ANITIAN®

FedRAMP Comprehensive

Cloud Service Provider: AWS

Level: High

1.1. Anitian Continuous Compliance Integrations

During the preparation and integration phase for an initial ATO audit, Anitian will provide access to our "FedRAMP Insights" SaaS application (See Appendix A for Service Level Agreements). This application integrates with Subscriber accounts and environments on AWS to run automated continuous compliance checks across their deployed resources. FedRAMP Insights provides an overview of which resources have been scanned and lists which specific compliance checks have failed to align with FedRAMP compliance standards for a typical AWS environment. With this assessment, Subscriber is better able to prepare their environment for initial ATO reviews and audits.

1.2. Reporting of Findings

Anitian will provide an exportable overview of the compliance state of all environments with which a Subscriber has established integrations, as well as a complete executive summary report of the Subscriber's technical readiness to take on the FedRAMP journey. The dashboard depicts current compliance status based on applicable control families, resource families, or open tasks. It will also indicate blockers / showstoppers to be addressed before the next steps in the FedRAMP journey can be taken. Subscriber will be able to export CSV formatted documents of all latest compliance checks that have been run.

Anitian will facilitate advisory service interviews to assess your application's readiness for FedRAMP through virtual sessions. Team members will assess compliance with key controls, consult on ATO boundary definition and creation and provide recommendations for identified gaps. All information gathered by our compliance team will be bundled into an Executive Summary Report which will be available to Subscriber.

1.3. Compliance Automation Platform

The below table describes the individual components of Anitian's Compliance Automation Platform.

Identity	Certificate Management
	Identity and Access Management
	Internal Domain Name Service
	Multifactor Authentication
Network	Network Firewall
	Proxy (Perimeter Security)
	Remote Access
	Web Application Firewall
	Compliance Guardrails
	Configuration Scanning
	Endpoint Security
	Security Information & Event Monitoring (SIEM)
	Vulnerability Scanning – Containers
	Vulnerability Scanning – OS
	Vulnerability Scanning – DB
	Vulnerability Scanning – Web App

Foundational	Encryption
	File Integrity Monitoring
	Malware Detection
Visualization & Tools	Vulnerability Management Dashboard
	Compliance SLA Dashboard
	POA&M update automation

1.4. Service Level Agreement

During the Term, Anitian shall provide Subscriber with software support and maintenance services ("Support Services") described in this Addendum to the Agreement ("Support Services Schedule"). Capitalized terms not defined in this Addendum will have the meanings described in the body of the Agreement.

1.4.1. Overview

1.2.1.1 Software Support and Maintenance.

Anitian will provide defect identification, analysis, restoration and resolution services for the Software so that the current Release of the Software and one (1) then-prior Release of the Software (with a "Release" meaning a Software version designated by a number to the left of the decimal, e.g., 1.x, 2.x, etc.) will operate and conform to the Documentation. Subscriber acknowledges that Anitian's obligations with respect to Software support apply only to the extent the Software is installed and running in an environment that meets Anitian's minimum technical specifications for the version of the Software used by Subscriber. Anitian has no obligation or other liability for any failure of the Software on any hardware or system that does not meet those specifications.

1.2.1.2 Improvements.

During the Term, Anitian may, in its sole discretion, develop updates, upgrades, enhancements and improvements. Anitian will provide Subscriber with such updates, upgrades, enhancements, and improvements that Anitian generally offers to other Anitian subscribers. Subscriber will be responsible for the installation of any such Improvements and Anitian will reasonably assist Subscriber with the installation of any such Improvements.

1.2.1.3 Error Corrections.

Anitian will use commercially reasonable efforts to correct failures of the Software to perform in materially accordance with its Documentation ("Errors") reported by Subscriber in writing to Anitian. Anitian will diligently research and use commercially reasonable efforts to identify and mitigate potential Errors that are not reproducible. Anitian will utilize remote diagnostic procedures whenever possible for Error diagnosis and Error correction. Anitian may not issue Error corrections for all Errors. Anitian will work with Subscriber on a best effort basis to identify and implement reasonable technical work arounds when possible.

1.2.1.4 Documentation.

Anitian will provide updates as appropriate to the User Guides and other Documentation as required to reflect modifications to the Software.

1.2.1.5 Out of Scope Services.

Support provided at the request of the Subscriber, 'outside the scope of this Agreement, if

any, shall be provided pursuant to Anitian's then-current applicable policies and procedures, including, at a minimum, if applicable, execution of Anitian's then-current license agreements and/or consulting/professional services agreement and payment of Anitian's then-current fees and costs associated with such services. Anitian will obtain Subscriber's prior written consent prior to performing any services that falls outside the scope of this Agreement. Subscriber acknowledges that Anitian is not providing process expertise / support, process change management, cultural change management, corporate or market level communications, market level training or project management with this Agreement. Further, these Support Services do not include any installation, implementation, configuration, business rule changes, customization, or any support for Software Releases that are superseded by three releases or more (e.g., if the current software release is 6.x, then releases 3.x and older will be out of scope). Support for older Releases may be available for additional fees. Any custom Software enhancements requested by Subscriber will be evaluated and, if approved, will be a separate project and statement of work at Anitian's current software development rates. Any installation or implementation services required to install updates or upgrades will be pursuant to a separate statement of work and will be charged additional fees. Furthermore, if an integration component is changed or upgraded, the work needed to update the Software to restore normal operating condition will be considered a Software enhancement.

1.2.1.6 Multivendor Coordination

Anitian's obligation to provide the Support Services described in this Exhibit in accordance with the schedule described in this Exhibit is subject, to the extent necessary, to timely cooperation from Subscriber and Subscriber vendors whose products interact with Software to reproduce and diagnose the problem.

1.4.2. Defect and Service Levels

1.2.2.1 Definitions

The following terms apply for purposes of this Support Services Schedule:

- "Defect" means an Error or flaw in the Software that causes an incorrect and unexpected result based on the design.
- "Response Time" means the time from which the Subscriber reports the Defect until Anitian acknowledges the reporting of the Defect.
- "Restoration" means the return of the Software to a reasonable operating condition determined by both Anitian and Subscriber without providing a Resolution.
- "Resolution" means the return of the Software to a reasonable operating condition with a permanent solution or reasonable workaround.
- "Severity 1 Level Defect" means a Defect during operation of the Software that causes Subscriber to be unable to either use the Software or perform time critical business functions with the Software. There are no available workarounds and Subscriber is operating under an absolute work stoppage situation with respect to the Software.
- "Severity 2 Level Defect" means a Defect during operation that causes Software to stop working properly and there are no acceptable, alternative solutions. While other areas of the Software are not impacted, the reported issue has created a significant, negative, yet non-critical impact on Subscriber's productivity or service level to its customers.
- "Severity 3 Level Defect" means a Defect during operation that does not materially impact a significant number of Subscriber's customers or causes minor limitations to functionality of the Software.

1.4.3. Service Level Targets

Anitian shall achieve the following targets with respect to Response Time, and shall use

commercially reasonable efforts to achieve the following target with respect to Restoration Time and Resolution Time:

Type of Outage	Description	Initial Response	Outage Resolution Procedures
Severity 1 Level	A Defect during operation of the Software that causes Subscriber to be unable to either use the Software or perform time critical business functions with the Software. There are no available workarounds and Subscriber is operating under an absolute work stoppage situation with respect to the Software.	As soon as possible, but no longer than 1 hour	Commence work within four (4) hours after receipt of the Defect notice and sufficient supporting information per Section 3 (Contacting Anitian for Support Services) and dedicate all necessary resources with appropriate technical expertise sufficient for correcting the problem to work on the problem in a diligent and continuous (i.e., 24x7, including weekends and holidays) manner until a fix or workaround is provided to Subscriber; provided, however, that Subscriber acknowledges and agrees that Anitian's obligation to work on the problem in a continuous manner shall not preclude Anitian from relieving individual resources for a reasonable time period. During such period Subscriber will be provided with periodic status reports.
Severity 2 Level	A Defect during operation that causes Software to stop working properly and there are no acceptable, alternative solutions. While other areas of the Software are not impacted, the reported issue has created a significant, negative, yet non-critical impact on Subscriber's productivity or service level to its customers.	As soon as possible, but no longer than 4 hours	Commence work within eight (8) hours after receipt of the Defect notice and sufficient supporting information per Section 3 (Contacting Anitian for Support Services) and dedicate all necessary resources with appropriate technical expertise sufficient for correcting the problem to work on the problem in a diligent and continuous (i.e., 24x7, including weekends and holidays) manner until a fix or workaround is provided to Subscriber; provided, however, that Subscriber acknowledges and agrees that Anitian's obligation to work on the problem in a continuous manner shall not

Type of Outage	Description	Initial Response	Outage Resolution Procedures
			preclude Anitian from relieving individual resources for a reasonable time period. During such period Subscriber will be provided with periodic status reports.
Severity 3 Level	A Defect during operation that does not materially impact a significant number of Subscriber's customers or causes minor limitations to functionality of the Software.	No longer than 1 business day	Commence work within five (5) business days after receipt of the Defect notice and sufficient supporting information and include as a roadmap item for future release.

1.4.4. Access to Subscriber Systems

Anitian will identify in writing those individuals who need access to Subscriber's systems in order to provide support under this Software Support Schedule ("Anitian Support Personnel"). Subscriber will provide those individuals with login credentials to Subscriber's system, including a unique username and password. Anitian will take reasonable security precautions to protect access to Subscriber's systems, including sending notice to Subscriber within 24 hours if any Anitian Support Personnel cease working for Anitian, in order that Subscriber may disable the login credentials. Further, Anitian will comply with Subscriber's reasonable security procedures as provided in writing to Anitian.

1.4.5. Contacting Anitian for Support Services

1.2.5.1 Support Hours

Anitian shall provide email-based support for use by Authorized Users Monday through Friday, 7 am EST to 5 pm PST, US holidays excluded, for problem resolution assistance. This Support is only available to Authorized Users. Subscriber may designate up to three (3) Authorized Users. This support is exclusively for problems with Software and does not include guidance on compliance or assisting Subscriber's auditors.

1.2.5.2 Contact Method

Subscriber may contact Anitian through their Program Manager or via the ServiceNow Platform.

1.4.6. Limitations

Anitian will not monitor any other reporting methods for Support Service issues and cannot guarantee that it will receive or respond to any support contact that is not made by Authorized Users or through the Approved Contact Method. The terms of this Support Services Schedule do not apply to any contact that is made outside of the Approved Contact Method or by a person who is not an Authorized User and Service Levels will not be monitored on any support request that does not use the Approved Contact Method or is not by an Authorized User.

1.4.7. Subscriber Obligations

Subscriber will provide the following to assist Anitian during the defect identification, analysis, restoration and resolution process:

- Adequately skilled and knowledgeable resources. These resources must be available at all times when Anitian is working to remedy a Defect reported by Subscriber (e.g., 24x7 for Severity Level 1 Defects). If Anitian needs additional information or support from the Subscriber to work on a Defect and a Subscriber resource is not available, then the measured time for the Service Levels will stop until the information or support is provided by Subscriber.
- Reasonable remote access to Subscriber's production environment where the Software is installed.
- Reasonable remote access to an up-to-date testing or staging environment where the Software and all integrated applications and required components are installed.

1.4.8. Escalation

If Anitian does not meet the terms outlined above in this Support Services Schedule, the Subscriber may escalate the Defect by requesting an escalation on the ticket via support email a defined under section 3.2.

1.4.9. Reporting

Provided that Subscriber complies with its obligations in Sections 3 and 4 of this Support Services Schedule, then Anitian shall provide the following reporting:

Defects reported by Subscriber through Approved Contact Method will be documented, tracked and prioritized by Anitian. Anitian will provide access to all Defects reported by Subscriber through such methods during the previous month. The information will include the following:

- Defect Number
- Software Name
- Description
- Date Reported
- Time Reported
- Reported By
- Actual Response Time
- Actual Restoration Time
- Actual Resolution Time
- Overall Status
- Root Cause of Defect
- Summary of resolution steps or actions
- Severity Level

1.4.10. Expansion Price(s):

Incremental environment expansion costs for Compliance Automation Platform are as follows:

GB Ingested into SIEM per Month	Annual Cost
Up to 750 GB	$670,000
751 GB – 1,500 GB	$937,000
1,501 GB – 2,2,50 GB	$1,079,400
2,251 GB – 3,000 GB	$1,136,360

ANITIAN

1.5. Compliance and Security Operations

Anitian will perform security and compliance monitoring of the ISE on a 24 hours per day, 7 days per week, 365 days per year basis.

Anitian will manage the Compliance Automation Environment components.

A Compliance and Security Operations subscription requires deployment and provisioning of Anitian proprietary, security monitoring and detection capabilities into the environment.   The capabilities are installed during the Onboarding Services phase and are unique and essential to the Compliance and Security Operations service.

Compliance and Security Operations Service Level Agreements (SLAs) are described within Sections 1.11 of this document.

The Compliance and Security Operations subscription scope is limited to the Anitian Compliance Automation Platform and the In-Scope Application Environment.

The table below describes the Compliance and Security Operations Services ("SecOps") subscription.

Table Key:

Service: The Compliance and Security Operations service to be provided by Anitian.

Description: Provides for supplemental details about the Compliance and Security Operations service.

In-Scope:

- **Included**: The Service is included in the FR Comprehensive price.
- **Not included**: The Service is not included in the FR Comprehensive price.

Service	Description	In-Scope
Compliance Automation Environment Administration:	Anitian provides the following administrative functions for the Compliance Automation Environment: • Alert management • Patching • Configuration tuning and updates • Tuning security controls • Change management	Included
Security Monitoring:	Anitian conducts ongoing review of security and compliance data and controls, including • Validation of the operational state of controls, alerts, and logging • Investigation of events for signs of compromise, abuse, infiltration, exfiltration, or environment degradation • Review of any blocked or detected threats and determine appropriate response	Included

Service	Description	In-Scope
Incident Response:	Anitian will provide initial response to any detected or suspected threats. Anitian classifies incident handling as: • Sev 1: Suspected operational issue or security incident, including Anitian-SecOps investigation and analysis. • Sev 2: Non-breaking operational issue or plausible security incident, including Anitian SecOps remediation and incident response. • Sev 3: Breaking operational issue or active security incident, including Anitian SecOps remediation and incident response.	Included
Incident Handling:	Up to ten (10) hours per month	Included
Security Alerts:	Anitian will implement a library of security alerts, and actively add, tune, and modify alerts based on emerging threats or environment changes.	Included
Threat Intelligence:	Anitian implements data from threat intelligence feeds into the SIEM such as public and private data feeds, deceptions, and aggregates the entirety of output from Anitian's security components to determine where the most severe threats exist.	Included
Automated Responses:	Where appropriate and relevant, Anitian will setup automated responses to respond to threats or operational alerts.	Included
Endpoint Detection and Response:	Anitian will tune endpoint security agents for optimal, automated detection and response.	Included
Vulnerability Management:	Anitian will manage vulnerability scanning for the ISE as follows: • Configure, manage, and monitor vulnerability scanning jobs for both the Compliance Automation Environment and AE for vulnerabilities. • Report all discovered vulnerabilities to Subscriber. • Analyze and remediating vulnerabilities identified in the Compliance Automation Environment. • Report vulnerabilities identified in the AE-to the Subscriber to remediate.	Included
Certified Staff:	All personnel fulfilling SecOps are USA citizens with background checks. Subscriber may, at their discretion and expense, conduct additional background checks.	Included
Artifact Repository:	Anitian will setup secure, encrypted repositories to manage any forensics, compliance, or security analysis data that requires such storage.	Included
Audit Support:	Up to twenty (20) hours per year of audit support for the initial or any follow-on audits.	Included
	Note: The below services are not Included in the SecOps price.	
Application performance monitoring	Monitoring of Subscriber's application(s) for performance, availability, or general operation.	Not Included

Service	Description	In-Scope
Application development	Development, optimization, or troubleshooting of Subscriber's application software	Not Included
General Technical Support:	Technical support for Subscriber's application, Cloud-Service Provider (i.e. AWS), or third-party products not included with Compliance Automation Platform.	Not Included
Database optimization	Analysis, tuning, or configuration of databases used for Subscriber's application(s).	Not Included
Data loss prevention	Scanning and monitoring of data communications outside of the environment. Anitian offers this as an add-on service.	Not Included
Risk Assessments	Assessment of organizational risk and the completion of risk management documentation and/or reports.	Not Included
Code scanning	Static or dynamic scanning of application source code.	Not Included

1.6.   SecOps Responsibility Description

A key part of the SecOps service is the principle of *separation of tasks, unification of responsibility*.

Unification of responsibility: Due to FedRAMP requirements, the Subscriber must remain ultimately responsible for the operation and security of both the Compliance Automation Environment and Application Environment.

Separation of tasks: As part of the SecOps services, the Subscriber will assign select tasks to Anitian as is necessary to run the environment.

1.6.1. SecOps Responsibility Table

The management and operation of the ISE is a collaborative effort between Anitian and Subscriber. The table below defines the separation of responsibilities for the management of both the Compliance Automation Environment (CAE) and the Application Environment (AE).

Key:

     ✓   Primary Responsibility
     ⇔   Collaborate and Assist with Primary
     -        No responsibility

Service		Responsibility			
		Anitian		Subscriber	
		CAE	AE	CAE	AE
Environment Administration	Alert management	✓	⇔	-	✓
	Patching	✓	⇔	-	✓
	Configuration tuning	✓	⇔	-	✓
	Security tuning	✓	⇔	-	✓
	Operational monitoring	✓	⇔	⇔	✓
	Change management	✓	⇔	⇔	✓
Incident Response	Incident investigation	✓	✓	⇔	⇔
	Incident analysis	✓	✓	⇔	⇔
	Severity 1	✓	✓	-	-

Service		Responsibility			
		Anitian		Subscriber	
		CAE	AE	CAE	AE
	Severity 2	✔	✔	⇔	⇔
	Severity 3	✔	✔	✔	✔
Security Operations	Alert tuning	✔	✔	-	⇔
	Threat intelligence	✔	✔	-	-
	Automated response	✔	✔	-	-
	Endpoint detection and response (EDR)	✔	✔	-	⇔
	Intrusion detection and prevention (IDS/IPS)	✔	✔	-	⇔
	Vulnerability management	✔	✔	-	⇔
	File Integrity Monitoring	✔	✔	⇔	⇔
	Malware Detection	✔	✔	⇔	⇔

1.7. SecOps Deliverables

Task	Description	Schedule
Security and Compliance Dashboard	Anitian will provide dashboards for on-demand reports including • Summary & Detailed view of all weaknesses discovered during the last 90 days • New vulnerabilities this month (since last POA&M report) in known POA&M format, sortable by "days to compliance breach" for easy patch prioritization • Vulnerability Trends categorized by weakness type • Exports of filtered views & pre-defined reports	Available 24/7
Vulnerability Report	Anitian will provide a monthly report of vulnerabilities identified and validated in the in-scope environment. This report will provide some content for the monthly Plan of Action and Milestones (POA&M) report. Typical content in this report: • Inventory of the environment • List of identified vulnerabilities and associated descriptions and severity rankings.	Monthly
Anitian Touchpoint	Anitian will provide half-hour briefings to review and discuss open tickets and answer questions. An agenda must be set prior to the meeting to ensure the right attendance. This could include a review of the product roadmap or current security threats. This briefing will be delivered as a telephone or video conference call.	On Demand (max 1 per month)

1.8. SecOps Out-of-Scope Services

Should Subscriber request out-of-scope services from the Anitian SecOps team, the following rates will apply:

Service / Item	Remote Rate / Day
General compliance or security advisory services	$2,400
Technical writing for security and/or compliance documents	$2,400
Software or cloud engineering services	$2,400
Digital forensics and investigative work	$2,800
Additional dashboards, reports, or content for SIEM	$2,400

ANITIAN

1.9. Security Operations Service Level Agreements

Type	Description	Response
Incident Response	A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.	• Reports suspected or confirmed incidents immediately to Subscriber • 1 hour; acknowledges Subscriber reported incident • 2 hours; engaged on incident • 4 hours; investigation begins • 8 hours; first situational update • Daily; situational update until remediation/resolution

Outage	Anitian cannot perform our contractual responsibilities for Subscriber, or an Anitian-managed tool or service is preventing Subscriber from performing their contractual duties for their clients.	• 1 hour; acknowledge outage and investigation begins
		  ▪ Update corresponding ServiceNow ticket 2 times per day until resolution
		  ▪ Daily status calls with Subscriber if no resolution in 24 hours

Change Management	Standard Change Definition: A standard change is a pre-authorized change that is low risk, relatively common and follows a specified procedure or work instruction. Emergency Change Definition: A change that must be implemented as soon as possible. This change is of such a high priority that it bypasses group and peer review and approval and goes straight to the Authorization state for approval by the CAB approval group.	• Standard Change: 6 hours • Emergency Change: 1 hour

Scheduled FedRAMP patching and vulnerability remediation	FedRAMP Vulnerability Management Program: Vulnerability identification within Operating Systems (OS), Web Applications, Databases (DBs), and Containers that follow the subsequent patching program required by FedRAMP Compliance.	• High Vulnerability:
		  ▪ 24 hours/dynamic notification to Subscriber
		  ▪ 30 days to resolve/remediate
		• Moderate Vulnerability:
		  ▪ 7 days/dynamic notification to Subscriber
		  ▪ 90 days to resolve/remediate
		• Low Vulnerability:
		  ▪ 30 days/dynamic notification to Subscriber
		  ▪ 180 days to resolve/remediate

2. DOCUMENTATION PACKAGE

Anitian will create the FedRAMP Package documentation (FedRAMP R5 of the NIST SP 800-53 Rev5) through interviews, questionnaires, and working sessions, as needed. The FedRAMP Package includes the System Security Plan (SSP) and attachments.

As part of this process, Anitian will provide advisory services in relation to the implementation of control requirements and FedRAMP Program navigation.

Process:

- Anitian will review existing documentation related to the Cloud Service Offering (CSO).
- Anitian will conduct interviews or submit questionnaires.
- Anitian will deliver a draft SSP package (in whole or in parts, based on time and working process) for Subscriber review.
- After review and update(s), Anitian will deliver a final FedRAMP Package.

Deliverables:

- Create FedRAMP required documents that constitute a FedRAMP Package:
  - FedRAMP Security Controls
  - Federal Information Processing Standards (FIPS) 199 Security Categorization
  - Information Security Policies & Procedures
  - Digital Identity Workbook
  - Rules of Behavior (RoB)
  - Information System Contingency Plan (ISCP)
  - Configuration Management Plan (CMP)
  - Incident Response Plan (IRP)
  - Control Implementation Summary (CIS) / Customer Responsibility Matrix (CRM)
  - Privacy Threshold Analysis (PTA)
  - Laws & Regulations
  - Continuous Monitoring Program Plan
  - Cryptographic Modules Table

Subscriber Responsibilities:

- The Subscriber will be responsible for determining the final implementation of services, process, and/or technology updates, including final dates for the implementation schedule.
- The Subscriber is responsible for coordinating with their assigned Authorizing Official for approval of timelines or additional requirements.
- The Subscriber is responsible for developing the following documentation as part of the overall FedRAMP package:
  - User Guide
  - Cloud Service Offering Inventory (in FedRAMP required template)
  - System Development Lifecycle (SDLC)
  - Supply Chain Risk Management Plan (SCRMP)
  - Privacy Impact Assessment (PIA) (if applicable)
  - Concept of Operations / System Design
  - System Description, Authorization Boundary Diagram, Data Flow Diagram(s), Network Architecture
  - Any additional documents requested by FedRAMP, JAB, or Agency not included in the list of scoped documents above.

  In scope services include:

  - Weekly Project and Compliance Syncs
  - Support during FedRAMP Audit

ANITIAN

APPENDIX A: FEDRAMP INSIGHTS SERVICE LEVEL AGREEMENTS

A.1. Service Level Agreement

During the Term, Anitian shall provide Subscriber with software support and maintenance services ("Support Services") described in this Addendum to the Agreement ("Support Services Schedule"). Capitalized terms not defined in this Addendum will have the meanings described in the body of the Agreement.

A.1.1. Overview

A.1.1.1.   Software Support and Maintenance.

Anitian will provide defect identification, analysis, restoration and resolution services for the current release of the Software will operate and conform to the Documentation.

A.1.1.2.   Improvements.

During the Term, Anitian may, in its sole discretion, develop updates, upgrades, enhancements and improvements to the Software. Anitian will apply such updates, upgrades, enhancements, and improvements that Anitian generally offers to other Anitian subscribers.

A.1.1.3.   Error Corrections

Anitian will use commercially reasonable efforts to correct failures of the Software to perform in materially accordance with its Documentation ("Errors") reported by Subscriber in writing to Anitian. Anitian will diligently research and use commercially reasonable efforts to identify and mitigate potential Errors that are not reproducible. Anitian may not issue Error corrections for all Errors. Anitian will work with Subscriber on a best effort basis to identify and implement reasonable technical work arounds when possible.

A.1.1.4.   Out of Scope Services.

Support provided at the request of the Subscriber, 'outside the scope of this Agreement, if any, shall be provided pursuant to Anitian's then-current applicable policies and procedures, including, at a minimum, if applicable, execution of Anitian's then-current license agreements and/or consulting/professional services agreement and payment of Anitian's then-current fees and costs associated with such services. Anitian will obtain Subscriber's prior written consent prior to performing any services that falls outside the scope of this Agreement. Subscriber acknowledges that Anitian is not providing process expertise / support, process change management, cultural change management, corporate or market level communications, market level training or project management with this Agreement. Further, these Support Services do not include any installation, implementation, configuration, business rule changes, or customization. Furthermore, if an integration component is changed or upgraded, the work needed to update the Software to restore normal operating condition will be considered a Software enhancement.

A.1.1.5.   Multivendor Coordination

Anitian's obligation to provide the Support Services described in this Exhibit in accordance with the schedule described in this Exhibit is subject, to the extent necessary, to timely cooperation from Subscriber and Subscriber vendors whose products interact with Software to reproduce and diagnose the problem.

ANITIAN

A.1.1.5.1.   Defect and Service Levels

Definitions

The following terms apply for purposes of this Support Services Schedule:

- "<u>Defect</u>" means an Error or flaw in the Software that causes an incorrect and unexpected result based on the design.
- "<u>Response Time</u>" means the time from which the Subscriber reports the Defect until Anitian acknowledges the reporting of the Defect.
- "<u>Restoration</u>" means the return of the Software to a reasonable operating condition determined by both Anitian and Subscriber without providing a Resolution.
- "<u>Resolution</u>" means the return of the Software to a reasonable operating condition with a permanent solution or reasonable workaround.
- "<u>Severity 1 Level Defect</u>" means a Defect during operation of the Software that causes Subscriber to be unable to either use the Software or perform time critical business functions with the Software. There are no available workarounds and Subscriber is operating under an absolute work stoppage situation with respect to the Software.
- "<u>Severity 2 Level Defect</u>" means a Defect during operation that causes Software to stop working properly and there are no acceptable, alternative solutions. While other areas of the Software are not impacted, the reported issue has created a significant, negative, yet non-critical impact on Subscriber's productivity or service level to its customers.
- "<u>Severity 3 Level Defect</u>" means a Defect during operation that does not materially impact a significant number of Subscriber's customers or causes minor limitations to functionality of the Software.

A.1.2. Service Level Targets

With respect to Anitian's Continuous FedRAMP Integrations, Anitian shall achieve the following targets with respect to Response Time, and shall use commercially reasonable efforts to achieve the following target with respect to Restoration Time and Resolution Time:

Type of Outage	Description	Initial Response	Outage Resolution Procedures
Severity 1 Level	A Defect during operation of the Software that causes Subscriber to be unable to use the Software.	No longer than 1 business day.	Commence work within one (1) business days after receipt of the Outage notice.
Severity 2 Level	A Defect during operation that causes Software to stop working properly, provide incorrect information, or other form of unacceptable performance. While other areas of the Software are not impacted, the reported issue has created a significant, negative, yet non-critical impact on Subscriber's	No longer than 1 business day.	Commence work within five (5) business days after receipt of the Defect notice and sufficient supporting information.

A.1.3. Access to Subscriber Systems

Anitian will identify in writing those individuals who need access to Subscriber's systems in order to provide support under this Software Support Schedule ("Anitian Support Personnel"). Subscriber will provide those individuals with login credentials to Subscriber's system, including a unique username and password. Anitian will take reasonable security precautions to protect access to Subscriber's systems, including sending notice to Subscriber within 24 hours if any Anitian Support Personnel cease working for Anitian, in order that Subscriber may disable the login credentials. Further, Anitian will comply with Subscriber's reasonable security procedures as provided in writing to Anitian.

A.1.3.1.   Contacting Anitian for Support Services

Support Hours

Anitian shall provide email-based support for use by Authorized Users Monday through Friday, 7 am EST to 5 pm PST, US holidays excluded, for problem resolution assistance. This Support is only available to Authorized Users. Subscriber may designate up to three (3) Authorized Users. This support is exclusively for problems with Software and does not include guidance on compliance or assisting Subscriber's auditors.

Contact Method

Subscriber may contact Anitian through email to insights-support@anitian.com.

A.1.3.1.1.   Limitations

Anitian will not monitor any other reporting methods for Support Service issues and cannot guarantee that it will receive or respond to any support contact that is not made by Authorized Users or through the Approved Contact Method. The terms of this Support Services Schedule do not apply to any contact that is made outside of the Approved Contact Method or by a person who is not an Authorized User and Service Levels will not be monitored on any support request that does not use the Approved Contact Method or is not by an Authorized User.

A.1.3.1.2.   Subscriber Obligations

Subscriber will provide the following to assist Anitian during the defect identification, analysis, restoration and resolution process:

- Adequately skilled and knowledgeable resources. These resources must be available at all times when Anitian is working to remedy a Defect reported by Subscriber (e.g., 24x7 for Severity Level 1 Defects). If Anitian needs additional information or support from the Subscriber to work on a Defect and a Subscriber resource is not available, then the measured time for the Service Levels will stop until the information or support is provided by Subscriber.

A.1.3.1.3.   Escalation

If Anitian does not meet the terms outlined above in this Support Services Schedule, the Subscriber may escalate the Defect by requesting an escalation on the ticket via support email a defined under section 3.2.