Fail	No me ava

3.3 Operational Responsiveness

Maintenance and transparency gaps

online does not mean maintained

Recent updates

evidence often limited or absent

News / service announcements

evidence often limited or absent

Annual reports / performance data

evidence often limited or absent

Named platform owner

evidence often limited or absent

Named technical vendor

evidence often limited or absent

Analytics ownership

evidence often limited or absent

A platform can remain online while slowly becoming outdated, unsupported or disconnected from current government structures.

Inclusion and trust gaps

Igbo-language support	limited evidence for critical services
Official endorsement	missing or unclear on some platforms
State logo / branding	not consistent across platforms
Verified contact channels	not always visible
Rural/low-bandwidth users	needs stronger design consideration

Trust is a design requirement in public-sector platforms.

If citizens cannot confirm that a platform is official, safe and supported, adoption suffers.

What the findings mean for citizens

where platform gaps become real-life friction

Find

confusion about official platform

Trust

fear of submitting data

Use

mobile/layout/access issues

Complete

service journey breaks

Hear back

no confirmation or response time

The real test is not whether the platform loads. The test is whether the citizen achieves the intended outcome.

What the findings mean for government

- Central platform register
- Minimum security standards
- Service-level agreements
- Accessibility compliance
- Shared design system
- Performance reporting
- Lifecycle maintenance budget
- Formal handover process

Without these controls, digital projects depend on particular people, vendors or administrations instead of stable institutions.

The value BRINCS has created

Common language

Pass, Partial, Fail, severity and evidence

Repeatable process

future teams do not start from zero

Accountability

issues can be assigned to owners

Institutional memory

survives personnel changes

Basis for official action

findings can support MDA memos

Continuous improvement

quarterly or annual repeat reviews

BRINCS created a baseline, a standard, an evidence model and a path to accountability.

Immediate recommendations

first 30 days

Confirm ownership — policy, content, technical and vendor contacts

Restore availability — 404s, certificates, broken journeys

Remove public defects — dummy text, broken links, typos, inactive icons

Complete evidence — screenshots, paths, devices, severity

Complete scorecards — validate before public ranking

30

days to establish ownership + fix critical public defects

Short-term recommendations

31–90 days

Security

headers • SSL/HTTPS • sessions • authorised testing

User experience

mobile overlays • homepage purpose • breadcrumbs • branded 404

Feedback

auto-acknowledgement • response times • escalation routes • active social links

Accessibility

WAVE testing • alt text • heading structure • form labels

Goal: convert the review into visible service-quality improvement within one quarter.

Medium-term roadmap

3–12 months

The medium-term work is about institutionalising the standard, not just fixing one platform.

1

Digital Service Standard

state-wide minimum requirement

2

Asset Register

single source of truth for platforms

3

Quarterly Health Reviews

repeat assessments and remediation tracking

4

Shared Design System

consistent public-sector interface

5

Monitoring & Analytics

uptime, certificates, usage, feedback

6

Lifecycle Budgeting

maintenance, backup, recovery and handover

Proposed governance model

clear roles, shared accountability

ICT Agency

platform register • standards • audits • domain/hosting policy • MDA capacity support

MDA Owners

content • service ownership • citizen response • funding • performance reporting

Technical Teams / Vendors

security • uptime • updates • backups • bug fixing • deployment documentation

Each platform should have named policy, content, technical and support owners.

Remediation priority model

fix what blocks service and trust first

P1	**Critical service availability**	platform down, invalid certificate, core journey impossible
P2	**Security and privacy**	missing protective controls, unclear data handling
P3	**Citizen journey**	broken forms, unclear instructions, mobile barriers
P4	**Feedback and accountability**	no confirmation, response time or escalation
P5	**Content and presentation**	typos, dummy text, missing logo, inactive social links

Remediation must follow citizen risk, not ease of fixing.

Sustainability plan

- Transfer manual
- Controlled repository
- Review coordinator
- MDA focal persons
- Repeat assessments
- Remediation tracker
- Updated checklist
- Sensitive findings restricted

The review should become a recurring governance practice, not a one-time school project.

How success should be measured

dashboard indicators for future reviews

Availability

platform uptime

Security

critical issues resolved

Ownership

named owners

Accessibility

WAVE/keyboard pass

Feedback

acknowledgement + response time

Maintenance

updated content + patch plan

Adoption

service completion success

Trust

official identity and contact clarity

Future success is not “number of websites reviewed”; it is improvement in service availability, security, accessibility, response and completion.

Resilient digital government is not built through isolated websites.

It is built through standards, ownership, evidence, maintenance, citizen trust and continuous improvement.

PROJECT BRINCS

BUILDING RESILIENCE IN NIGERIA'S CIVIL SERVICE