
# Software Testing Organisations Licensing Guideline (STOL Guideline)



**July 2026**

**1.0.** Software Testing Organisations Licensing Guideline **Title**

**2.0.** **Explanatory Note**

Software testing plays a critical role in ensuring that software systems function as intended, meet user requirements, and adhere to quality, security, and performance standards. As Nigeria continues to advance its digital economy, the reliability and integrity of software systems used across both public and private sectors are of paramount importance.

The objective of this document is to outline the licensing requirements and criteria for third-party Licensed Software Testing Organisations (LSTO) in Nigeria. It aims to provide a clear and comprehensive Guideline for the accreditation process, detailing the standards, responsibilities, and qualifications required for licensing. It establishes the compliance and operational requirements for licensed organisations and provides guidelines for monitoring and enforcement. Ultimately, the goal is to ensure that all software developed or deployed within Nigeria meets the highest standards of quality, security, and performance, fostering trust and reliability in the nation's digital infrastructure.

**3.0.** **Objectives**

The licensing of Software Testing Organisations under this Guideline is intended to achieve the following objectives:

- To promote high standards of software testing and quality assurance, ensuring that software systems deployed in Nigeria are robust, reliable, and fit for purpose.
- To establish a clear regulatory structure that ensures testing organisations operate in compliance with applicable legal, ethical, and professional standards.
- To strengthen confidence in software systems used across public and private sectors by ensuring that testing is conducted by accredited and competent entities.
- To foster the growth of local expertise and professional development within the software testing ecosystem, enhancing Nigeria's competitiveness in the global digital economy.
- To promote a structured and competitive market for software testing services, driven by clear standards, best practices, and continuous improvement.

**4.0.** **Authority**

This Guideline is issued by the National Information Technology Development Agency (NITDA) pursuant to its

mandate under the NITDA Act 2007 to develop, regulate, and advise on Information Technology practices, standards, and guidelines in Nigeria.

NITDA is responsible for the overall management of the licensing process, including setting standards, issuing licenses, and conducting periodic reviews and audits.

**5.0.** **Scope**

This Guideline applies to all Software Testing Organisations seeking to provide software testing services within Nigeria and all entities engaging such services for the development, deployment, or operation of software systems.

The provisions of this Guideline shall apply to software systems classified under the defined tiers, including high-impact, moderate-impact, and low-impact systems, as determined by the classification criteria set out in this document.

This Guideline shall also apply to all stakeholders involved in the software testing licensing process, including regulatory authorities, technical partners, and licensed testing organisations.

**6.0.** **Framework Integration Clause**

This Guideline shall be read together with the National Software Development Guideline and the Software Testing Guideline which collectively constitute the **National Software Quality Assurance Framework for Nigeria.**

**7.0.** **Commencement**

This Guideline shall come into effect on a date to be determined and communicated by the National Information Technology Development Agency (NITDA).

Notwithstanding the above, NITDA may provide a transition period for compliance, during which existing Software Testing Organisations and affected entities shall take necessary steps to align with the requirements of this Guideline.

**8.0.** **Definitions**

For the purposes of this Guideline, the following terms shall have the meanings assigned to them below:
**"NITDA"** means the National Information Technology Development Agency, the regulatory authority responsible for the development, regulation, and oversight of Information Technology practices in Nigeria.
**"Licensed Software Testing Organisation (LSTO)" or "Licensed Testing Organisation (LSTO)"** means an

organisation accredited and licensed by NITDA to provide software testing services in accordance with this Guideline.

**"Software Testing Services"** means the processes, methodologies, and activities undertaken to verify and validate that software systems meet specified requirements, including functionality, performance, security, and compliance.

**"Licensing"** means the formal approval granted by NITDA to a Software Testing Organisation to operate and provide testing services under defined standards and conditions.

**"Accreditation"** means the recognition of an organisation's technical competence, capacity, and compliance with prescribed standards for software testing.

**"Certification"** means the formal attestation that an organisation, personnel, or system meets specific standards or requirements, including national or international benchmarks.

**"Tier" or "Class"** means the classification of software systems or testing organisations based on complexity, risk, impact, and operational requirements as defined under this Guideline.

**"Class A / Tier 1 (High-Impact & High-Risk Systems)"** refers to software systems where failure could result in catastrophic consequences, including risks to national security, human safety, or economic stability.

**"Class B / Tier 2 (Moderate-Impact & Medium-Risk Systems)"** refers to software systems where failure may cause significant operational disruption or financial loss without catastrophic consequences.

**"Class C / Tier 3 (Low-Impact & Low-Risk Systems)"** refers to software systems with limited operational impact where failure results in minor inconvenience or minimal risk.

**"Compliance"** means adherence to the standards, requirements, and obligations set out in this Guideline and any applicable laws or regulations.

**9.0. Responsibilities of Licensed Entities**

Licensed Testing Organisations (LSTO) must adhere to the following responsibilities to maintain their licensure:

a. Ensure that all testing processes and practices are aligned with the standards set by NITDA. This includes following best practices for software testing, verification, and validation.
b. Maintain transparent records of testing processes, methodologies, and results. Licensed organisations must be able to provide detailed reports and documentation for audit and review by NITDA.

c. Licensed organisations must commit to continuous professional development, including keeping their staff updated on the latest testing tools, methodologies, and industry trends.
d. Ensure that all software being tested meets the required quality standards. This includes verifying that the software behaves as expected, meets user needs, and complies with relevant regulations.
e. Provide regular reports to NITDA, including information on testing outcomes, issues identified, and actions taken to resolve defects. These reports help ensure that the testing body is meeting its obligations and that software quality is maintained.
f. Licensed organisations must operate within the legal Guideline of Nigeria, including compliance with data privacy laws, cybersecurity regulations, and other relevant legislation.
g. An LSTO shall not undertake the testing of any software developed by the LSTO itself or by any of its subsidiaries, affiliates, or related entities. For each testing engagement, the LSTO shall submit a declaration of no conflict of interest to NITDA together with the testing report. Any breach of this provision shall constitute grounds for the immediate suspension of the licence, pending investigation and any further regulatory action deemed appropriate by NITDA.
h. LSTOs shall maintain strict confidentiality of all client information, including source code, system architecture, vulnerability findings, test data, and personal data obtained during testing engagements. Confidentiality obligations shall be formalised in a written confidentiality agreement before each engagement commences, shall survive the termination of the engagement for not less than 5 years, and shall extend to all LSTO personnel, subcontractors, and tools involved in the engagement. LSTOs shall not retain client source code, data, or vulnerability findings beyond 12 months after engagement completion without the client's written consent

**10.0.** **Licensing Process**

The procedure for Licensing Software Testing Organisations (LSTO) follows a structured process designed to assess an organisation's ability to meet the required standards and operate within the legal and regulatory Guideline. The procedure includes the following key steps:

a. **Application Submission**
Testing organisations seeking licensure must submit an application to NITDA, including information on their qualifications, experience, infrastructure, and compliance with the licensing criteria.

b. **Preliminary Review**
NITDA will conduct an initial review of the application within 15 working days to ensure that the organisation meets the basic eligibility criteria. This includes checking for relevant certifications, experience, and technical competence.

c. **Evaluation of Compliance**
A thorough evaluation will be conducted within 20 working days to assess the organisation's compliance with the governance, operational, and technical requirements as specified by NITDA.

d. **Issuance of License**
If the organisation meets all necessary requirements, NITDA will issue a licence within 10 working days, allowing the organisation to provide software testing services in Nigeria. Where NITDA is unable to comply with any of the stipulated timeline, it shall communicate the reason for the delay to the applicant in writing.

e. **Ongoing Monitoring and Audits**
After licensure, NITDA will conduct periodic audits and reviews to ensure continued compliance with the standards. Any violations or non-compliance may lead to penalties or the revocation of the license.

f. **Renewal Process**
Licenses will have a defined renewal cycle, and testing organisations must submit a renewal application before the expiration of their license. The renewal process will include a review of the organisation's performance, compliance, and any updates to relevant standards.

**11.0. Tiered Accreditation /Licensing Categories**

To ensure compliance with the National Software Testing Guideline, a tiered licensing Guideline for Software Testing Services (STS) organisations has been developed.

This Guideline categorises licensing requirements based on the complexity of software being tested, ensuring alignment with industry best practices and national objectives.

Below are the licensing criteria for each tier, including objective parameters to determine software complexity:

1. **Class A: High-Impact & High-Risk Systems**
2. **Class B: Moderate-Impact & Medium-Risk Systems**
3. **Class C: Low-Impact & Low-Risk Systems**

**Multi-dimensional Classification Matrix**
Software is classified based on **weighted scores** across 5 objective dimensions. Each dimension has clear, measurable criteria.

**Dimension 1: Safety & Criticality Impact**

| Impact Level | Score | Criteria |
|---|---|---|
| **Catastrophic** | 5 | Failure could cause: Loss of life, national security breach, financial collapse (>₦1B loss), permanent environmental damage |
| **Critical** | 4 | Failure could cause: Serious injury, major financial loss (₦100M-₦1B), significant public disruption, breach of sensitive government data |
| **High** | 3 | Failure could cause: Business operational disruption (days), financial loss (₦10M-₦100M), privacy breach affecting >10,000 individuals |
| **Medium** | 2 | Failure could cause: Temporary service disruption (hours), financial loss (₦1M-₦10M), privacy breach affecting 1,000-10,000 individuals |
| **Low** | 1 | Failure could cause: Minor inconvenience, financial loss (<₦1M), privacy breach affecting <1,000 individuals |

| Compliance Level | Score | Regulations/Standards |
|---|---|---|

| | | |
|---|---|---|
| **Mandatory** | 5 | Requires certification under: PCI-DSS, HIPAA, SOX, ISO 27001, AND sector-specific (CBN banking, NHIS healthcare) |
| **High** | 4 | Requires compliance with: NDPA, GDPR, AND industry standards (ISO 9001, ISO/IEC 29119) |
| **Medium** | 3 | Requires compliance with: NDPA OR equivalent data protection regulation |
| **Basic** | 2 | Requires general business compliance (CAC, FIRS) only |
| **Minimal** | 1 | No specific regulatory requirements |

**Dimension 2: Regulatory & Compliance Requirements**

**Dimension 3: Architecture & Integration Complexity**

| **Architecture Level** | **Score** | **Technical Criteria** |
|---|---|---|
| **Distributed & Critical** | 5 | >20 microservices; >15 external system integrations; multi-cloud/geo-distributed; real-time data synchronization required |
| **Enterprise Integration** | 4 | 10-20 services/components; 8-15 external integrations; hybrid cloud/on-premise |
| **Moderate Integration** | 3 | 5-10 services/components; 3-8 external integrations; single cloud provider |
| **Limited Integration** | 2 | 2-5 services/components; 1-3 external integrations; on-premise or single cloud |
| **Standalone** | 1 | Single service/application; no external integrations |

| **Data Level** | **Score** | **Data Characteristics** |
|---|---|---|
| **Highly Sensitive** | 5 | Processes: Biometric data, financial transactions (>₦100M daily), health records, classified government data |

| | | |
|---|---|---|
| **Sensitive** | 4 | Processes: Personal financial data, identity documents, legal records, >100,000 user profiles |
| **Confidential** | 3 | Processes: Personal identifiable information (PII), business intellectual property, 10,000-100,000 users |
| **Internal** | 2 | Processes: Internal business data, non-sensitive user data (<10,000 users) |
| **Public** | 1 | Processes only public/non-sensitive information |

**Dimension 4: Data Sensitivity & Scale**

**Dimension 5: Performance & Availability Requirements**

| Performance Level | Score | Service Level Requirements |
|---|---|---|
| **Mission-Critical** | 5 | 99.99%+ availability; <100ms response time; >50,000 concurrent users; disaster recovery (RTO<1h, RPO<15min) |
| **Business-Critical** | 4 | 99.9% availability; <500ms response time; 10,000-50,000 concurrent users; DR (RTO<4h, RPO<1h) |
| **High Performance** | 3 | 99.5% availability; <1s response time; 1,000-10,000 concurrent users; backup recovery <24h |
| **Standard** | 2 | 99% availability; <2s response time; 100-1,000 concurrent users; basic backup |
| **Basic** | 1 | No specific SLA; <5s response time acceptable; <100 concurrent users |

| Software Class | Score Range | Alternative Classification Rule |
|---|---|---|
| **Class A (High-Impact/Hight Risk)** | 18-25 points | **OR** Any single dimension scores 5 |
| **Class B (Moderate-Impact/Medium Risk)** | 11-17 points | **AND** No single dimension scores 5 |
| **Class C (Low-Impact/Low Risk)** | 5-10 points | **AND** No dimension scores >3 |

**CLASSIFICATION DECISION MATRIX**
**Calculation Method:**
**Total Score =** Sum of scores from all 5 dimensions (Maximum: 25 points)

**Classification Boundaries**

**Automatic Class A Classification (Non-negotiable):**
Software is **automatically Class A** if it meets ANY of these criteria:

1. **Safety-Critical**: Medical devices, aviation systems, nuclear controls, autonomous vehicles
2. **National Critical Infrastructure**: Power grid, water treatment, telecommunications core, election systems
3. **Large-Scale Financial**: Processes >₦1B daily transactions, central bank systems, stock trading platforms
4. **National Security**: Military, intelligence, law enforcement critical systems
5. **Mass Public Service**: Serves >5 million citizens (national ID, tax, pension systems)

**12.0. Class A (High-Impact & High-Risk Systems)**

**Operational Definitions with Quantitative Thresholds**

**Definition:** Systems where failure could result in catastrophic consequences to human safety, national security, economic stability, or public welfare.

**Quantitative Thresholds (ANY ONE qualifies as Class A):**

1. **User Scale**: >100,000 active users OR >50,000 concurrent users
2. **Financial Impact**: Processes >₦100M daily transactions OR manages assets >₦10B
3. **Data Volume**: Database >10TB OR processes >1M transactions/day
4. **Integration Points**: >15 external APIs/systems OR >20 internal microservices
5. **Regulatory**: Subject to ≥2 mandatory certifications (e.g., PCI-DSS + ISO 27001)

**Examples:**

- Core banking systems (Finacle, Flexcube)
- National identity management (NIN)
- Healthcare EHR with patient treatment systems
- National payment switches
- Air traffic control systems

**Class B (Moderate-Impact & Medium-Risk Systems)**

**Definition:** Systems essential for business operations but with limited public safety impact, where failure causes significant disruption but not catastrophe.

**Quantitative Thresholds:**

1. **User Scale**: 10,000-100,000 active users OR 1,000-50,000 concurrent
2. **Financial Impact**: Processes ₦10M-₦100M daily transactions
3. **Data Volume**: Database 1TB-10TB OR 100,000-1M transactions/day
4. **Integration Points**: 5-15 external systems OR 5-20 internal services
5. **Regulatory**: Subject to NDPA compliance + 1 industry standard

**Examples:**

- Corporate ERP systems (SAP, Oracle)
- Medium/large e-commerce platforms
- University management systems
- State government portals

- Insurance policy administration

**Class C (Low-Impact & Low-Risk Systems)**
**Definition:** Systems with limited operational impact where failure causes minor inconvenience or limited financial loss.
**Quantitative Thresholds (ALL must be true):**

1. **User Scale**: <10,000 active users AND <1,000 concurrent
2. **Financial Impact**: Processes <₦10M daily transactions
3. **Data Volume**: Database <1TB AND <100,000 transactions/day
4. **Integration Points**: ≤5 external systems
5. **Regulatory**: Only basic business compliance required

**Examples:**

- Small business websites
- Mobile apps (non-critical functions)
- Departmental tools
- Personal productivity software
- Brochure websites

**Reclassification Asessement**

1. **Presumptive Classification**: Software owners declare classification with supporting evidence
2. **Regulatory Verification**: NITDA may reclassify based on documented assessment
3. **Appeal Process**: 30-day window to appeal classification with additional evidence
4. **Annual Review**: Classification reviewed annually or upon significant system changes

## 13.0. TIERED ORGANIZATIONAL CAPACITY GUIDELINE

**Organizational Licensing Requirements for Software Testing Companies**

**Class A (High-Impact) Testing Organizations**
**1. ORGANIZATIONAL STRUCTURE & GOVERNANCE**

- **Legal Establishment**: Valid CAC registration
- **Organizational Structure**: Must have:
  - Dedicated testing department with clear hierarchy
  - Separate quality assurance and compliance functions
  - Risk management committee overseeing testing operations
- **Experience Portfolio**: Must demonstrate testing of at least **3 Class A systems** in the last 3 years, with:
  - Detailed case studies including testing methodologies used

    - Client references and performance reports
    - Resolution of critical defects found

**2. HUMAN RESOURCE CAPACITY**

- **Minimum Team Size**: 20 full-time testing professionals
- **Certification Requirements**:
    - **Testing Management**: At least 2 ISTQB Expert Level or equivalent
    - **Senior Testers**: Minimum 3 ISTQB Advanced Level certified or equivalent
    - **Security Testing**: At least 5 certified security testers (e.g., CISSP, CEH, OSCP or equivalent)
    - **Performance Testing**: At least 10 certified performance testers
    - submit certification reports to NITDA within five (5) business days.
- **Experience Requirements**:
    - Testing Director: 10+ years experience, 5+ years in testing Class A Solutions
    - Test Managers: 5+ years experience each
    - Lead Testers: 3+ years experience each

NITDA may prescribe additional requirements from time to time

**3. TECHNICAL INFRASTRUCTURE**

- **Testing Labs**:
    - Physical testing facility with controlled access (ISO 27001 compliant)
    - Multiple environment configurations (development, testing, staging, production-simulation)
    - Disaster recovery site with data synchronization
- **Tools** (Must own licenses for Enterprise-grade tools for):
    - **Test Automation**
    - **Performance Testing**
    - **Security Testing**
    - **API Testing**

**4. COMPLIANCE & REGULATORY ADHERENCE**

- NDPA Certified,

- NITDA Indigenous IT Service Providers and Contractors Registration
- ISO/IEC 27001 (Information Security Management)
- ISO/IEC 29119-3 (Testing Documentation) compliance
- CMMI Level 3 or TMMi Level 3

**Class B (Moderate-Impact) Testing Organizations**

**1. ORGANIZATIONAL STRUCTURE & GOVERNANCE**

- **Legal Establishment**: Valid CAC registration
- **Organizational Structure**: Must have:
  - Dedicated testing team with reporting structure
  - Quality assurance function (can be combined role)
- **Experience Portfolio**: Must demonstrate testing of at least **3 Class B systems** in the last 2 years

**2. HUMAN RESOURCE CAPACITY**

- **Minimum Team Size**: 10 full-time testing professionals
- **Certification Requirements**:
  - **Testing Management**: At least 2 ISTQB Advanced Level certified or equivalent
  - **Testers**: Minimum 5 ISTQB Foundation Level certified or equivalent
  - **Specialists**: At least 3 certified security testers, 2 performance testers
- **Experience Requirements**:
  - Test Manager: 5+ years experience testing Class B Solutions
  - Senior Testers: 3+ years experience each

NITDA may prescribe additional requirements from time to time.

**3. TECHNICAL INFRASTRUCTURE**

- **Testing Labs**:
  - Physical testing facility with controlled access (ISO 27001 compliant)
  - Multiple environment configurations (development, testing, staging, production-simulation)
  - Disaster recovery site with data synchronization
- **Tools**: (Must own licenses for Enterprise-grade tools for)

    - **Test Management**
    - **Automation**
    - **Performance**
    - **Security**

**4. COMPLIANCE & REGULATORY ADHERENCE**

- NDPA Certified,
- NITDA Indigenous IT Service Providers and Contractors Registration
- ISO/IEC 27001 (Information Security Management)
- ISO/IEC 29119-3 (Testing Documentation) compliance
- CMMI Level 3 or TMMi Level 3

**Class C (Low-Impact) Testing Organizations**

**1. ORGANIZATIONAL STRUCTURE & GOVERNANCE**

- **Legal Establishment**: Valid CAC registration

**2. HUMAN RESOURCE CAPACITY**

- **Minimum Team Size**: 2 full-time testing professionals
- **Certification Requirements**:
    - **Lead Tester**: minimum of 1 ISTQB Advanced Level certified or equivalent
    - **Tester**: minimum of 1 ISTQB Foundation Level or equivalent
- **Experience Requirements**:
    - Lead Tester: 2+ years experience
    - Testers: 1+ years experience each

NITDA may prescribe additional requirements from time to time

**3. TECHNICAL INFRASTRUCTURE**

- **Tools**:
    - **Test Management**
    - **Automation**
    - **Basic Tools**

**4. COMPLIANCE**

- NDPA Certified,
- NITDA Indigenous IT Service Providers and Contractors Registration

Note: Licensees operating at higher-tier accreditation levels may perform testing and related activities across lower-tier categories. Conversely, lower-tier licensees are not authorised to perform testing or activities designated for higher-tier accreditation levels.

**14.0.** When an LSTO is assigned a Software Testing Service for a Client, a fee will accrue to the LSTO. This fee is subject to the complexity of the software that the LSTO is licensed to test. The licensing fees for each tier are designed to reflect the level of infrastructure, expertise, and resources required to test software of varying complexity. **Licensing Fees**

**15.0.** **High-Impact & High-Risk Systems** **Tiers/Testing Scope/Fee Structure**

Covers large-scale enterprise systems with advanced security, performance, compliance, and integration testing.
₦20,000,000

**Moderate Impact & Medium Risk System**

Covers medium-scale enterprise applications with moderate security, functionality, and performance testing.
₦10,000,000

**Low Impact and Low Risk System**

Covers small-scale applications, web apps, and niche-market software with basic functional and usability testing.
₦2,500,000

**16.0.** NITDA shall maintain an official and up-to-date register of all Licensed Software Testing Organisations (LSTOs). **Public Register**

The register shall include relevant information on licensed entities, including their licensing status, classification tier, and validity period.

Updated information will be recorded in the national database of licensed testing organisations.

**17.0.** **License Validity & Renewal** **Reassessment, Renewal, and Periodic Review**

A License issued to a Licensed Testing Organisation (LSTO) under this Guideline shall be valid for a period of two (2) years from the date of issuance.

To maintain licensed status, LSTOs are required to initiate the renewal process at least six (6) months prior to the expiration of the licence. Renewal is contingent upon the organisation demonstrating continued compliance with all applicable licensing requirements, including the maintenance of requisite resources, infrastructure, and qualified personnel.

Failure to renew a licence before its expiration shall result in the licence becoming invalid, and the organisation shall not be authorised to provide services under this Guideline until such renewal is duly approved by the Agency.

**License Renewal Process**

Steps for License Renewal

1. **Application Submission:**
   · LSTO submits a license renewal application at least six (6) months before the expiration of the current license.
   · Application must be submitted along with the required supporting documents and proof of compliance.
2. **Verification of Compliance:**
   NITDA will review compliance records, including but not limited to the specified requirements, and may prescribe additional compliance obligations or documentation as deemed necessary by the Agency:
   · Testing reports from the past licensing period.
   · Adherence to national and international testing standards.
   · Quality of services provided to clients.
   · Audit history and compliance with security regulations.
3. **Audit and Inspection (if applicable):**
   · NITDA may conduct an on-site or remote audit to ensure continued compliance.
   · Review of infrastructure, personnel qualifications, and testing methodologies.
4. **Approval and License Issuance**:
   · If the LSTO meets all requirements, NITDA will issue a renewed license certificate.
   · Updated information will be recorded in the national database of licensed testing organisations.

**Rejection and Appeal Process**

- If renewal is denied, the LSTO will receive a detailed report on deficiencies.
- The LSTO may appeal within 30 days, providing evidence of corrective actions taken.
- If the appeal is successful, the renewal process will resume. Otherwise, the license will lapse.

**Periodic Audits and Inspections**

Periodic audits and inspections will be conducted by NITDA to assess whether Licensed Testing Organisations (LSTO) are complying with the necessary standards. These audits

will help ensure that organisations maintain the infrastructure, tools, and qualified personnel required for their tier and identify any areas of non-compliance. These audits and inspections are critical for maintaining the integrity of the licensing process and ensuring that organisations continue to operate within the prescribed standards.

**18.0. Revocation of License: Grounds and Procedures**

**Complaints, Sanctions, and Appeals**

The revocation of a license is a serious action taken by NITDA if a software testing organisation is found to have violated the terms of its licensing agreement or fails to meet ongoing requirements.

**Grounds for Revocation:**

- **Non-compliance with Regulations:** Failure to adhere to national and international software testing standards, including compliance with security, data protection, and quality assurance regulations.
- **Failure to Meet Testing Standards**: If it is reported and subsequently discovered that the testing organisation has cleared software for deployment without it meeting the necessary testing requirements as outlined in the testing guidelines, it shall be considered a breach of professional responsibility. This includes but is not limited to, approving software that fails to pass critical tests related to security, performance, functionality, or compliance. Such action will result in the revocation of the testing organisation's license, as it compromises the integrity of the software testing process and puts end-users, clients, and the software ecosystem at significant risk.
- **Misrepresentation**: Providing false information during the licensing or renewal process, including misrepresentation of resources, personnel qualifications, or services.
- **Failure to Perform Testing Services as Committed:** If the organisation consistently fails to deliver software testing services or provides substandard results.
- **Legal Violations**: Violation of any relevant Nigerian laws.

**Revocation Procedure**

Where NITDA has reason to believe that a Licensed Software Testing Organisation (LSTO) has failed to comply

with the requirements of these Guidelines or any applicable law, the following procedure shall apply:

- Notice of Non-Compliance: NITDA shall issue a written Notice of Non-Compliance setting out the specific grounds, supporting evidence, and the corrective measures required. The LSTO shall be afforded a period of thirty (30) days to respond and, where applicable, remedy the identified deficiencies within such period or any additional period as may be determined by the Agency.

- Immediate Suspension in Cases of Serious Misconduct: Notwithstanding paragraph (1), NITDA may immediately suspend an LSTO's licence pending investigation where there is evidence of fraud, false certification, deliberate misrepresentation, or any other serious misconduct that may compromise the integrity of the licensing regime.

- Review and Determination: Upon receipt of the response or the expiration of the response period, NITDA shall conduct a final review through a panel comprising at least three senior officials who were not involved in the initial assessment. The panel shall issue a written determination, stating the reasons for its decision, within thirty (30) days.

- Revocation of Licence: Where non-compliance is established and remains unremedied, or where serious misconduct is proven, NITDA may revoke the licence of the LSTO and remove the organisation from the official register of Licensed Software Testing Organisations.

- Appeal: An LSTO whose licence has been revoked may, within thirty (30) days of receiving the notice of revocation, appeal the decision to an independent Appeal Panel constituted by NITDA. The Appeal Panel may include representatives from relevant professional or industry bodies, as determined by the Agency, and shall issue its decision within forty-five (45) days of receipt of the appeal.

- Public Notification and Further Action: NITDA may publish notice of any licence revocation within five (5) business days where it considers such publication

necessary in the public interest. Cases involving fraud, misconduct, or violations of applicable laws may be referred to the appropriate regulatory, investigative, or law enforcement authorities for further action.

- Reapplication: An LSTO whose licence has been revoked shall not be eligible to reapply for a period determined by NITDA, which shall not be less than three (3) years. Any reapplication shall be subject to satisfactory evidence of remediation and full compliance with all applicable requirements.

**Enforcement Actions for Non-compliance**

To maintain the integrity of the licensing Guideline, effective enforcement actions will be taken against Licensed Testing Organisations (LSTO) found to be non-compliant with the regulations. Enforcement actions will be proportional to the severity of the non-compliance and will aim to correct the issues and deter future violations.

- **Enforcement Actions:**
  Warning Notices: For minor infractions, a written warning will be issued, outlining the nature of the non-compliance and the corrective measures required.
- Corrective Action Plans: Organisations found to be in violation will be required to submit a corrective action plan that outlines the steps they will take to rectify the non-compliance. NITDA will monitor the implementation of the corrective actions.
- Fines and Penalties: In cases of serious or repeated non-compliance, financial penalties shall be levied. These fines are intended to serve as a deterrent and to encourage compliance.
- Suspension of License: If an organisation is found to be in severe violation of the licensing regulations or fails to address corrective actions within the stipulated timeframe, NITDA may suspend the organisation’s license temporarily.
- Revocation of License: For the most serious violations, such as fraud, negligence, or persistent non-compliance, the organisation’s license may be permanently revoked, barring it from providing software testing services in the country.
- Public Disclosure of Violations: In cases of serious non-compliance or revocation of license, NITDA will publicly disclose the violation, including the reasons

for enforcement actions, to maintain public trust and transparency.

**This Instrument was signed this 14th Day of July 2026**

**Kashifu Inuwa Abdullahi *CCIE***

Director-General/CEO

National Information Technology Development Agency