DAMILARE ADENOLA AND CO LAW PRACTICE

LAW FOR WHAT AFRICA IS BECOMING

Client Alert

NITDA's Software Quality Assurance Framework

Compliance Implications for Tech Firms, Government Contractors, and Regulated Entities

PRACTICE AREA	JURISDICTION	ISSUED
Technology & Regulatory	**Federal Republic of Nigeria**	**31 July 2026**

EXECUTIVE SUMMARY

00 Overview

IN BRIEF

The National Information Technology Development Agency (NITDA) has launched the National Software Quality Assurance (SQA) Framework — a regulatory instrument issued under the NITDA Act 2007 establishing Nigeria's first comprehensive, mandatory regime for the development, testing, and certification of software deployed by government agencies and, on a broader footing, private sector operators.

From **Q2 2027**, no Federal Government software project will obtain IT Project Clearance without independent, third-party certification issued by a Licensed Software Testing Organisation (LSTO) accredited by NITDA. The Framework also creates Nigeria's first formal licensing regime for entities providing software testing services.

This alert examines the background, structure, and scope of the Framework, and sets out its practical implications for technology firms, government contractors, and regulated private entities.

01 Background & Regulatory Context

NITDA derives its regulatory authority from the NITDA Act 2007, which empowers the Agency to develop, regulate, and advise on information technology practices and standards across Nigeria. The Agency has, for over a decade, expressed concern over the prevalence of substandard and inadequately tested software within both public procurement and the wider Nigerian digital economy.

As early as 2016, NITDA operated a software testing laboratory and encouraged penetration testing and certification, particularly within the banking, insurance, and pension sectors, in response to a documented rise in data breaches and system failures. That earlier initiative, however, remained largely voluntary and lacked a formal licensing architecture for third-party testers.

> *"The Framework is intended to reduce the incidence of costly information technology failures, strengthen national cybersecurity, and improve public confidence in digital government services."*

— Statement attributed to NITDA's Director of Corporate Communications and Media Relations, Mrs Hadiza Umar, and a directive signed by the Director-General, Mallam Kashifu Inuwa Abdullahi.

The SQA Framework represents a considerably more formalised evolution of NITDA's earlier policy objective, building a permanent licensing architecture around what was previously a voluntary practice.

02 Structure of the Framework

The SQA Framework is not a single instrument but an umbrella comprising three interlocking guidelines, each addressing a distinct stage of the software lifecycle. These instruments are expressly intended to be read together and jointly constitute the Framework.

01

National Software Development Guideline

Prescribes structured software development lifecycles, secure coding practices aligned with OWASP standards, standardised system documentation, and compliance with WCAG 2.1 AA for citizen-facing digital platforms.

02

National Software Testing Guideline

Introduces mandatory pre-deployment testing standards covering functionality, cybersecurity, performance under peak operational load, and interoperability with existing systems.

03

STOL Guideline

Establishes the regulatory regime for accreditation and licensing of Licensed Software Testing Organisations (LSTOs) — the independent bodies responsible for evaluating and certifying software prior to deployment.

03 Scope of Application

A careful reading of the STOL Guideline indicates that the Framework's scope is considerably broader than its government-facing headline suggests. Section 5.0 of the Guideline provides that it applies to all software testing organisations seeking to provide testing services within Nigeria, and to all entities engaging such services for the development, deployment, or operation of software systems. No express limitation confines this scope to Federal Government projects.

Key Point

The mandatory IT Project Clearance requirement is the enforcement mechanism specific to government procurement — but the underlying classification and licensing architecture is, on its face, sector-agnostic.

The Guideline's risk-based classification methodology assigns software of any provenance — public or private — to one of three tiers, using a weighted, five-dimension scoring matrix (safety & criticality, regulatory requirements, architectural complexity, data sensitivity, and performance/availability). The quantitative thresholds below determine tier placement in practice.

TIER	QUALIFYING THRESHOLDS	REPRESENTATIVE SYSTEMS
Class A	*Any one* of: >100,000 active users or >50,000 concurrent users; >₦100m daily transactions or >₦10bn assets managed; database >10TB or >1m transactions/day; >15 external integrations; or subject to 2+ mandatory certifications (e.g. PCI-DSS + ISO 27001).	Core banking platforms, national identity systems, national payment switches, air traffic control.
Class B	10,000–100,000 active users or 1,000–50,000 concurrent; ₦10m–₦100m processed daily; database 1TB–10TB; 5–15 external integrations; NDPR plus one industry standard.	Corporate ERP systems, large e-commerce platforms, state government portals, insurance administration.
Class C	*All* of: <10,000 active users and <1,000 concurrent; <₦10m daily transactions; database <1TB; ≤5 external integrations; basic business compliance only.	Small business websites, departmental tools, non-critical mobile applications.

Automatic Class A Triggers

Regardless of scale, software is automatically Class A if it is safety-critical (e.g. medical devices, aviation), forms part of national critical infrastructure (power grid, water, telecoms core, election systems), processes >₦1bn in daily transactions, supports national security functions, or serves more than five million citizens (e.g. national ID, tax, or pension systems).

Because this matrix is defined by measurable thresholds rather than by ownership, private sector systems meeting these thresholds — particularly in banking, telecommunications, insurance, and large-scale digital platforms — fall within the Framework's conception of high or moderate impact software, notwithstanding the absence of an explicit private sector mandate. Sectoral regulators may, in time, adopt or reference these standards independently of any direct action by NITDA.

The Licensing Regime for Testing Organisations

The STOL Guideline establishes a formal licensing procedure for entities wishing to conduct third-party software testing. Prospective Licensed Testing Organisations (LTOs) must submit an application demonstrating qualifications, experience, and technical infrastructure, following which NITDA conducts a preliminary review, a substantive compliance evaluation, and, where satisfied, issues a licence.

Licensing requirements scale with the risk tier for which accreditation is sought. Organisations seeking **Class A accreditation** must, among other requirements, maintain a minimum of twenty full-time testing professionals, hold recognised certifications such as ISTQB Expert Level and CISSP, CEH, or OSCP for security testing personnel, operate an ISO/IEC 27001-compliant testing facility, and demonstrate prior experience testing at least three Class A systems within the preceding three years. Class B and Class C requirements are correspondingly less onerous.

A licence, once granted, is valid for two years and must be renewed at least six months prior to expiry. NITDA retains supervisory authority through periodic audits and inspections, and may suspend or revoke a licence for non-compliance, misrepresentation, or the certification of software that has not, in fact, met the requisite testing standards. Revocation may also result in public disclosure of the violation.

04 Compliance Timeline

2016

NITDA operates a voluntary software testing laboratory, encouraging penetration testing and certification within banking, insurance, and pension sectors.

2026 — Transitional Period

NITDA conducts nationwide stakeholder engagement and capacity-building programmes, and will shortly issue an Expression of Interest inviting technology firms to apply for licensing as testing organisations.

Q2 2027 — Framework Becomes Mandatory

IT Project Clearance for Federal Government software projects requires independent, third-party LSTO certification. Licence renewal cycles (2-year validity) begin running from first grant.

Practical Note

This transitional window affords both prospective testing organisations and affected government contractors a defined period within which to align their operations with the new requirements before the Q2 2027 deadline.

GUIDANCE

05 Implications & Recommendations

- **Government contractors and technology firms** supplying software to Federal Government institutions should treat the Framework as a material addition to project planning and risk allocation. Procurement timelines, vendor contracts, and budget projections should account for the additional stage of independent testing and certification required prior to deployment from Q2 2027.
- **Contracts with a deployment horizon beyond Q2 2027** would benefit from provisions anticipating this requirement now, including clear allocation of responsibility for testing costs and timelines between parties.
- **Technology firms with the requisite capacity** should consider the licensing regime as a discrete commercial opportunity, and may wish to position themselves to apply for Class A, B, or C accreditation once the Expression of Interest is issued.
- **Regulated private entities** — particularly in banking, insurance, telecommunications, and large-scale digital services — should not read the absence of an explicit private sector mandate as an absence of exposure. Affected entities would be well advised to review existing software development and testing practices against the Framework's standards in anticipation of eventual regulatory convergence.

Conclusion

The National Software Quality Assurance Framework marks a significant and considered expansion of NITDA's regulatory reach over software development, testing, and deployment in Nigeria. While its immediate and mandatory effect is confined to Federal Government software projects through the IT Project Clearance mechanism, its underlying architecture — built around measurable risk and impact thresholds rather than the identity of the software owner — signals a broader ambition to standardise software quality across the Nigerian digital economy.

BOTTOM LINE

Government contractors, technology firms, and regulated private entities alike would be prudent to begin assessing their present and prospective exposure to the Framework well in advance of its coming into full effect in Q2 2027.

ABOUT THE AUTHOR

Damilare Adenola

MANAGING PARTNER, DACO LP

Damilare Adenola is the Managing Partner at DACO LP. His research and advisory work centres on technology and regulatory compliance, corporate and non-profit governance, and public sector engagement within the Nigerian legal system.

This alert is issued for general informational purposes only and does not constitute legal advice. Entities affected by the National Software Quality Assurance Framework should seek specific guidance tailored to their circumstances before taking any action in reliance on its contents.

01

TECHNOLOGY & REGULATORY COMPLIANCE

02

CORPORATE & NON-PROFIT GOVERNANCE

03

PUBLIC SECTOR ENGAGEMENT

CONTACT DACO LP

House TD7, Global Estate
Apo Primary, FCT Abuja

☎ +234 903 750 6418

✉ info@dacolpafrica.com

🌐 www.dacolpafrica.com

@ Dacolpafrica

SOURCES

NITDA, "National Software Quality Assurance Framework" (press statement, 29 July 2026), nitda.gov.ng · NITDA, Software Testing Organisations Licensing Guideline (April 2026), nitda.gov.ng/wp-content/uploads/2026/04/Software-Testing-Organisations-Licensing-Guidelines.pdf · NITDA, National Software Testing Guideline (April 2026), nitda.gov.ng/wp-content/uploads/2026/04/National-Software-Testing-Guideline.pdf