General Services Administration
Federal Acquisition Service
Technology Transformation Services
1800 F St NW | Washington, DC | 20405

cloud.gov Support Services

Quality Assurance Surveillance Plan

INTRODUCTION

This Quality Assurance Surveillance Plan (QASP) has been developed to evaluate contractor actions while implementing the Performance Work Statement (PWS). It is designed to provide an effective surveillance method of monitoring contractor performance for each listed objective on the project tasks in the task order. It also provides a systematic method to evaluate the services the contractor is required to furnish.

STANDARD

The contractor is responsible for management and quality control actions to meet the terms of the task order. The role of the COR is quality assurance to ensure task order standards are achieved. The contractor shall perform all work required in a satisfactory manner in accordance with the requirements of the PWS. The COR shall notify the CO for appropriate action if it is likely that the contractor will not achieve successful completion of project tasks in accordance with the performance objectives and acceptable quality levels (AQLs) identified below.

PERFORMANCE REQUIREMENTS MATRIX

The COR will evaluate the performance objectives through surveillance as reflected below by reviews and acceptance of work products and services.

Deliverable or Required Services Performance Standard(s):

Deliverable or Required Services	Performance Standard(s)	Acceptable Quality Level (AQL)	Method of Surveillance
Meet Continuous Monitoring objectives	Participate in FedRAMP security scanning, monitoring, remediation, and authorization activities	Remediation of critical or high issues within 30 days and moderate issues within 90 days	Review by team FedRAMP Liaison and FedRAMP JAB Technical Review staff (monthly)
Assist with troubleshooting unexpected behavior	Assist in troubleshooting problems in the platform's operations during normal business hours. Examples: a customer is unable to bind services, a brokered service is unavailable, a security alert is firing, etc.	Respond promptly during business hours when cloud.gov teammates ask for help with a problem (one business hour) or assign a task in the cloud.gov issue tracking system (one business day).	Manual review of activity and interactions (bi-weekly)
	Assess whether unexpected system behavior is explainable as a routine operational incident or a potential indicator	Be able to provide expert assistance on Cloud Foundry-specific components, including logical reasoning about	Manual review of activity and interactions (bi-weekly)

	of compromise. In the latter case, the contractor will be expected to help gather evidence.	unknown problems and referencing documentation and logs.	
Increase automation and maintainability	Reduce the manual overhead necessary for operating the platform, rotating secrets, performing updates, etc.	Reduced time to handle incidents, make deployments, recover from contingencies, etc. Tangible artifacts: scripts that automate common tasks, automated pipelines in Concourse, document a repeatable procedure, etc.	Combination of manual review, metrics from CI/CD system, and outage reports. (quarterly)
Improve resilience and recoverability	Improve the resilience of the cloud.gov platform and increase likelihood of complete, full recovery in case of a major contingency event.	Improvements to coverage and automation of contingency plan processes. Interpreting errors and minor disruptions as opportunities for automation and	Combination of manual review and results of contingency plan exercises. (quarterly)

		prevention of recurrence.	
Assist with documentation of significant changes	Contribute to documents for compliance review processes.	Meets FedRAMP general document acceptance criteria: https://www.fedramp.gov/assets/resources/documents/FedRAMP_General_Document_Acceptance_Criteria.pdf	Manual review of documents (bi-weekly)
	Assist with producing evidence that the system works as described during compliance reviews.	Participation in scheduled auditing sessions, such as demonstrating how a component works to an auditor.	Manual review of participation (bi-weekly)
Tested Code	Code delivered under the order must have substantial test code coverage and a clean code base.	Minimum of 90% test coverage of all new code. Changes to existing code should not reduce existing coverage.	Combination of manual review and automated testing, using agreed-upon publicly-available SaaS products
Accepted	Functions agreed upon as the Acceptance Criteria for a given user story	All functions appear and operate as expected	Manual review of Government personnel (TTS) for user-facing features and bugs. Some user stories can be accepted by developers
Accessible	Client-side rendering must conform with	0 errors reported for 508 Standards using an automated	http://squizlabs.github.io/HTML_CodeSniffer/ or

	section 508 standards.	scanner and 0 errors reported in manual testing	https://github.com/pa11y/pa11y
Deployed	Code must successfully build and deploy in a reproducible manner	Continuous deployment via pipeline to two logically-isolated environments: (1) staging (representative of the production environment) and (2) production	Combination of manual review and automatic testing
	Minimal outage time for production pushes	Non-database deployments incur no downtime. Deployments which require downtime take no more than one hour and the outage window is announced to customers in advance.	Manual review of deployment
Documented	All dependencies (and licenses for dependencies) are listed and all major functions are documented. System diagram is provided as appropriate to the release.	In order to meet TTS needs as agreed to following initial releases with the Product Owner, COR, and CO	Combination of manual review and automatic testing

Available	Code must be stored in a version-controlled open-source repository.	All of the code needed to deploy and run must be available.	The COR will assess code availability.
Secure code	New code must be free of medium- and high-level static and dynamic security vulnerabilities	Clean tests from a static testing SaaS, such as Gemnasium, and from OWASP ZAP, and/or documentation explaining any false positives.	https://pages.18f.gov/before-you-ship/
System Infrastructure	High uptime	99.99% or higher availability	ELK and Prometheus Monitoring
	Prompt outage notification	Detect any service disruptions within two minutes	Manual review of performance during outage

If any deliverables produced by the contractor during performance fail the quality levels provided above, the contractor will correct those deliverables to meet the specified quality level at no extra cost to the Government.

PROCEDURES

The COR, along with the cloud.gov director and team members as appropriate, will inspect all tasks required by the task order to ensure contractor compliance with the task order requirements at the conclusion of each sprint, which shall have a length of two weeks or less. Delivery will occur by pull request from the contractor’s repository to 18F repositories. If inspection results are satisfactory, the pull request will be merged; otherwise, deficiencies will be noted in the pull request or through issues as described below. The COR may find the delivery satisfactory even though further work is required, provided that the specific requirements of the task are met.

At the conclusion of each sprint, the COR, along with the the cloud.gov director, will review the completed user stories and related functionality. Incomplete or inadequate code and user stories will be noted in a mutually agreed-upon issue tracker, such as Trello or GitHub Issues, and links to each issue shared with the CO. The contractor may respond in that tracker as appropriate, addressing the accuracy and validity of the defect as well as any planned corrective action (if not already noted). The team will discuss and document actions to prevent recurrence in scheduled sprint retrospectives.

At the conclusion of the period of performance, a similar procedure will be followed to document discrepancies and to assess overall performance. If any of the services do not conform to the task order requirements, the COR may require the contractor to perform the services again in conformity with task order requirements. Any work that is not accepted must be completed in the next sprint, unless the cloud.gov product lead agrees to move it to a later sprint. The COR shall not certify satisfactory performance for the task order until all defects have been corrected. When the defects in services cannot be corrected by re-performance, the Government may:

Require the contractor to take necessary action to ensure that future performance conforms to task order requirements; and, reduce the task order price to reflect the reduced value of the services performed. The COR shall, in addition to providing documentation to the CO, maintain a complete quality assurance file. The file will contain copies of all reports, evaluations, recommendations, and any actions relating to the Government's performance of the quality assurance function, including originals of all surveillance activity checklists. All such records will be retained for the life of the task order. The COR shall forward these records to the CO at completion or termination of the task order.

ACCEPTANCE OF SERVICES

Acceptance of services shall be based upon surveillance procedures described in this QASP. Before approving/certifying any contractor invoices, the COR will verify that all invoiced services have been performed in compliance with task order requirements. The COR shall not certify satisfactory performance for the task order until all defects have been corrected.