|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  |  | |  |
|  | FedRAMP® Security Assessment Plan (SAP)  for {{SSP|SECURITYPLAN.CSPORGNAME}}  {{SSP|SECURITYPLAN.SYSTEMNAME}}  Version {{SSP|SECURITYPLAN.VERSION}}  {{SSP|SECURITYPLAN.DATESUBMITTED}} | |  |
|
|  |  | |  |
|  |  | Controlled Unclassified Information info@fedramp.gov  fedramp.gov |  |

TEMPLATE REVISION HISTORY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Pages | Description | Author |
| 06/06/2014 | 2.0 | All | Major revision for Special Publication (SP) 800-53 Revision 4. Includes new template and formatting changes. | FedRAMP PMO |
|  |  | All | Reformatted to FedRAMP Document Standard, added repeated text schema, and content fields to tables that were not Control Tables.  Revised cover page, changed document designation to Confidential Unclassified Information (CUI),  Removed front matter section How This Document is Organized.added repeated text schema, and content fields to tables that were not Control Tables.  Revised cover page, changed document designation to Confidential Unclassified Information (CUI),  Removed front matter section How This Document is Organized. | FedRAMP PMO |
| 01/20/2016 | 3.0 |  | Converted to standard document template  Removed Acronyms and referenced FedRAMP Glossary and Acronyms resource document  Clarity edits, and instructions for the new Integrated Inventory Template Section 2.2 | FedRAMP PMO |
|  |  |  | Renamed document from "Security Assessment Plan (SAP) Template to "FedRAMP Security Assessment Plan (SAP) Template” | FedRAMP PMO |
| 10/21/2016 | 3.1 |  | Updated logo | FedRAMP PMO |
| 06/30/2023 | 4.0 | All | Initial publication after combining the Initial and Annual SAP templates. New template can also be used for Significant Change Requests. | FedRAMP PMO |

**How to contact us**

For questions about FedRAMP, or for questions about this document including how to use it, contact [info@FedRAMP.gov.](mailto:info@FedRAMP.gov)

For more information about FedRAMP, see [www.FedRAMP.gov](http://www.fedramp.gov).

Delete this Template Revision History page and all other instructional text from your final version of this document.

|  |
| --- |
| ***Instructions:*** |
| *Once you begin populating this template, it becomes a draft document. The word “template” can be removed wherever it appears. As you populate the template, you will see prompts to enter different types of data. There are no repeatable fields in this template. Please ensure that the inserted wording makes grammatical sense, as applied. You may, if desired, use Word’s “Find” and “Replace with” function to replace repeated terms, such as {{SSP|SECURITYPLAN.SYSTEMNAME}}.*  ***CSP Name, CSO Name***  *Ensure the CSP Name and CSO Name match the SSP entries.*  ***Date Selection***  *Data items that must contain a date should be in this format, mm/dd/yyyy.*  ***Item Choice***  *Data items may have a limited number of value choices, noted in parentheses as choices. Insert the appropriate choice.*  ***Instructional Text***  *Instructions are provided to help you understand how to complete this SAP template. Before delivering the final version of the SAP, be sure to delete all instructional text.*  Delete this instructional text from your final version of this document. |

Prepared by

|  |  |
| --- | --- |
| Identification of Organization that Prepared this Document | |
| **Organization Name** | {{SSP|SECURITYPLAN.PREPORGNAME}} |
| **Street Address** | {{SSP|SECURITYPLAN.PREPADDRESS}} |
| **Suite/Room/Building** | {{SSP|SECURITYPLAN.PREPOFFICE}} |
| **City, State Zip** | {{SSP|SECURITYPLAN.PREPCITYSTATE}} |

Prepared for

|  |  |
| --- | --- |
| Identification of Cloud Service Provider | |
| **Organization Name** | {{SSP|SECURITYPLAN.CSPORGNAME}} |
| **Street Address** | {{SSP|SECURITYPLAN.CSPADDRESS}} |
| **Suite/Room/Building** | {{SSP|SECURITYPLAN.CSPOFFICE}} |
| **City, State Zip** | {{SSP|SECURITYPLAN.CSPCITYSTATE}} |

Document Revision History

| **Date** | **Description** | **Version** | **Author** |
| --- | --- | --- | --- |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |

TABLE OF CONTENTS

[1 Introduction 7](#_Toc132927559)

[1.1 About This Document 7](#_Toc132927560)

[1.2 Who Should Use This Document? 7](#_Toc132927561)

[2 Background 8](#_Toc132927562)

[2.1 Purpose 8](#_Toc132927563)

[2.2 Applicable Laws, Regulations, Standards, and Guidance 8](#_Toc132927564)

[3 Scope 9](#_Toc132927565)

[3.1 Location of components 11](#_Toc132927566)

[3.2 IP Addresses Slated for Testing 11](#_Toc132927567)

[3.3 Role Testing Exclusions 12](#_Toc132927568)

[3.4 Role Testing for Significant Change Requests 13](#_Toc132927569)

[4 Assumptions 13](#_Toc132927570)

[5 Methodology 14](#_Toc132927571)

[5.1 Control Testing 15](#_Toc132927572)

[5.2 Data Gathering 15](#_Toc132927573)

[5.3 Sampling 16](#_Toc132927574)

[5.4 Penetration Test 18](#_Toc132927575)

[6 Test Plan 18](#_Toc132927576)

[6.1 Security Assessment Team 18](#_Toc132927577)

[6.2 CSP Testing Points of Contact (POCs) 19](#_Toc132927578)

[6.3 Testing Performed Using Automated Tools 20](#_Toc132927579)

[6.4 Testing Performed Using Manual Methods 20](#_Toc132927580)

[6.5 Schedule 22](#_Toc132927581)

[7 Rules of Engagement 23](#_Toc132927582)

[7.1 Disclosures 24](#_Toc132927583)

[7.1.1 Security Testing May Include 24](#_Toc132927584)

[7.1.2 Security Testing Will Not Include 25](#_Toc132927585)

[7.2 End of Testing 25](#_Toc132927586)

[7.3 Communication of Test Results 25](#_Toc132927587)

[7.4 Limitation of Liability 26](#_Toc132927588)

[8 Signatures 26](#_Toc132927589)

[Appendix A FedRAMP {{SSP|SECURITYPLAN.SYSTEMNAME}} Security Controls Selection Worksheet 27](#_Toc132927590)

[Appendix B Sampling Methodology 28](#_Toc132927591)

[Appendix C Penetration Testing Plan and Methodology 28](#_Toc132927592)

[Appendix D Significant Change Request Documentation 31](#_Toc132927593)

# Introduction

## About This Document

This document is developed as a template when creating a FedRAMP Security Assessment Plan (SAP). This template should be used for all initial authorization assessments, annual assessments, combined annual assessments (i.e., JAB annual assessments that may also include significant change assessments), and significant change assessments.

Independent assessors (IAs) must complete this SAP template in cooperation with a cloud service provider (CSP). This plan is based upon a specific cloud service offering’s (CSO’s) system security plan (SSP). This SAP should not move forward towards completion until a CSP has provided an IA with a final and signed SSP from which to proceed.

A CSP must keep in mind that an IA must follow all FedRAMP requirements in preparing this SAP. Failure to follow FedRAMP requirements may result in retesting, delaying the authorization process.

This document uses the term authorizing official (AO). For systems pursuing a Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO), AO refers to the JAB. For systems pursuing a FedRAMP Agency Authorization, AO refers to each leveraging agency’s AO.

## Who Should Use This Document?

This SAP template is intended to be populated by a FedRAMP recognized third party assessment organization (3PAO) or an independent assessment organization (IAO) when documenting the plan to complete a FedRAMP security assessment. AOs will review this completed SAP to understand the scope and methodology of the assessment.

CSPs pursuing a JAB P-ATO are required to use a FedRAMP recognized 3PAO to conduct the security assessment. It is incumbent upon a CSP to ensure that their 3PAO assessors hold the appropriate certifications and have the required years of experience (see Section 6.1). CSPs pursuing a FedRAMP Agency Authorization may use other IAOs, if directed to do so by their agency partner; however, the use of a FedRAMP recognized 3PAO is encouraged.

If an agency elects to use their own IA team or a third-party assessor, that is not a FedRAMP recognized 3PAO, the agency AO must attest to the independence of the assessment organization. In addition, the IAO must always use FedRAMP provided templates.

Throughout the remainder of this template, an assessor subcontracted with/employed by either a FedRAMP recognized 3PAO or an independent assessment organization (IAO) will be collectively referred to as an “IA”.

# Background

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services. Security assessments are an integral part of the FedRAMP security authorization process.

Cloud services must be assessed by an IA. The use of an IA reduces the potential for conflicts of interest that could occur in verifying the implementation status and effectiveness of the security controls. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, Managing Information Security Risk states:

*Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of the security assessment results; and (iii) ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based, authorization decision.*

## Purpose

This SAP has been developed by {{MA|LEADASSESSOR.FULLNAME}} and is for <Choose One: an initial assessment/an annual assessment/an annual assessment and significant change assessment/a significant change assessment> of the {{SSP|SECURITYPLAN.CSPORGNAME}}, {{SSP|SECURITYPLAN.SYSTEMNAME}}. The SAP provides the goals for the assessment and details how the assessment will be conducted.

## Applicable Laws, Regulations, Standards, and Guidance

The FedRAMP-applicable laws, regulations, standards and guidance is included in the {{SSP|SECURITYPLAN.SYSTEMNAME}} SSP section – System Security Plan Approvals. Additionally, in Appendix L of the SSP, the {{SSP|SECURITYPLAN.CSPORGNAME}} has included laws, regulations, standards, and guidance that apply specifically to this system.

# Scope

Table ‑ Assessment Scope

| **FedRAMP Package ID** | **CSP Name** | **CSO Name** |
| --- | --- | --- |
| {{SSP|SECURITYPLAN.FEDRAMPID}} | {{SSP|SECURITYPLAN.CSPORGNAME}} | {{SSP|SECURITYPLAN.SYSTEMNAME}} |

|  |
| --- |
| ***Instruction:*** |
| *Determine what type of assessment will be included in this SAP (e.g., initial, annual, significant change, etc.). Use the correct narrative and remove any narratives that are not applicable.*  Delete this instructional text from your final version of this document. |

**Initial Assessment:**

This plan is for an initial assessment of {{SSP|SECURITYPLAN.SYSTEMNAME}}, a **{{SSP|SECURITYPLAN.OVERALLCATEGORIZATION}}** baseline system. 100% of the FedRAMP security controls in the system baseline are assessed. The security controls that will be assessed are listed in Appendix A.

**Annual Assessment:**

This plan is for an annual assessment of {{SSP|SECURITYPLAN.SYSTEMNAME}}, a **{{SSP|SECURITYPLAN.OVERALLCATEGORIZATION}}** baseline system. After the initial security assessment, FedRAMP requires that the system is assessed annually thereafter (12 months from an agency ATO / JAB P-ATO date). While the entire set of security controls is assessed during the initial assessment, a subset is assessed during the annual assessment. The control selection is in accordance with the criteria outlined in the [FedRAMP Annual Assessment Guidance](https://www.fedramp.gov/assets/resources/documents/CSP_Annual_Assessment_Guidance.pdf) and includes:

* Core controls (required annually)
* CSP-selected controls required to address system changes that have been implemented and/or changed by a CSP since their last assessment (this excludes those controls or portions of controls previously assessed under a significant change within the same annual period)
* Validation of Plan of Action & Milestones (POA&Ms) closed since the last assessment
* Validation of POA&Ms identified as vendor dependencies (VDs) or deviation requests (DRs)
* CSP-selected controls identified as “Not Applicable” (N/A) to validate they are, in fact, not applicable
* Controls that have not been assessed, at least once in a three year period, to ensure controls are meeting periodicity requirements

The detailed control list, including the rationale for each control’s selection, is included in SAP Appendix A, FedRAMP {{SSP|SECURITYPLAN.SYSTEMNAME}} Security Controls Selection Worksheet.

**Significant Change:**

This document <Choose One: is for/also includes> the assessment plan for <Choose One: a significant change/several significant changes>. Appendix D includes the significant change request documentation submitted by {{SSP|SECURITYPLAN.CSPORGNAME}} to the <Choose One: AO/JAB>.

Appendix A includes the associated control selections. {{MA|LEADASSESSOR.FULLNAME}} will evaluate (review and/or test), as necessary, <Choose One: all items related to continuous monitoring activities/all items related to continuous monitoring activities as well as those that are applicable to the significant change assessment/continuous monitoring activities that are only applicable to the significant change assessment>, {{MA|LEADASSESSOR.FULLNAME}} will evaluate all open POA&M items (including VDs); POA&M closures (to confirm adequate closure) and validate and confirm continued relevance and applicability of DRs ((false positives (FPs), risk adjustments (RAs), and operational requirements (ORs)) <Choose One (if significant change(s) are included): including those applicable to the significant change assessment/applicable only to the significant change assessment>.

|  |
| --- |
| ***Instruction:*** |
| *If the CSP is leveraging another cloud service, use the following narrative and table. Otherwise, delete the narrative and table.*  Delete this instructional text from your final version of this document. |

{{SSP|SECURITYPLAN.SYSTEMNAME}} leverages the FedRAMP Authorized CSOs listed in Table 3-2. {{SSP|SECURITYPLAN.CSPORGNAME}}, as a customer of these CSOs, must meet customer requirements documented by the leveraged CSOs in the customer responsibility matrix (CRM). Therefore, {{MA|LEADASSESSOR.FULLNAME}} will validate to the best of their ability that {{SSP|SECURITYPLAN.SYSTEMNAME}} is in compliance with customer requirements documented in the CRMs of the leveraged CSOs.

Table ‑ Leveraged Systems CSP/CSO

| **FedRAMP Package ID** | **CSP Name** | **CSO Name** |
| --- | --- | --- |
| {{SSP|SECURITYPLAN.FEDRAMPID}} | {{SSP|SECURITYPLAN.CSPORGNAME}} | {{SSP|SECURITYPLAN.SYSTEMNAME}} |

## Location of components

The physical locations of all the different components that will be tested are described in Table 3-3.

Table ‑ Location of Components

| **Data Center Site Name** | **Address** | **Description of Components** |
| --- | --- | --- |
| {{QL-GETCONTROLS|PARENTID.PARENTMODULE|ITEMS[\*].ASSESSMENTS[\*].FACILITY.NAME}} | {{QL-GETCONTROLS|PARENTID.PARENTMODULE|ITEMS[\*].ASSESSMENTS[\*].FACILITY.ADDRESS}}  {{QL-GETCONTROLS|PARENTID.PARENTMODULE|ITEMS[\*].ASSESSMENTS[\*].FACILITY.CITY}} {{QL-GETCONTROLS|PARENTID.PARENTMODULE|ITEMS[\*].ASSESSMENTS[\*].FACILITY.STATE}} {{QL-GETCONTROLS|PARENTID.PARENTMODULE|ITEMS[\*].ASSESSMENTS[\*].FACILITY.ZIPCODE}} | {{QL-GETCONTROLS|PARENTID.PARENTMODULE|ITEMS[\*].ASSESSMENTS[\*].FACILITY.DESCRIPTION}} |

## IP Addresses Slated for Testing

|  |
| --- |
| ***Instruction:*** |
| *The entire system inventory must be tested. If this SAP is solely for a significant change or includes a significant change in the annual assessment, the additional components associated with that change must be identified in the SAP Appendix D. However, if this SAP is exclusively for an annual or initial assessment, IAs are instructed NOT to embed or attach the FedRAMP Integrated Inventory Worksheet to the SAP. Instead, IAs should simply reference SSP Appendix M in this section of the SAP. If additional components are discovered during testing, the security assessment report (SAR) must describe the deviation from the SAP. Both the SSP and FedRAMP Integrated Inventory Workbook must be updated to reflect the additional component(s) prior to authorization.*  *It is at the initial assessment that the CSP and IA agree on how the testing should proceed. This sets the baseline to be tested for all ensuing annual assessments. However, at every annual assessment, the CSP and IA must determine if the inventory has gone through any significant changes during the year. It is at that point that the components/parameters of the inventory testing either grow, decrease, or remain the same. If the number of components was determined by sampling, the CSP and IA must ensure that the* [FedRAMP Guide for Sampling](https://www.fedramp.gov/assets/resources/documents/CSP_Vulnerability_Scan_Requirements_Using_Sampling.pdf) is strictly followed.  Delete this instructional text from your final version of this document. |

SSP Appendix M, FedRAMP Integrated Inventory Workbook, captures the inventory items for the entire system and includes all the following required to be tested for the authorization of this system:

* Operating systems/infrastructure,
* Container images (as applicable),
* Databases, and
* Web application components

The SSP Appendix M, FedRAMP Integrated Inventory Workbook. is current for this assessment.

Any components that are being added to the inventory, removed from the inventory, or are being modified or directly impacted by a significant change, are identified in Appendix D of this SAP.

The methodology section of this document describes the approach to the assessment of the inventory.

## Role Testing Exclusions

|  |
| --- |
| ***Instruction:*** |
| *If any roles were excluded from testing, use the following table to document the role type and reason for exclusion. If no roles were excluded, leave the table blank.*  Delete this instructional text from your final version of this document. |

Table ‑ Exclusions for Role Testing

| **Role Type** | **Reason for Exclusion** |
| --- | --- |
|  |  |
|  |  |

## Role Testing for Significant Change Requests

|  |
| --- |
| ***Instruction:*** |
| *If this SAP is for a significant change request (SCR), include the following; otherwise, remove it.*  Delete this instructional text from your final version of this document. |

Additional roles that are being introduced as part of significant changes will be tested and are noted in Appendix D. Role testing will be performed to test the authorization restrictions for each role. {{MA|LEADASSESSOR.FULLNAME}} will access the system while logged in as different user types and attempt to perform restricted functions for that user.

# Assumptions

|  |
| --- |
| ***Instruction:*** |
| *The assumptions listed are default assumptions. An IA must edit these assumptions as necessary for each unique engagement. While some systems conform to a methodology, the methodology offered here is only an example and can be used for the basis of the CSO assessment; however, the JAB and FedRAMP PMO expect each CSO assessment to be unique and may have a much-expanded testing methodology applied.*  Delete this instructional text from your final version of this document. |

The following assumptions were agreed upon between {{SSP|SECURITYPLAN.CSPORGNAME}} and {{MA|LEADASSESSOR.FULLNAME}} when developing this SAP:

* This SAP is based on {{SSP|SECURITYPLAN.SYSTEMNAME}} SSP {{SSP|SECURITYPLAN.VERSION}}, dated {{SSP|SECURITYPLAN.DATESUBMITTED}}, in its entirety. This includes all SSP appendices. The {{SSP|SECURITYPLAN.CSPORGNAME}} is responsible for providing {{MA|LEADASSESSOR.FULLNAME}} the most current SSP.
* Scans will be provided in both machine readable and human readable format.
* {{SSP|SECURITYPLAN.SYSTEMNAME}} resources, including documentation and individuals with knowledge of the {{SSP|SECURITYPLAN.SYSTEMNAME}} systems and infrastructure and their contact information, will be available to {{MA|LEADASSESSOR.FULLNAME}} staff during the time necessary to complete assessments.
* The {{SSP|SECURITYPLAN.CSPORGNAME}} will provide login account information / credentials necessary for {{MA|LEADASSESSOR.FULLNAME}} to use its testing devices to perform authenticated scans of all devices and applications.
* The {{SSP|SECURITYPLAN.CSPORGNAME}} will permit {{MA|LEADASSESSOR.FULLNAME}} to connect its testing laptops to the {{SSP|SECURITYPLAN.CSPORGNAME}} networks defined within the scope of this assessment.
* The {{SSP|SECURITYPLAN.CSPORGNAME}} will permit communication from {{MA|LEADASSESSOR.FULLNAME}} testing appliances to an internet hosted vulnerability management service to permit the analysis of vulnerability data, as applicable.
* Security controls that have been identified as “Not Applicable” (NA) in the SSP will be validated by {{MA|LEADASSESSOR.FULLNAME}} as “Not Applicable”, and further testing will not be performed on these security controls during the assessment. This process is completed for all assessments, including annual assessments. For this assessment, the following controls identified as NA controls will be validated by {{MA|LEADASSESSOR.FULLNAME}}: **<List all NA controls that will be validated by the IA for this assessment>.**
* Significant upgrades or changes to the infrastructure and components of the system undergoing testing will not be performed during the security assessment period.
* For onsite control assessment, {{SSP|SECURITYPLAN.CSPORGNAME}} personnel will be available should the {{MA|LEADASSESSOR.FULLNAME}} staff determine that either after hours work, or weekend work, is necessary to support the security assessment.
* Add assumptions here; these must be agreed to by the CSP and IA…
* Add …
* Add …

# Methodology

|  |
| --- |
| ***Instruction:*** |
| *FedRAMP provides a documented methodology, which describes the process for testing the security controls. IAs may edit this section to add information, but may not remove any of the pre-existing text. The IA should review the FedRAMP SAR template to understand the requirements for documenting assessment results.*  Delete this instructional text from your final version of this document. |

## Control Testing

{{MA|LEADASSESSOR.FULLNAME}} will perform an assessment of the {{SSP|SECURITYPLAN.SYSTEMNAME}} security controls using the methodology described in NIST SP 800-53A, incorporating the methodology required by FedRAMP as noted below, and any other methods of testing that may be required to thoroughly test this system authorization boundary. {{MA|LEADASSESSOR.FULLNAME}} will use the FedRAMP Security Requirements Traceability Matrix (SRTM) Workbook to evaluate the security controls. Contained in Excel worksheets, these test procedures contain the test objectives and associated test cases to determine if a control is effectively implemented and operating as intended. The results of the testing shall be recorded in the SRTM workbook for the appropriate High, Moderate, or Low baseline (provided on the FedRAMP Documents and Resources page under Templates) along with information that notes whether the control (or control enhancement) is satisfied or not.

{{MA|LEADASSESSOR.FULLNAME}} will ensure that all {{SSP|SECURITYPLAN.SYSTEMNAME}} security controls that have an alternative implementation are included in the final SRTM workbook with test procedures that capture the intent of the control. {{SSP|SECURITYPLAN.CSPORGNAME}} is advised that testing alternative control implementations involves additional IA rigor since it is much more difficult to prove the intent of the control is being met. The alternative control implementations that are tested for this assessment are: ***<List all alternative control implementations that will be tested by the IA for this assessment>.***

Deviations from the SAP-defined methodology are described below.

## Data Gathering

{{MA|LEADASSESSOR.FULLNAME}} data gathering activities will consist of the following:

* Request {{SSP|SECURITYPLAN.CSPORGNAME}} to provide FedRAMP required documentation.
* Ensure {{SSP|SECURITYPLAN.CSPORGNAME}} provides the list of controls identified as “Alternative Implementation” and “Not Applicable” in the SSP.
* Request any follow-up documentation, files, or information needed that is not provided in FedRAMP required documentation.
* Travel to the {{SSP|SECURITYPLAN.CSPORGNAME}} sites as necessary to inspect systems and meet with CSP staff.
* Obtain information using security testing tools.
* Ensure that the testing proceeds as outlined in this SAP. If the testing must be augmented or reduced in scope, these are considered “Deviations” and must be recorded in the SAR.

Security controls will be verified using one or more of the following assessment methods:

* Examine: {{MA|LEADASSESSOR.FULLNAME}} will review, analyze, inspect, or observe one or more assessment artifacts as specified in the SRTM. Note that the SSP is considered a "roadmap" for identification and collection of other artifacts. Therefore, other CSP artifacts should be provided (e.g., screenshots, policies, procedures, records etc.).
* Interview: {{MA|LEADASSESSOR.FULLNAME}} will conduct discussions with individuals within the organization to facilitate assessor understanding, achieve clarification, or obtain evidence.
* Technical Tests: {{MA|LEADASSESSOR.FULLNAME}} will perform technical tests, including penetration testing on system components, using automated and manual methods.

## Sampling

The sampling methodology for evidence/artifact gathering, related to controls assessment, is described in Appendix B.

|  |
| --- |
| ***Instruction:*** |
| *The IA must assess a sampling of components for vulnerability scanning in accordance with* [FedRAMP Guide for Determining Eligibility and Requirements for the Use of Sampling for Vulnerability Scans.](https://www.fedramp.gov/assets/resources/documents/CSP_Vulnerability_Scan_Requirements_Using_Sampling.pdf) *For an initial assessment, 100% of the inventory must be scanned or the sampling methodology must ascertain that the sampling does represent 100% of the system inventory. A sampling of the assets within each of the standard system images is considered sufficient. The IA must attest that the sample selected is sufficient to represent the state of the unique inventory.*  *When the IA is considering sampling methods for testing controls, the IA must attest that the sample selected (e.g., account requests/terminations/transfers process, change control process, etc) is sufficient to represent the unique state of the system and status of the control being tested.*  Delete this instructional text from your final version of this document. |

{{MA|LEADASSESSOR.FULLNAME}} <Choose One: will/will not> use sampling when performing vulnerability scanning.

{{MA|LEADASSESSOR.FULLNAME}} <Choose One: will/will not> use sampling when testing the following controls:

* List
* List
* List

|  |
| --- |
| ***Instruction:*** |
| *If vulnerability scanning sampling is used, include the following text; otherwise, remove it.*  Delete this instructional text from your final version of this document. |

The vulnerability scanning sampling methodology is described in Appendix B and is in accordance with the [FedRAMP Guide for Determining Eligibility and Requirements for the Use of Sampling for Vulnerability Scans](https://www.fedramp.gov/assets/resources/documents/CSP_Vulnerability_Scan_Requirements_Using_Sampling.pdf). While scanning sampling may be conducted for scanning, all scanning will be performed authenticated.

|  |
| --- |
| ***Instruction:*** |
| *If vulnerability scanning sampling is not used, include the following text; otherwise, remove it.*  Delete this instructional text from your final version of this document. |

{{MA|LEADASSESSOR.FULLNAME}} validates that all components in the authorization boundary as captured in the {{SSP|SECURITYPLAN.SYSTEMNAME}} SSP, Appendix M, FedRAMP Integrated Inventory Workbook will be 100% tested, or representative of 100% tested, and will be 100% authenticated vulnerability scans.

{{MA|LEADASSESSOR.FULLNAME}} validates that all security controls required to be tested have appropriate sample sizes for items such as account requests, account terminations, account transfers, change control processes as captured in the {{SSP|SECURITYPLAN.SYSTEMNAME}} SSP, {{SSP|SECURITYPLAN.VERSION}}, {{SSP|SECURITYPLAN.DATESUBMITTED}}. The controls sampling methodology is described in Appendix B.

## Penetration Test

The Penetration Test Plan and Methodology is attached in Appendix C.

# Test Plan

The {{MA|LEADASSESSOR.FULLNAME}} security assessment team, {{SSP|SECURITYPLAN.CSPORGNAME}} points of contact, testing schedule, and testing tools that will be used are described in the sections that follow.

## Security Assessment Team

|  |
| --- |
| ***Instruction:*** |
| *The IA is required to provide a minimum of three personnel for each assessment: a senior assessor, junior assessor, and penetration tester. There may be two senior assessors and a penetration tester, where one senior assessor is acting in a junior assessor’s role as long as both assessors meet the senior assessor training, experience, and certification criteria. There is no exception that can be devised to have only two junior assessors (no senior assessor) and a penetration tester.*  *Alternatively, a significant change request (SCR) may not require a penetration tester. For SCRs, there may be a senior and a junior assessor or two senior assessors to complete the testing.*  *Additionally, CA-8 is required in Li-SaaS as "Document and Assess". However, CA-8 (1) is NOT part of the Low (and therefore, Li-SaaS) baseline, which means there is no requirement for an independent testing team. Therefore, IAs should only assess the quality of the penetration test.*  *SCRs notwithstanding, there is no deviation or exemption for this requirement for High, Moderate, and Low security assessments.*  Delete this instructional text from your final version of this document. |

The {{MA|LEADASSESSOR.FULLNAME}} security assessment team consists of the individuals listed in Table 6-1. {{SSP|SECURITYPLAN.CSPORGNAME}} is urged to check the capabilities of the named individuals to ensure that each is qualified to hold the position, per A2LA’s personnel requirements specified in the [A2LA R311 - Specific Requirements: Federal Risk and Authorization Management Program (FedRAMP)](https://a2la.qualtraxcloud.com/ShowDocument.aspx?ID=5621).

Note that this document is signed in Section 8, by the {{MA|LEADASSESSOR.FULLNAME}} and {{SSP|SECURITYPLAN.CSPORGNAME}}. {{SSP|SECURITYPLAN.CSPORGNAME}} has a right and a responsibility to ensure that competent assessors are providing the assessment services. The document should not be signed until {{SSP|SECURITYPLAN.CSPORGNAME}} has validated the IA team.

Table ‑ {{MA|LEADASSESSOR.FULLNAME}} Security Assessment Team

| **Name** | **Assessment Role** | **Validated by IA** | **Validated by CSP** |
| --- | --- | --- | --- |
| «BeginGroup:MembersAssessors»«BeginGroup:RolesAssessors»«MembersAssessors:FullName» | «RoleDisplayName» |  |  |
|  |  |  |  |

## CSP Testing Points of Contact (POCs)

|  |
| --- |
| ***Instruction:*** |
| *The IA must obtain at least three POCs from the CSP to use for testing communications. One of the contacts must be an “on call” team member who has points of contact (POC) with the operations center (e.g., NOC and SOC). The CSP POCs listed must be those who actively participate in the assessment effort and participate in meetings with the JAB, agency partner, and FedRAMP PMO.*  Delete this instructional text from your final version of this document. |

The {{SSP|SECURITYPLAN.CSPORGNAME}} POCs are found in Table 6-2. {{MA|LEADASSESSOR.FULLNAME}} has internal processes to contact the CSP should the need arise.

Table ‑ {{SSP|SECURITYPLAN.CSPORGNAME}} Points of Contact

| **Name** | **Role** |
| --- | --- |
| {{SSP|SECURITYPLAN.SYSTEMOWNER.FULLNAME}} | {{SSP|SECURITYPLAN.SYSTEMOWNER.JOBTITLE}} |
| {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.FULLNAME}} | {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.JOBTITLE}} |

## Testing Performed Using Automated Tools

|  |
| --- |
| ***Instruction:*** |
| *The CSP should ensure that the IA-named tools perform the “purpose” to which the IA refers. For example, Tool X does static code analysis, but not dynamic code analysis; Tool Y does web application scanning, but not database scanning; Tool Z does database scanning, but does not do static code analysis. It is the CSP’s responsibility to ensure that the named tools can perform the named “Purpose of Tool”.*  Delete this instructional text from your final version of this document. |

{{MA|LEADASSESSOR.FULLNAME}} plans to use the following tools noted in Table 6-3 to perform testing of the {{SSP|SECURITYPLAN.SYSTEMNAME}}.

Table ‑ Assessment Tools

| **Tool Name** | **Vendor/Organization Name & Version** | **Purpose of Tool** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

## Testing Performed Using Manual Methods

|  |
| --- |
| ***Instruction:*** |
| *Describe what technical tests will be performed through manual methods without the use of automated tools. The results of all manual tests must be recorded in the SAR. Examples are listed in the first four rows. Delete the examples and record the real tests. Add additional rows as necessary. Identifiers must be in the format MT-1, MT-2, etc., which indicates “Manual Test 1”, “Manual Test 2”, etc.*  *By the examples offered (i.e., CAPTCHA and OSCP), an IA should test to this depth for a CSO. In the event that this manual testing list becomes too extensive, the IA should determine which testing will cover the security of the system most holistically. This list to address everything in a given environment across all controls in scope, does take extra effort and will be different for each CSO. The IA may find that certain service models and deployment models benefit from a specific battery of tests and should use those.*  *Alternatively, the table, below, may be removed and added as an additional appendix to the SAP. Be sure to replace the template text with: “The {{MA|LEADASSESSOR.FULLNAME}} will perform manual testing to ensure that the CSO is secure. The details of this are defined in Appendix <Insert Appendix Letter>”, and include a hyperlink to that appendix.*  Delete this instructional text from your final version of this document. |

Table ‑ Testing Performed Through Manual Methods

| Test ID | Test Name | Description |
| --- | --- | --- |
| MT-1 | Alternative Implementation of Security Control (Example) | The IA has indicated what the testing will be for the SSP controls listed as “Alternative Implementations”. The CSP should be aware that testing alternative implementations does take extra rigor to ensure the intent of the control is met.  *[Instruction: The manual methods employed for each of the controls should be listed here with each testing method recorded individually. Each control will have its own line item for testing. Remove this instructional text once this table is fully populated.]* |
| MT-2 | Validation of N/A Controls | The IA will validate that controls listed as “Not Applicable” are not applicable. The CSP should be aware that validation of “Not Applicable” controls sometimes provides insight that the control is actually applicable and should be implemented. Once the control is implemented, the IA must retest to ensure the intent of the control is met.  *[Instruction: The validation employed for each of the controls should be listed here with each validation method recorded individually. Each control will have its own line item for testing. Remove this instructional text once this table is fully populated.]* |
| MT-3 | CAPTCHA | <Insert Description Text>  *[Instruction: Record how to test the CAPTCHA function on the Web. Remove this instructional text once this table is fully populated.]* |
| MT-4 | OCSP | <Insert Description Text>  *[Instruction: Record how to test to determine if OCSP is validating certificates. Remove this instructional text once this table is fully populated.]* |
| <Insert Test ID> | <Insert Test Name> | <Insert Description Text>  *[Instruction: Use as many rows as necessary. Remove this instructional text once this table is fully populated.]* |

## Schedule

|  |
| --- |
| ***Instruction:*** |
| *Provide the security assessment schedule. The schedule must be presented to a CSP, by an IA, before commencing the assessment.*  Delete this instructional text from your final version of this document. |

The security assessment schedule can be found in Table 6-5. Any deviations from this accepted schedule are recorded in the SAR as Deviations.

Table ‑ Assessment Schedule

| Task Name | Start Date | Finish Date |
| --- | --- | --- |
| Prepare SAP |  |  |
| Meeting to Review SAP |  |  |
| Update and Finalize SAP |  |  |
| Review CSP Documentation |  |  |
| Conduct Interviews of CSP Staff |  |  |
| Perform Testing |  |  |
| Vulnerability Analysis and Threat Assessment |  |  |
| Risk Exposure Table Development |  |  |
| Complete Draft SAR |  |  |
| Draft SAR Delivered to CSP |  |  |
| Issue Resolution Meeting |  |  |
| Complete Final Version of SAR |  |  |
| Provide Final Version of SAR to CSP |  |  |

# Rules of Engagement

|  |
| --- |
| ***Instruction:*** |
| *FedRAMP provides and recommends the Rules of Engagement (ROE), as listed in the section that follows. IAs must edit this ROE as necessary. The final version of the ROE must be signed by both an IA and CSP. See NIST SP 800-115, Appendix B, for further guidance.*  Delete this instructional text from your final version of this document. |

The ROE is a document designed to describe proper notifications and disclosures between an owner of a tested system and an IA. In particular, a ROE includes information about targets of automated scans and IP address origination information of automated scans (and other testing tools). Together with the information provided in preceding sections of this document, this document shall serve as a ROE once signed.

## Disclosures

Any testing will be performed according to the terms and conditions, cited in this SAP and the Penetration Testing ROE, once this SAP is signed by both parties. These ROEs must be upheld to minimize risk exposure that could occur during security assessment testing.

The following sections provide additional disclosures accepted by the IA and the CSP for proceeding with this Security Assessment.

### Security Testing May Include

Every assessment requires certain disclosures. Sometimes a CSO may have the same disclosures as another CSO, but not usually. IAs and CSPs are required to ensure that all requirements contracted between the CSP and IA are adequate for both parties. Examples of inclusive disclosures appear below. Add to and delete from this list, as applicable.

* Port scans and other network service interaction and queries
* Network sniffing, traffic monitoring, traffic analysis, and host discovery
* Attempted logins or other use of systems, with any account name, token, password, and privilege
* Attempted SQL injection and other forms of input parameter testing
* Use of exploit code for leveraging discovered vulnerabilities
* Password cracking via capture and scanning of authentication databases
* Spoofing or deceiving servers regarding network traffic
* Altering running system configuration except where denial of service would result
* Adding user accounts
* Add more here as bullets…

### Security Testing Will Not Include

|  |
| --- |
| ***Instruction:*** |
| *If a CSP and IA list exclusions that do not seem reasonable for most CSOs, those exclusions must be followed by a rationale and the logic explaining the exclusion. Add to and delete from the following list, as applicable.*  Delete this instructional text from your final version of this document. |

Examples of exclusive disclosures appear below. Security testing will not include any of the following activities:

* Changes to assigned user passwords
* Modification of user files or system files
* Telephone modem probes and scans (active and passive)
* Intentional viewing of {{SSP|SECURITYPLAN.CSPORGNAME}} staff email, Internet caches, and/or personnel cookie files
* Denial of Service attacks
* Exploits that will introduce new weaknesses to the system
* Intentional introduction of malicious code (e.g., viruses, Trojans, worms, etc.)
* Add exclusions here; however, be aware that FedRAMP may not agree with the exclusions listed (e.g., no testing of client side components indicated as imperative for use of the system)

## End of Testing

{{MA|LEADASSESSOR.FULLNAME}} will notify <Insert Name of Person> at {{SSP|SECURITYPLAN.CSPORGNAME}} when security testing has been completed.

## Communication of Test Results

All documentation generated by this security assessment effort, is to be handled securely, in such a way to protect the confidentiality, integrity and availability of the data, and according to {{SSP|SECURITYPLAN.CSPORGNAME}} and {{MA|LEADASSESSOR.FULLNAME}} acceptable requirements. Security testing results will be provided and disclosed to the individual POCs at {{SSP|SECURITYPLAN.CSPORGNAME}} as noted in this document. This should be accomplished within <Insert Number of Days> days after security testing has been completed.

## Limitation of Liability

|  |
| --- |
| ***Instruction:*** |
| *Insert any Limitations of Liability associated with the security testing below. Edit the provided default Limitation of Liability as needed.*  Delete this instructional text from your final version of this document. |

{{MA|LEADASSESSOR.FULLNAME}}, and its stated partners, shall not be held liable to {{SSP|SECURITYPLAN.CSPORGNAME}} for any and all liabilities, claims, or damages arising out of or relating to the security vulnerability testing portion of this Agreement, howsoever caused and regardless of the legal theory asserted, including breach of contract or warranty, tort, strict liability, statutory liability, or otherwise.

{{SSP|SECURITYPLAN.CSPORGNAME}} acknowledges that there are limitations inherent in the methodologies implemented, and the assessment of security and vulnerability relating to information technology is an uncertain process based on past experiences, currently available information, and the anticipation of reasonable threats at the time of the analysis. There is no assurance that an analysis of this nature will identify all vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate all exposure.

# Signatures

The following individuals at {{MA|LEADASSESSOR.FULLNAME}} and {{SSP|SECURITYPLAN.CSPORGNAME}} have been identified as having the authority to agree to security testing of {{SSP|SECURITYPLAN.SYSTEMNAME}}. {{SSP|SECURITYPLAN.CSPORGNAME}} has validated that the {{MA|LEADASSESSOR.FULLNAME}} assessors assigned to this project fulfill the FedRAMP assessor requirements, as noted in Section 6.1 and formally named in Table 6-1. This section must be signed and dated prior to an IA beginning an assessment.

| Acceptance and Signature | | | |
| --- | --- | --- | --- |
| I have read the above Security Assessment and Rules of Engagement and I acknowledge and agree to the tests and terms set forth in the plan. | | | |
| IA Representative: | <print> |  |  |
| IA Representative: | <signature> | Date: | <mm.dd.yyyy> |
| CSP Representative: | <print> |  |  |
| CSP Representative: | <signature> | Date: | <mm.dd.yyyy> |

1. FedRAMP {{SSP|SECURITYPLAN.SYSTEMNAME}} Security Controls Selection Worksheet

|  |
| --- |
| ***Instruction:*** |
| *Embed or reference copies of the FedRAMP Security Controls Selection Worksheet. If this is a full assessment, please note here that this is a full assessment where 100% of the security controls in the baseline are tested.*  *Specifying why a control is selected helps an AO/JAB ensure the appropriate controls are selected and gain insight on the impact of changes. If a significant change request (SCR) assessment is included, identify which controls pertain to which SCR.*  *If a control is selected for multiple reasons, specify all reasons (e.g. annual assessment core controls testing, annual assessment controls periodicity testing, SCR, etc.).*  Delete this instructional text from your final version of this document. |

1. Sampling Methodology

|  |
| --- |
| ***Instruction:*** |
| *Embed or reference copies of the sampling methodology for security controls assessment and vulnerability scanning (if applicable).*  Delete this instructional text from your final version of this document. |

1. Penetration Testing Plan and Methodology

|  |
| --- |
| ***Instruction:*** |
| *IAs may embed a file containing the plan or include the plan in this section. The plan must minimally include the attack vectors noted in the FedRAMP Penetration Test Guidance. Additionally, IAs are required to identify and test against the most applicable tactics that would be adopted by a malicious actor based on the FedRAMP Penetration Test Guidance section regarding threat models. Finally, IAs must outline the specific attack narratives of verification and validation of vulnerabilities identified during testing. This requirement will ensure that the approach and attack models are properly met.*  *An IA and CSP may add more lines to this table to accommodate testing parameters. Note that the Penetration Testing Plan and Rules of Engagement must be submitted and include all of the agreed upon threat and attack models.*  *See NIST SP 800-115 for further guidance. CSPs must be careful to differentiate between penetration testing and vulnerability assessment; these are not the same activity. The penetration test should not be strictly limited to automated scanning techniques, but manual techniques, as well.*  Delete this instructional text from your final version of this document. |

The following table captures the minimum requirements for penetration testing based on FedRAMP requirements. Additional attack vectors are outlined in the table below and will be recorded in the {{SSP|SECURITYPLAN.SYSTEMNAME}} Penetration Test Report. Deviations between this list and the Penetration Test Report will be recorded and explained in the SAR table “Deviations from the SAP”.

Techniques to test each system may vary depending on the service offering (IaaS, PaaS, SaaS, and Hybrid). Due to system commonalities, the mandatory attack vectors apply to all systems, as indicated by the “x” in the “Include” column. Ensure that all the appropriate threat models and attack models are marked a “x”, as well. The {{SSP|SECURITYPLAN.SYSTEMNAME}} Penetration Test Report will include the testing of all the parameters, as indicated in this table.

*Table C-1 Mandatory and Additional Attack Vectors*

| Include | Mandatory Attack Vectors | Include | Threat Models | Include | Attack Models |
| --- | --- | --- | --- | --- | --- |
| **X** | ***External to Corporate*** |  | ***Internet based (Untrusted):*** |  | ***Enterprise*** |
| **X** | ***External to CSP Target System*** |  | Network threat actor |  | Reconnaissance |
| **X** | ***Tenant to CSP Management System*** |  | Attack on CSP managed user |  | Resource Development |
| **X** | ***Tenant to Tenant*** |  | Email attack against CSP managed user |  | Initial Access |
| **X** | ***Mobile Application to Target System*** |  | Application threat actor |  | Execution |
| **X** | ***Client-side Application and/or Agents to Target System*** |  | Physical based attack |  | Persistence |
|  |  |  | ***CSP Corporate (Untrusted and Trusted)*** |  | Privilege Escalation |
|  |  |  | Breach of CSP management systems |  | Defense Evasion |
|  |  |  | Breach of CSP managed support system and/or networks |  | Credential Access |
|  |  |  | Breach of CSP managed enclave of authorized systems |  | Discovery |
|  |  |  | Corporate insider threat |  | Lateral Movement |
|  |  |  | Lost CSP managed system |  | Collection |
|  |  |  | Interconnected networks including international entities, foreign adversaries internally  pivoting to US CSO enclave |  | Command and Control |
|  |  |  | Ransomware spread from CSP Corporate |  | Exfiltration |
|  |  |  | Unauthorized physical access to authorized system |  | Impact |
|  |  |  | ***Internal Threat (Untrusted and Trusted)*** |  | ***Mobile*** |
|  |  |  | Weak permissions and access control |  | Initial Access |
|  |  |  | Abuse of services of authorized system |  | Execution |
|  |  |  | Ransomware spread from government system |  | Persistence |
|  |  |  | Multi organization access to authorized system |  | Privilege Escalation |
|  |  |  | Unauthorized physical access to authorized system |  | Defense Evasion |
|  |  |  |  |  | Credential Access |
|  |  |  |  |  | Discovery |
|  |  |  |  |  | Lateral Movement |
|  |  |  |  |  | Collection |
|  |  |  |  |  | Command and Control |
|  |  |  |  |  | Exfiltration |
|  |  |  |  |  | Impact |
|  |  |  |  |  | Network Effects |
|  |  |  |  |  | Remote Service Effects |

# Significant Change Request Documentation

|  |
| --- |
| ***Instruction:*** |
| *Embed or reference copies of the SCRs that were submitted by the CSP to the AO/JAB for review. If this SAP is not being used for a SCR, remove this entire Appendix.*  Delete this instructional text from your final version of this document. |

The following is SCR documentation that was submitted by {{SSP|SECURITYPLAN.CSPORGNAME}} to <Choose One: AO/JAB>:

* <Insert the SCR Form(s) and Supporting Documents>
* <Insert the SCR Inventory (e.g., any components that are being added to the inventory, removed from the inventory, or are being modified or directly impacted by the change(s).>
* <Insert the Embedded Excel File using the FedRAMP Standard Inventory Template>

Roles are described in the {{SSP|SECURITYPLAN.SYSTEMNAME}} SSP, Section 11, Separation of Duties. Additional roles that are being introduced as part of significant changes will be tested and are noted in Table D-1. Role testing will be performed to test the authorization restrictions for each role. {{MA|LEADASSESSOR.FULLNAME}} will access the system while logged in as different user types and attempt to perform restricted functions for that user.

*Table D-1 Role Based Testing*

| **Role Name** | **Test User ID** | **Associated Functions** |
| --- | --- | --- |
|  |  |  |
|  |  |  |