Software Quality Security & Testing Services

Service Description

Software Quality, Security & Testing Services is a subscription fee based managed shared service, which offers a highly reliable, scalable, secure, and cost-effective testing platform that state agencies and local government entities (within North Carolina) can utilize 24 x 7 for managing their testing projects and/or fulfilling their functional, user acceptance testing (UAT), performance and monitoring, security, and mobile testing requirements.

Software Quality, Security & Testing Services follows the SaaS “Software as a Service” delivery model to support, maintain, and host a full range of software quality, security & testing tools - PractiTest, Neoload, Tosca, Tosca Mobile, Applitools, Fortify and Dynatrace - to meet the testing demands for today's evolving and highly complex IT business and public facing applications.

Customers of the service can use their own personnel to support their testing requirements or employ testing professionals/subject matter experts (SMEs) provided by Software Quality, Security & Testing Services on a time and materials (T&M) basis or a combination of both. Below are the types of optional testing services available through SQS Testing Services on a T&M basis. For information about annual subscription rates and T&M hourly charges, reference the How Do We Charge section.

Optional Testing Services

Testability Assessment Consulting Services

- Test readiness and optimization assessment
- Requirements verification and review
- Test plan and test framework development
- Software testing lifecycle integration
- Test artifact imports or third-party tool integration into PractiTest
- Specialized (non-default) monitoring configurations
- Setup/configuring off-site Neoload Load Generators/Tosca DEX workstations
- Implementi functional automation framework using Tosca/Tosca Mobile
- Methodologies supported are Waterfall, Agile and Hybrid

Application Test Management Services

- Manual test case development and maintenance
- Data base level verification testing
- Data and Scope related functional testing
- User interface (UI) validation testing
- System integration and functional regression testing
- Cross browser and exploratory testing
- Defect management and status reporting
- Test execution and test results reporting
- Create customized project reports and dashboard for status monitoring
- Integration with third party tools using Rest API

Application Test Automation Services

- Automated test script development and maintenance
- Visual Regression testing and analysis
- Writing manual and automation testcases
- Schedule the test runs
- Embed emulators and simulators into mobile testing strategy
- Test across a variety of actual smartphones, tablets, and wearables
- Test native, hybrid, and web mobile applications across any type of devices, operating systems
- Parallel execution on multiple devices at the same time

Application Performance Testing & Analysis Services

- Performance test requirements gathering
- Architecture review and setup server monitors
- Load test scripting and maintenance
- Load, stress and performance testing
- Application bottleneck analysis
- Threshold and capacity analysis
- Configuration and system tuning recommendations
- Test results and analysis reporting

Application Monitoring Services

- Gather application and infrastructure requirements
- Solution proof of concept – host and execution
- Onboard, setup and training of monitoring solutions identified
- Client requirements customization and configuration (including Dashboards)
- Troubleshoot and pinpoint performance bottleneck using Dynatrace (application performance monitoring)
- Access to Knowledge library through Teams channel, documentation, and community practice sessions

Application Security Services

- Runtime Vulnerability Analytics, powered by Davis AI engine which monitors changes in environments like container dynamics, elastic scaling, multi-version deployments, rollbacks and provides precise answers about nature and sources of vulnerabilities
- Runtime Application Protection
- Automatically detects and remediate vulnerabilities
- Full coverage across production rollbacks and outdated release, feature flags and deployment patterns
- Precise and automatic risk and impact assessment with risks prioritized by data access path and actual production execution
- Obtain source code to scan
- Feed source code to static scanner (Fortify Static Code Analyzer or SCA)
- Generate and analyze results, compare vulnerabilities over multiple scans, report, etc.
- Add Templates, Applications and Security Rules

Hours of Availability

This service is available 24/7 via the Web or virtual private network (VPN tunnel) connectivity, excluding planned outages, maintenance windows, and unavoidable events. All the infrastructural and system level changes are performed by the vendors on contract during the agreed standard Sunday maintenance window only. All the changes performed by vendor are pre and post verified by SQS team & it's customers. In addition to the Standard DIT Sunday Maintenance Windows, site-specific and service-specific changes may be coordinated with customers at non-standard times.

Customer Responsibilities

- Identify and provide a primary point of contact for the DIT Software Quality, Security & Testing Service Owner for initiating SQS service delivery, coordination and implementation activities
- Provide a qualified person to participate as needed in the governance and oversight process for the Software Quality, Security & Testing service. This person will represent the interests of the Agency via a governance process for defining and shaping the strategic and tactical evolution of the service.
- Customers using SME testing resources provided by the Software Quality, Security and Testing services will be required to provide application design information as well as functional and/or performance requirements to the SQS Testing service team in order to facilitate the test planning and test execution activities.
- Agency applications being tested using the SQS Testing service will be hosted by the owning agency, not by the SQS Testing service.
- Support requests relating to the use of the service will be initiated by opening an incident or request ticket with the DIT Service Desk.

Global Service Levels

- Global Service Levels include the general areas of support that are applicable to every DIT service.
- The purpose of the Service Level Agreement (SLA) is to document support provided for all DIT services in the Global Service Levels, document the service provided in the Service Description and document any optional customer specific requirements (additions or changes) in the Addendum. However, if there are any differences, information documented in the SLA Addendum takes precedence over the information stated in the Global Service Levels and/or the Service Description.

Service Support

- Hours of Support

  The DIT Service Desk operates 24 x 7 and offers a single point of contact for all customer inquiries related to the State of North Carolina's business and technical infrastructures. The Service Desk agents provide business and technical infrastructure analysis, problem solving, and first and second level diagnostics.

- Contacting Support

  Call the Service Desk at 919-754-6000 or toll free at 1-800-722-3946 or create a ticket with DIT ServiceNow https://ncgov.servicenowservices.com/sp_dit

- Incidents and Service Requests

  - Ticket Creation

    Any critical Incident or critical Service Request should be initiated by calling the DIT Service Desk. If a critical Incident or Service Request is initiated by DIT ServiceNow, it must be followed up with a telephone call to the Service Desk to ensure proper prioritization. When creating a ticket with ServiceNow, summarize the nature of the Incident or Service Request in the Subject field.

    Upon creation of a ticket, the customer will automatically receive through eMail a Receipt Confirmation with the ticket or reference number. This confirmation denotes that the Incident or Service Request has been logged at DIT ServiceNow and that it is being assigned to a work group. The customer is responsible for ensuring that their eMail address is provided to the DIT Service Desk for update and resolution notification purposes.

  - Ticket Prioritization

    The DIT Service Desk assigns a Priority to every Incident or Service Request that is initiated. The DIT Prioritization Model is used to ensure a consistent approach to defining the sequence in which an item needs to be resolved and to drive the assignment of resources.

    The Priority assigned to a ticket depends upon:
    - The Impact on the business: size, scope and complexity of the Incident
    - The Urgency to the business: time within which resolution is required
    - The resource availability
    - The expected effort in resolving or completing a task

  - Incident Target Customer Status Update and Resolution Times

    The following chart shows the Incident Target Customer Status Update and Target Resolution Times by Priority after creation and initial assessment / assignment of a ticket by the Service Desk. Resolution Times are measured in clock hours and/or minutes unless otherwise specified.

- The Target Customer Status Update Time is the time interval that the Service Desk has to update the Customer who reported the Incident on ticket status.
- The Target Resolution Time is the total time from ticket creation to Incident resolution and restoration of service to the user. Service may be restored either by a workaround or by a permanent solution. DIT strives to resolve ninety percent of Incidents within the time frame specified for each Priority.

Priority	Target Customer Status Update Time	Target Resolution Time
Critical	Every 60 minutes or as agreed upon with the Customer(s)	4 hours or less
High	Every 2 hours or as agreed upon with the Customer(s)	8 hours or less
Medium	Upon request	24 hours or less
Low	Upon request	3 business days

- Service Request Target Customer Status Update and Resolution Times
  - **Target Customer Status Update Time**
    For all Priority Levels, the Target Customer Status Update Time will be as agreed upon with the customer upon ticket creation.
  - **Target Resolution Time**
    All Service Requests will require a Target Resolution Date. The date will be entered into the IT Service Management tool upon creation by the Service Desk Agent and will be set based on the provisioning time established for the specific request type. This date should be a mutually agreed upon target date per request type as defined within each customer's Service Level Agreement. In the absence of such date agreements or definitions, the target date will initially be populated with the customer required date and may be revised later as appropriate.

Customer Communication

As previously stated, DIT will update customers as Incidents are being worked and upon Incident resolution. DIT will also provide communications when Incidents or outages occur that may impact the customers through SQS Services Community channels and emails. Customers will be added to the community channels by SQS team as soon as they are onboarded. Customer is also requested to provide the customer resource list those needs to be added to the SQS community channels for communication and SQS service information regarding upcoming change events that have the potential to impact services and lines of business.

Customer Escalation

The DIT Service Desk is the single point of contact for initiating all Incidents and Service Requests, including any requests for ticket escalation. Please contact the DIT Service Desk at 919-754-6000 or toll free at 1-800-722-3946 or create a ticket with DIT ServiceNow https://ncgov.servicenowservices.com/sp_dit

The Business and Technology Services Leader assigned to your agency is available to address any questions you may have about DIT services, processes or information technology business needs. You may contact your Business and Technology Services Leader directly or initiate a Service Request with the DIT Service Desk.

Security Standards and Policies

- DIT services adhere to DIT and State CIO Security Standards and Policies
- The Customer is responsible for ensuring that their systems and services are compliant with and follow State CIO Security Standards and Policies

Business Continuity Plan

DIT has a Continuity of Operations Plan (COOP) to ensure the continuity of critical business functions.

Service Level Reviews

- DIT will use a phased approach in initially conducting Service Level Reviews. Thereviews will be facilitated by the DIT Customer Service group and conducted at a minimum on a quarterly basis or as needed. A Business and Technology Services Leader and the customer will participate in the reviews.
- Service Level Agreements (SLA) will be reviewed, and/or renewed, at least once per year or as required. Customers may request a review of Service Level Agreements at any time by contacting the DIT Customer Service group. The SLA will also require review under any of the following conditions:
    - Whenever there is a significant and/or sustained change to the delivery of the service
    - Whenever there is a significant change requested to the SLA that supports the DIT service
- As a result of these reviews or as other information is provided, Service Improvement Programs will be implemented as needed.

Metrics and Reports

Metrics and reports will be discussed at the Service Level Reviews. Archival of all reports shall follow the records retention schedule adopted by the North Carolina Office of Information Technology Services and the State Records Branch General Schedule, as applicable.

Report Name	Reporting Metric	Reporting Interval	Reporting Source
SLA Report for Incidents Resolved	Resolved incidents within and outside of the SLA; Service	Monthly	Service Management Reporting Tool

	Request Resolution Times		

Dispute Resolution

The Parties (DIT and the Customer) agree that it is in their mutual best interest to resolve disputes informally and amicably. If representatives of the Parties are unable to resolve any dispute after reasonable negotiation, such issue shall be escalated to the respective legal counsel of the Parties, and then, if necessary, to the heads of the respective agencies. If the dispute still remains unresolved, then either Party may seek resolution using the mechanism set out in N.C.G.S. 147-33.93.

Confidentiality

As a result of this SLA, each Party (DIT and the Customer) is likely to have access to information or records of the other Party that is exempt from disclosure under applicable law. Such information shall be deemed “Confidential Information.” Each Party shall maintain all Confidential Information of the other Party in strictest confidence and will not at any time use, publish, reproduce or disclose any Confidential Information, except to the extent necessary to carry out the Party’s duties under this SLA or as expressly authorized in writing by the other Party.

Each Party shall, prior to disclosing any Confidential Information to any contractor or other third party, promptly seek and obtain authorization for the disclosure from the other Party and shall ensure that the contractor or other third party is subject to a non-disclosure agreement enforceable in North Carolina. Nothing in this paragraph is intended to prevent either Party from compliance with any order issued by a North Carolina state or federal court.

Ownership and Custody of Data

All data or other records held or stored by DIT as a result of this SLA shall be considered the property of, and in the custody of, the Customer. In the event of a request made to DIT for access to Customer records pursuant to the North Carolina Public Records Act or by other legal process, DIT will decline such requests and indicate to the requestor that DIT is not the custodian of such records. DIT will refer the requestor to the Customer and will notify the Customer of such request as soon as is reasonable under the circumstances, in order to provide the Customer with an opportunity to state or otherwise argue its own position concerning such request.