|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  |  | |  |
|  | FedRAMP® Security Assessment Report (SAR)  for <Insert CSP Name>  <Insert CSO Name>  <Version X.X>  <MM/DD/YYYY> | |  |
|
|  |  | |  |
|  |  | info@fedramp.gov  fedramp.gov |  |

TEMPLATE REVISION HISTORY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Pages | Description | Author |
| 01/20/2017 | 3.1 | All | * Changed “Zip” to “ZIP” and corrected input field label in the “Prepared By” section * Corrected horizontal axis of table 3-6 from “Likelihood” to “Impact” * Corrected references to the Security Assessment Summary Worksheet, and added it to the FedRAMP website * Corrected erroneous footers reading “Confidential Unclassified Information” to “Controlled Unclassified Information”, and removed duplicate page numbers appearing in some footers in the middle of the footer text * Corrected typographical errors, capitalization, format * Added and clarified instruction boxes * Made all external links appear in the text for clarity * Corrected missing common input fields by including them as linked form fields * Removed Appendix K, which referred to an immature Table Creation Tool. | FedRAMP |
| 02/22/2017 | 3.2 | Appendix A, Section 4 | Updated TOC to capture Appendix A RISK EXPOSURE TABLE | FedRAMP |
| 03/09/2017 | 3.3 | Appendix H | * Implementation Statement Differential changed back to “Yes” or “No” from “Low”, “Moderate” or “High” (this changed the verbiage throughout Appendix H) * Updated table of contents to ensure pages numbers are current | FedRAMP |
| 06/06/2017 | 3.3 | Cover | Updated logo | FedRAMP |
| 01/21/2022 | 3.3 | 1,3,36 | Updated outdated links | FedRAMP |
| 06/30/2023 | 4.0 | All | * Initial publication after combining the initial and annual SAR templates * New template can also be used for significant change requests | FedRAMP |
| 12/06/2024 | 5.0 | All | * Updated to remove JAB and PMO references * Added columns to Table 2-2 Summary of Risks That Remained Open at the Conclusion of the Assessment | FedRAMP |

**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. 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 <Insert CSO Name>.*  ***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 SAR template. Before delivering the final version of the SAR, 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** | <Enter Company/Organization> |
| **Street Address** | <Enter Street Address> |
| **Suite/Room/Building** | <Enter Suite/Room/Building> |
| **City, State Zip** | <Enter City, State, and Zip Code> |

Prepared for

|  |  |
| --- | --- |
| Identification of Cloud Service Provider | |
| **Organization Name** | <Enter Company/Organization> |
| **Street Address** | <Enter Street Address> |
| **Suite/Room/Building** | <Enter Suite/Room/Building> |
| **City, State Zip** | <Enter City, State, and Zip Code> |

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 6](#_Toc184297586)

[1.1 About This Document 6](#_Toc184297587)

[1.2 Who Should Use This Document? 6](#_Toc184297588)

[2 Executive Summary 7](#_Toc184297589)

[2.1 Purpose 14](#_Toc184297590)

[2.2 Applicable Laws, Regulations, Standards, and Guidance 14](#_Toc184297591)

[2.3 Scope 14](#_Toc184297592)

[2.3.1 Controls Assessed 15](#_Toc184297593)

[3 System Overview 15](#_Toc184297594)

[3.1 System Description 15](#_Toc184297595)

[4 Assessment Methodology 15](#_Toc184297596)

[4.1 Deviations from the SAP 16](#_Toc184297597)

[4.2 The SRTM 16](#_Toc184297598)

[4.3 Consideration of Threats 16](#_Toc184297599)

[4.4 Document Results 17](#_Toc184297600)

[5 Risks Known for Interconnected Systems and External Services 18](#_Toc184297601)

[Appendix A Risk Exposure Table 20](#_Toc184297602)

[Appendix B Security Requirements Traceability Matrix (SRTM) Workbook 20](#_Toc184297603)

[Appendix C Vulnerability Scan Results 20](#_Toc184297604)

[Appendix D Documentation Review Findings 31](#_Toc184297605)

[Appendix E Auxiliary Documents 31](#_Toc184297606)

[Appendix F Penetration Test Report 32](#_Toc184297607)

# Introduction

## About This Document

This document is developed as a template when creating a FedRAMP Security Assessment Report (SAR). This template should be used for all initial authorization assessments, annual assessments, and significant change assessments.

Independent assessors (IAs) must complete this SAR template based upon a specific cloud service offering’s (CSO’s) security assessment as captured in the CSO’s security assessment plan (SAP). This SAR documents the risk posture for a CSO based on a point-in-time security assessment.

A CSP must keep in mind that an IA must follow all FedRAMP requirements in preparing this SAR. 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 FedRAMP Agency Authorization, AO refers to each leveraging agency’s AO.

## Who Should Use This Document?

This SAR template is intended to be populated by a FedRAMP recognized third party assessment organization (3PAO) or an independent assessment organization (IAO) when documenting the results of a FedRAMP security assessment. AOs will review this completed SAR to make risk-based authorization decisions.

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 of the FedRAMP SAP Template). 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”.

# Executive Summary

Table ‑ <Insert CSP Name>, <Insert CSO Name> Information

| **FedRAMP Unique Identifier** | **CSP** | **CSO** | **Service Model** | **Deployment Model** | **Impact Level** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

|  |
| --- |
| ***Instruction:*** |
| *The Executive Summary begins here.*  *Note: For initial assessments, as well as assessments to uplift a CSO from the FedRAMP Moderate to the High baseline, all High risks must be remediated prior to an IA recommending the CSO for FedRAMP authorization. There are some specific use cases where an agency AO may allow High risks for the annual assessment. However, since all High findings must be remediated within 30 days, FedRAMP expects most High findings to be remediated prior to an annual assessment package submission. In such cases, an IA must provide solid rationale for recommending the CSO to maintain their FedRAMP authorization. Some High risks may be downgraded to Moderate due to mitigating factors. If an IA believes there is strong justification that a High risk can be downgraded to Moderate, the IA must submit a deviation request (DR) along with the risk adjustment (RA) in the Risk Exposure Table (RET). High ORs must be risk adjusted to a lower risk rating (i.e., a risk adjusted deviation request for an operational requirement).*  *For an initial or annual assessment, at a minimum, IAs must describe the following:*  *Overall alignment with the National Institute of Standards and Technology (NIST) definition of cloud computing according to NIST SP 800-145 (NOTE: This includes the requirement for a CSP to have a self-service portal);*  *Notable strengths and weaknesses;*  *Ability to consistently maintain a clearly defined system boundary;*  *Ability to accurately describe intra and inter-system user and sensitive metadata data flow;*  *Risks associated with interconnections used to transmit federal data/metadata or sensitive system data/metadata;*  *Risks associated with the use of external systems and services that are not FedRAMP Authorized;*  *Clearly defined customer responsibilities;*  *Unique or alternative implementations;*  *Overall maturity level relative to the system type, size, and complexity; and*  *Overall operational maturity relative to how long the system and required security controls have been in operation.*  Delete this and all other instructional text from your final version of this document. |

This is <Choose One: an initial assessment/an annual assessment/a combined annual assessment and significant change assessment/a significant change assessment> SAR as required by FedRAMP. This SAR aggregates the results of the required FedRAMP security assessment of the <Insert CSO Name> environment as recorded in the <Insert CSO Name> <Choose One: SSP/SSP and significant change documentation/significant change documentation>.

All identified findings are recorded in the SAR Appendix A, Risk Exposure Table (RET). The RET documents all open risks that remained at the conclusion of the assessment, including all risk adjustments (RAs), operational requirements (ORs), and vendor dependencies (VDs)[[1]](#footnote-2). These are identified in the “Risk Exposure Table (RET)” tab. Risks validated as closed during the assessment are identified in the “Risks Corrected During Testing” tab.

The assessment took place from <Choose One: for initial testing window MM/DD/YYYY to MM/DD/YYYY and remediation testing window MM/DD/YYYY to MM/DD/YYYY/this assessment began MM/DD/YYYY and ended MM/DD/YYYY>.

|  |
| --- |
| ***Instruction:*** |
| *Affirm the type of assessment completed for this SAR (e.g., initial, annual, significant change, etc.). Use the correct narratives and remove any narratives that are not applicable.*  Delete this instructional text from your final version of this document. |

**Initial Assessment:**

This report is for an initial assessment of <Insert CSO Name>, a <Choose One: High/Moderate/ Low> 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 of the SAP.

**Annual Assessment:**

This report is for an annual assessment of <Insert CSO Name>, a <Choose One: High/Moderate/ Low> baseline system. After the initial security assessment, FedRAMP requires that the system is assessed annually, thereafter (12 months from an agency 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 the CSP since the 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 <Insert CSO Name> Security Controls Selection Worksheet.

**Significant Change:**

This report <Choose One: is for/also includes> the assessment completed for <Choose One: a significant change/several significant changes>. The <Insert CSO Name> SAP, Appendix D includes the significant change request documentation submitted by <Insert CSP Name> to the agency AO.

Appendix A includes the associated control selections. <Insert IA Name> did 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 applicable to the significant change assessment. <Insert IA Name> did 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 to the significant change assessment>.

Below is a summary of risks that remained open at the conclusion of this assessment. Refer to the Appendix A RET workbook for additional details.

Table ‑ Summary of Risks that Remained Open at the Conclusion of this Assessment

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Category** | **Total** | **Operational Requirement (OR)\*** | **Vendor Dependency (VD)\*\*** | **SRTM Test Cases** | **OS Scans** | **Web Scans** | **DB Scans** | **Container Scans** | **Pen Test** | **CM-6 Finds** |
| **High (H)** | [Number] |  |  |  |  |  |  |  |  |  |
| **H RA to Moderate (M)** | [Number] |  |  |  |  |  |  |  |  |  |
| **M** | [Number] |  |  |  |  |  |  |  |  |  |
| **H RA to Low (L)** | [Number] |  |  |  |  |  |  |  |  |  |
| **M RA to L** | [Number] |  |  |  |  |  |  |  |  |  |
| **L** | [Number] |  |  |  |  |  |  |  |  |  |
| **Total Risks** | **[Number]** |  |  |  |  |  |  |  |  |  |

*\* ORs are considered open risks and are counted in the total number of risks identified for a system. A CSP should be actively seeking ways to mitigate or eliminate the risks associated with ORs.*

*\*\*VDs are considered open risks that must be counted in the total number of risks identified for a system. A CSP should be actively seeking ways to mitigate or eliminate the risks associated with VDs. If a VD is ongoing, a CSP may have to migrate to a different technology/vendor.*

Details of the assessment approach are documented in the SAP, <Insert Version X.X>, dated <Insert MM/DD/YYYY>. Any deviations from the approved SAP are noted in Table 4-1, *List of Assessment Deviations* below.

The following were completed for this assessment: <Choose all that apply: manual testing/penetration testing/ web application vulnerability scans/database vulnerability scans/operating system vulnerability scans/container vulnerability scans>.

|  |
| --- |
| ***Instruction:*** |
| *Choose the appropriate sentence and delete the inappropriate sentences. If there are multiple significant changes, list each significant change as identified in the SCR.*  *NOTE: If there are multiple significant changes, it is possible that there are a mix of “recommend” and “does not recommend” statements.*  *Identify and qualify the significant changes that are recommended beneath that recommendation statement.*  *Identify and qualify the significant changes that are NOT recommended beneath that recommendation statement.*  Delete this and all other instructional text from your final version of this document. |

<Insert IA Name> recommends this system for authorization.

<Insert IA Name> does not recommend this system for authorization.

<Insert IA Name> recommends this system for continued authorization.

<Insert IA Name> does not recommend this system for continued authorization.

<Insert IA Name> recommends the following <Choose One: significant change/significant change(s)> included in this assessment for authorization:

<List the significant changes that are approved for authorization.>

<Insert IA Name> does not recommend the following <Choose One: significant change/significant change(s)> included in this assessment for authorization.

<List the significant changes that are NOT approved for authorization.>

## Purpose

The purpose of this document is to report the results of a point-in-time assessment of the <Insert CSO Name> security posture that was performed according to the methodology described in Section 4.

## Applicable Laws, Regulations, Standards, and Guidance

The FedRAMP-applicable laws, regulations, standards, and guidance is included in the <Insert CSO Name> SSP section - System Security Plan Approvals. This version governs the requirements for this assessment. Additionally, in Appendix L of the SSP, the <Insert CSP Name> has included laws, regulations, standards, and guidance that apply specifically to this system.

## Scope

The scope of the <Insert CSO Name> assessment is documented in the <Insert CSP Name>, <Insert CSO Name> SAP, <Insert Version X.X>, dated <Insert MM/DD/YYYY>. Deviations from the SAP are captured in Section 4.1, Deviations from the SAP. NOTE: Net-new risks identified during remediation activities are captured on the “Open” tab of the <Insert CSO Name> Plan of Action & Milestones (POA&M). These risks are not captured in the RET because the RET represents a point-in-time assessment.

<Insert CSO Name> is physically located at the facilities noted in Table 2-3.

|  |
| --- |
| ***Instruction:*** |
| *If this system leverages a FedRAMP Authorized Iaas or IaaS/PaaS, list the locations of the primary and secondary data centers.*  Delete this and all other instructional text from your final version of this document. |

Table ‑ Site Names and Addresses

| **Data Center Site Name** | **Address** | **Description Of Components** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

As verified by <Insert IA Name>, this assessment includes the documents listed in the [FedRAMP Initial Authorization Package Checklist](https://www.fedramp.gov/assets/resources/templates/FedRAMP-Initial-Authorization-Package-Checklist.xlsx) and this SAR Appendix E - Auxiliary Documents.

### Controls Assessed

The security controls that were assessed are those identified in the approved <Insert CSO Name> SAP, <Insert Version X.X>, dated <Insert MM/DD/YYYY>.

# System Overview

## System Description

The <Insert CSO Name> system description and purpose are as captured in the <Insert CSP Name> <Insert CSO Name> SSP, <Insert Version X.X>, dated <Insert MM/DD/YYYY>.

|  |
| --- |
| ***Instruction:*** |
| *Insert a significant change description below this instruction if the document is being used for significant changes.*  Delete this and all other instructional text from your final version of this document. |

# Assessment Methodology

The assessment methodology is described in the <Insert CSO Name> SAP. <Insert IA Name> performed the assessment of <Insert CSP Name> <Insert CSO Name> against the <Insert CSO Name> environment based on the details captured in the <Insert CSO Name> <Choose One: SSP/SSP and significant change documentation noted in the SAP/significant change documentation noted in the SAP>. The assessment concluded on <Insert MM/DD/YYYY>.

## Deviations from the SAP

Deviations from the SAP-defined methodology are described below.

|  |
| --- |
| ***Instruction:*** |
| *If there are no deviations, this table is marked as N/A.*  Delete this and all other instructional text from your final version of this document. |

Table ‑ List of Assessment Deviations

| **Deviation ID** | **Deviation Description** | **Justification** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

## The SRTM

Risks identified by <Insert IA Name> through security control testing are recorded in the <Insert CSO Name> Security Requirements Traceability Matrix (SRTM) workbook.

As described in Section 4.4 below, risks identified (i) in the SRTM, (ii) through penetration testing, (iii) through vulnerability scanning, and (iv) through manual testing criteria are documented in the RET.

## Consideration of Threats

The Office of Management and Budget (OMB) and Cybersecurity and Infrastructure Security Agency (CISA) are working to move the U.S. government toward a zero-trust architecture where it must be presumed that anything may present a threat. Agencies must work with their CSOs to follow the CISA Zero Trust Architecture Model plans for implementing zero trust architecture.

## Document Results

The SAR Appendix A, RET contains the details of the system risks identified during the assessment, including:

1. All security controls failures noted in the SRTM

|  |
| --- |
| ***Instruction:*** |
| *For SRTM: Each column must be populated for every SRTM row entry. Ensure that the SRTM “Observations / Test Results” column clearly documents what was tested, how it was tested, and the end result of the test. Ensure the SRTM “Evidence'' column is also populated appropriately. If a portion of the security control fails, the entire control fails. If the end result documented in the “Observations / Test Results” column indicates a control failure, the “Assessment Result” must be marked as “Other than Satisfied”.*  *This guidance applies to entries in the RET regarding the SRTM to ensure all stakeholders understand.*  Delete this and all other instructional text from your final version of this document. |

1. All penetration testing failures

|  |
| --- |
| ***Instruction:*** |
| *For the penetration test results, ensure that every mandatory attack vector and every IA/CSP agreed upon attack vector(s) is/are recorded in the SAP. If any of the attack vectors are not included, explain these in the “Deviations from the SAP” section of this SAR.*  *This guidance applies to entries in the RET to ensure that the penetration testing exercise is as complete as possible and to ensure all stakeholders understand.*  Delete this and all other instructional text from your final version of this document. |

1. All vulnerabilities detected during scanning

|  |
| --- |
| ***Instruction:*** |
| *ALL scan-related findings must be included in the RET and must match the machine-readable results, one to one. All scan-related control findings (e.g., running unauthenticated scans) must be recorded in the RET.*  *This guidance applies to vulnerability scan findings recorded on the RET to ensure that the authenticated vulnerability scanning exercise is as complete as possible and to ensure all stakeholders understand.*  Delete this and all other instructional text from your final version of this document. |

1. All weaknesses identified during manual testing (other than penetration testing)

|  |
| --- |
| ***Instruction:*** |
| Manual testing and manual security control testing is the process where an IA must manually evaluate, test, then assess the effectiveness of security controls within a system. Manual testing may be required if the CSP has named controls in the SSP as “Alternative Implementations”. Many times, the testing procedures for these Alternative Implementations requires testing additional security controls that may be named in the NIST baseline but not in the FedRAMP baseline. Other times, the IA finds that a security control is not being met in one control family and that affects several other controls in other control families. While the initial testing of the other security controls might have appeared to have been met, the presence of the non-compliant security control implementation suggests that other controls are now involved. The IA may devise manual ways to provide some credence to the failures.  Delete this and all other instructional text from your final version of this document. |

# Risks Known for Interconnected Systems and External Services

|  |
| --- |
| ***Instruction:*** |
| *Relevant information is contained in the SSP tables “Leveraged FedRAMP Authorized Services” and “External Systems/Services, Interconnections, APIs, and CLIs Not Having FedRAMP Authorizations.” These tables contain all “Update Sources” for services installed within the system boundary that must be updated by the CSP and a summary of all interconnected systems and external services. If a product is mentioned in the SSP, the product must be listed in one of those two tables, as it logically falls into one of the above-mentioned descriptions. IAs must review and validate the leveraged and external services captured in the aforementioned tables.*  *If a CSO is leveraging an external service in a way that does not comply with FedRAMP requirements, including the FedRAMP Authorization Boundary Guidance, this is a finding that must be captured in the RET.*  *Per the above, “External Systems/Services, Interconnections, APIs, and CLIs Not Having FedRAMP Authorizations”, agency customers must understand that non-authorized services have not been assessed and represent unknown risk. Agency customers must understand how their data is interacting with such services and must assess and accept risk for the use of these external services, especially those services that provide critical security functionality. Therefore, risks associated with the use of non-authorized external systems/services, interconnections, APIs, and CLIs (listed in this table) must be captured in the RET.*  *In addition, external systems/services that are used by a CSO, but not mentioned in the “Leveraged and External Services” tables, must be captured in the RET.*  *Conversely, for the “Leveraged FedRAMP Authorized Services” risk, this is a non-finding that is the responsibility of FedRAMP Authorized service providers to remediate. These are not a customer’s responsibility to remediate and should not appear on the leveraging CSO POA&M.*  Delete this and all other instructional text from your final version of this document. |

Inherent relationships between <Insert CSO Name> and other interconnected systems may impact the overall system security posture. External services that are used to provide functionality to <Insert CSO Name> or used to manage and operate <Insert CSO Name> may also impact the overall system security posture (e.g. the extent to which data/metadata contained in the external service might be leveraged to exploit the main cloud service offering). Risks associated with interconnected systems, external systems/services, interconnections, APIs, and CLIs are documented in the RET.

1. Risk Exposure Table

The Risk Exposure Table (RET) captures all security risks identified during this assessment. This workbook also captures all risks that were validated by <Insert IA Name> as closed during testing. Beginning in this Revision 5 Report, FedRAMP would like any Configuration Findings, “CM-6 findings” tracked as follows: one finding in the RET as a CM-6 failure (multiple findings wrapped into one) and then **all**findings detailed out on the Configuration Findings tab. The CSP must record the same in their POA&M, on their POA&M Configuration Findings tab.

1. Security Requirements Traceability Matrix (SRTM) Workbook

The SRTM captures the results of the security controls testing.

|  |
| --- |
| ***Instructions:*** |
| *An IA must examine the CSO POA&M spreadsheet (required for CSOs with a FedRAMP authorization) to ensure that the IA has captured all findings that are still open. Sometimes an IA determines that a few POA&M items have closed based on remediations completed during the assessment.*  *The SRTM templates for High, Moderate, Low impact systems are available on the* [FedRAMP Documents and Templates webpage](https://www.fedramp.gov/documents-templates/).  Delete this and all other instructional text from your final version of this document. |

1. Vulnerability Scan Results

|  |
| --- |
| ***Instruction:*** |
| *Ensure both the raw, authenticated scan files and the human readable scan files are included for OS/infrastructure, containers, databases, and web applications. Do not submit this SAR without all scan files and results accompanying this package. The IA is responsible for ensuring that the CSP is capturing all inventory items in the FedRAMP Integrated Inventory Workbook; the scanning exercise must validate the inventory at this specific point in time. The inventory should be captured as follows:*   * *Containers: There needs to be an identifiable string in the scans that maps back to that image name/version in use; this is typically the repository/image/version# or can be represented as a hash.*    + *For the inventory:*     - *Column A should contain the Repository/Image Name/Version# (CSP Defined).*     - *Column B should contain the individual hash of the container in the registry for each of the containers in production that align to the Repository/Image Name/Version#.* * *For any scanned inventory item that is not a container, the identifier (e.g., the hostname, IP, or URL for web) should align to the asset and should be verified/found within the scans provided by the CSP/IA.* * *A hash used as a unique identifier (column A) for any asset that is internal only to the CSP and not found on the scans is not useful as it cannot be verified outside of the CSP through the delivered monthly/yearly scans.*   Delete this and all other instructional text from your final version of this document. |

Infrastructure Scan Results

Infrastructure scanning includes servers, storage, networking, virtualization software, services and management tools that support the computing requirements of a cloud computing model. Cloud infrastructure also includes a layer of programming (hardware abstraction layer or HAL) that allows a computer operating system to interact with a hardware device at a general or abstract level rather than at a detailed hardware level. HAL virtualizes and logically presents resources and services to users through application programming interfaces (APIs) and API-enabled command-line or graphical interfaces. An API is code that allows two software programs to communicate with each other.

<Insert Scanner Name, Vendor, and Version X.X> was used to scan the <Insert CSO Name> infrastructure. <Insert Percentage>% of the inventory was scanned. <Include the following if true> For the remaining inventory, the <Insert IA Name> performed a manual review of configuration files to analyze for existing vulnerabilities. Both the authenticated raw scan results and the human-readable version(s) are provided as a Zip file with this SAR. Infrastructure scan vulnerabilities are documented in the RET.

Infrastructure Scans: Inventory of Items Scanned

|  |
| --- |
| ***Instruction:*** |
| *The infrastructure scans must match the SSP Integrated Inventory Workbook exactly. If the scanning reveals system components that are not recorded in the Integrated Inventory Workbook, note this as a finding or deviation, or perhaps several findings/deviations if the discrepancy is based on several components. If a discrepancy exists provide the reasons why in this section.*  Delete this and all other instructional text from your final version of this document. |

<Choose One: There were no discrepancies found between the scanned and documented inventory/discrepancies with the scanned inventory and the documented inventory have been recorded in the RET. The discrepancies were due to <Describe Reasons Here>>.

Infrastructure Scans: Raw Scan Results

|  |
| --- |
| ***Instruction:*** |
| *The filenames of the raw scan results must be provided below and must accompany this SAR. If the raw results files are too large to embed in this document, provide the scans as an attachment to the SAR. Whether embedded or provided as a separate attachment, zip the raw scan files into one Zip file. In this section, provide the name of the Zip file along with the names of the raw scan files that the Zip file contains.*  Delete this and all other instructional text from your final version of this document. |

The table below includes raw infrastructure scan files from this assessment. Any new vulnerabilities introduced in remediation scan files, included in the table below and detected as of <Insert MM/DD/YYYY>, are outside the scope of this assessment. These new findings must be captured in a CSP's POA&M, for monthly continuous monitoring, in accordance with FedRAMP’s POA&M guidance.

Table C-1 Infrastructure Scans: Raw Scan Zip File Index

| **Title** | **File Name (Include Extension)** |
| --- | --- |
|  |  |
|  |  |
|  |  |

Infrastructure Scans: False Positive Reports

|  |
| --- |
| ***Instruction:*** |
| *Validate all false positives (FPs) identified. Once validated, the FPs are then considered closed and are recorded appropriately in the “Risks Corrected During Testing” tab of the RET.*  Delete this and all other instructional text from your final version of this document. |

<Insert IA Name> has validated all false positives (FPs) identified. While a validated FP confirms that there was no weakness present to correct, validated FPs are documented in the “Risks Corrected During Testing” tab of the RET as a convenient way to track FPs.

Database Scan Results

<Insert Scanner Name, Vendor, and Version X.X> was used to scan the <Insert CSO Name> databases. <Insert Percentage>% of all databases were scanned. <Include the Following if True> For the remaining inventory, the <Insert IA Name> performed a manual review of configuration files to analyze for existing vulnerabilities. Both the authenticated raw scan results and the human-readable version(s) are provided as an attachment to this SAR. Database scan vulnerabilities are documented in the RET.

Database Scans: Inventory of Databases Scanned

|  |
| --- |
| ***Instruction:*** |
| *The database scans must match the* [FedRAMP SSP Integrated Inventory Workbook](https://www.fedramp.gov/assets/resources/templates/SSP-Appendix-M-Integrated-Inventory-Workbook-Template.xlsx) *exactly. If the scanning reveals database components that are not recorded in the integrated inventory workbook, note this as a finding or deviation or perhaps several findings/deviations if the discrepancy is based on several components. If a discrepancy exists, provide the reasons why in this section.*  Delete this and all other instructional text from your final version of this document. |

<Choose One: There were no discrepancies found between the scanned and documented inventory/discrepancies with the scanned inventory and the documented inventory have been recorded in the RET. The discrepancies were due to <Describe Reasons Here>>.

Database Scans: Raw Scan Results

|  |
| --- |
| ***Instruction:*** |
| *The filenames of the raw scan results must be provided below and must accompany this SAR. If the raw results files are too large to embed in this document, provide the scans as an attachment to the SAR. Whether embedded or provided as a separate attachment, zip the raw scan files into one Zip file. In this section, provide the name of the Zip file along with the names of the raw scan files that the Zip file contains.*  Delete this and all other instructional text from your final version of this document. |

The table below includes raw database scan files from this assessment. Any new vulnerabilities introduced in remediation scan files, included in the table below and detected as of <Insert MM/DD/YYYY>, are outside the scope of this assessment. These new findings must be captured in a CSP's POA&M, for monthly continuous monitoring, in accordance with FedRAMP’s POA&M guidance.

Table C-2 Database Scans: Raw Scan Zip File Index

| **Title** | **File Name (Include Extension)** |
| --- | --- |
|  |  |
|  |  |
|  |  |

Database Scans: False Positive Reports

|  |
| --- |
| ***Instruction:*** |
| *Validate all FPs identified. Once validated, the FPs are then considered closed and are recorded appropriately on the “Risks Corrected During Testing” tab of the RET.*  Delete this and all other instructional text from your final version of this document. |

<Insert IA Name> has validated all FPs identified. While a validated FP confirms that there was no weakness present to correct, validated FPs are documented in the “Risks Corrected During Testing” tab of the RET as a convenient way to track FPs.

Web Scan Results

<Insert Scanner Name, Vendor, and Version X.X> was used to scan the <Insert CSO Name> Web applications. This includes all external APIs. <Insert Percentage>% of all Web applications were scanned. <Insert Percentage>% of all APIs were scanned. <Include the Following if True> For the remaining inventory, the <Insert IA Name> performed a manual review of configuration files to analyze for existing vulnerabilities. Both the authenticated, raw scan results and the human-readable version(s) are provided as a Zip file with this SAR. Web application scan vulnerabilities are documented in the RET.

|  |
| --- |
| ***Instruction:*** |
| *The Web application scans must match the* [FedRAMP SSP Integrated Inventory Workbook](https://www.fedramp.gov/assets/resources/templates/SSP-Appendix-M-Integrated-Inventory-Workbook-Template.xlsx) *exactly. If the scanning reveals components that are not recorded in the integrated inventory workbook, note this as a finding or deviation or perhaps several findings/deviations if the discrepancy is based on several components. If a discrepancy exists, provide the reasons why in this section.*  Delete this and all other instructional text from your final version of this document. |

<Choose One: There were no discrepancies found between the scanned and documented inventory/discrepancies with the scanned inventory and the documented inventory have been recorded in the RET. The discrepancies were due to <Describe Reasons Here>>.

Web Applications Scans: Raw Scan Results

|  |
| --- |
| ***Instruction:*** |
| *The filenames of the raw scan results must be provided below and must accompany this SAR. If the raw results files are too large to embed in this document, provide the scans as an attachment to the SAR. Whether embedded or provided as a separate attachment, zip the raw scan files into one Zip file. In this section, provide the name of the Zip file along with the names of the raw scan files that the Zip file contains.*  Delete this and all other instructional text from your final version of this document. |

The table below includes the raw Web application scan files from this assessment. Any new vulnerabilities introduced in remediation scan files, included in the table below and detected as of <Insert MM/DD/YYYY>, are outside the scope of this assessment. These new findings must be captured in a CSP's POA&M, for monthly continuous monitoring, in accordance with FedRAMP POA&M guidance.

Table C-3 Web Application Scans: Raw Scan Zip File Index

| **Title** | **File Name (Include Extension)** |
| --- | --- |
|  |  |
|  |  |
|  |  |

Web Applications Scans: False Positive Reports

|  |
| --- |
| ***Instruction:*** |
| *Validate all FPs identified. Once validated, the FPs are then considered closed and are recorded appropriately in the “Risks Corrected During Testing” tab of the RET.*  Delete this and all other instructional text from your final version of this document. |

<Insert IA Name> has validated all FPs identified. While a validated FP confirms that there was no weakness present to correct, validated FPs are documented in the “Risks Corrected During Testing” tab of the RET as a convenient way to track FPs.

Container Scan Results

<Insert Scanner Name, Vendor, and Version X.X> was used to scan the <Insert CSO Name> containers. <Insert Percentage>% of all container images were scanned. <Include the Following if True> For the remaining container inventory, the <Insert IA Name> performed a manual review of configuration files to analyze for existing vulnerabilities. Both the authenticated, raw scan results and the human-readable version(s) are zipped and associated with this SAR. Container vulnerabilities are documented in the RET.

Container Scans: Inventory of Container Images Scanned

|  |
| --- |
| ***Instruction:*** |
| *Container scans must align with the* [FedRAMP Vulnerability Scanning Requirements for Containers](https://www.fedramp.gov/assets/resources/documents/Vulnerability_Scanning_Requirements_for_Containers.pdf) *document.*  *"While individually deployed instances of containers should be tracked internally by the CSP, they do not need to be included as part of the FedRAMP Integrated Inventory Workbook Template, unless they are specifically the target of a scan performed by a security sensor."*  *If the scanning reveals components that are not recorded in the integrated inventory workbook, note this as a finding or deviation or perhaps several findings/deviations if the discrepancy is based on several components. If a discrepancy exists, provide the reasons why in this section.*  Delete this and all other instructional text from your final version of this document. |

<Choose One: There were no discrepancies found between the scanned and documented inventory/discrepancies with the scanned inventory and the documented inventory have been recorded in the RET. The discrepancies were due to <Describe Reasons Here>>.

Container Scans: Raw Scan Results

|  |
| --- |
| ***Instruction:*** |
| *The filenames, of the raw scan results, must be provided below and must accompany this SAR. If the raw results files are too large to embed in this document, provide the scans as an attachment to the SAR. Whether embedded or provided as a separate attachment, zip the raw scan files into one Zip file. In this section, provide the name of the Zip file along with the names of the raw scan files that the Zip file contains.*  Delete this and all other instructional text from your final version of this document. |

The table below includes the raw container scan files from this assessment. Any new vulnerabilities introduced in remediation scan files, included in the table below and detected as of <Insert MM/DD/YYYY>, are outside the scope of this assessment. These new findings must be captured in a CSP's POA&M, for monthly continuous monitoring, in accordance with FedRAMP’s POA&M guidance.

Table C-4 Container Scans: Raw Scan Zip File Index

| **Title** | **File Name (Include Extension)** |
| --- | --- |
|  |  |
|  |  |
|  |  |

Container Scans: False Positive Reports

|  |
| --- |
| ***Instruction:*** |
| *Validate all FPs identified. Once validated, the FPs are then considered closed and could be recorded appropriately on the “Risks Corrected During Testing” tab of the RET, in order to keep documented affirmation.*  Delete this and all other instructions from your final version of this document. |

<IA Name> has validated all FPs identified. While a validated FP confirms that there was no weakness present to correct, validated FPs are documented in the Risks Corrected During Testing tab of the RET as a convenient way to track FPs.

Other Automated and Miscellaneous Tool Results: Tools Used

Other Automated and Miscellaneous Tool Results: Inventory of Items Scanned

|  |
| --- |
| ***Instruction:*** |
| *Follow the same instructions noted in the OS/Infrastructure, Database, Web Application, and Containers sections. If there are no other tools used, mark this section as “Not Applicable”.*  Delete this and all other instructional text from your final version of this document. |

Other Automated and Miscellaneous Tool Results: Raw Scan Results

|  |
| --- |
| ***Instruction:*** |
| *Follow the same instructions noted in the OS/Infrastructure, Database, Web Application, Containers sections.*  *Examples:*  *Static code analysis*  *Dynamic code analysis*  *Configuration scan tool (CM-6)*  *Open source scan tools (if applicable)*  *If there are no other tools used, mark this section as “Not Applicable”.*  Delete this and all other instructional text from your final version of this document. |

The table below includes both the authenticated raw scan files and the human-readable version(s) from this assessment. Any new vulnerabilities introduced in remediation scan files, included in the table below and detected as of <Insert MM/DD/YYYY>, are outside the scope of this assessment. These new findings must be captured in a CSP's POA&M, for monthly continuous monitoring, in accordance with FedRAMP’s POA&M guidance.

Table C-5 Other Automated and Miscellaneous Tool Results: List of Raw Scan Result Files

| **Title** | **File Name (Include Extension)** |
| --- | --- |
|  |  |
|  |  |
|  |  |

Other Automated and Miscellaneous Tool Results: False Positive Reports

|  |
| --- |
| ***Instruction:*** |
| *Follow the same instructions noted in the OS/Infrastructure, Database, Web Application, Containers sections. If there are no other tools used, mark this section as “Not Applicable.”*  Delete this and all other instructional text from your final version of this document. |

<Insert IA Name> has validated all FPs identified. While a validated FP confirms that there was no weakness present to correct, validated FPs are documented in the “Risks Corrected During Testing” tab of the RET as a convenient way to track FPs.

Unauthenticated Scans

FedRAMP defines the thresholds for unauthenticated scans, where authenticated scans are possible under different circumstances (e.g., proper account configuration), in the [FedRAMP Continuous Monitoring Performance Management Guide](https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Performance_Management_Guide.pdf). Non-compliance with this threshold is documented as an open finding in the RET. Where authenticated scans are not possible, under any circumstances, <Insert IA Name> has documented the component, rationale, and the alternative assessment performed in Table C-7 below.

Table C-6 Summary of Unauthenticated Scans

| Identifier | Product/Embedded Component Description | Rationale | Alternative Assessment Methodology Description |
| --- | --- | --- | --- |
| UN0001 |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Documentation Review Findings

|  |
| --- |
| ***Instruction:*** |
| *Review findings associated with control implementation statements are captured at a granular level in the SRTM and must also be captured in the RET at a granular level. Enter “Documentation Review” in the “Weakness Detector Source” column in the RET.*  *Documentation findings associated with other portions of the SSP (e.g., incomplete, inaccurate, or inconsistent network boundary and data flow diagrams) must be captured as separate PL-2 findings in the RET.*  Delete this and all other instructional text from your final version of this document. |

All findings, including documentation review findings, are detailed in the SRTM and RET.

1. Auxiliary Documents

|  |
| --- |
| ***Instruction:*** |
| *Auxiliary documents are referenced in the SRTM “Evidence” column that go beyond the Appendices included with the SSP. Auxiliary documents must be readily available to reviewers via a CSP’s secure repository.*  Delete this and all other instructional text from your final version of this document. |

Auxiliary documents used by <Insert IA Name> to perform the testing for <Insert CSO Name> are listed below.

Table E-1 Auxiliary Documents

| **Title** | **Version** | **Filename** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. Penetration Test Report

|  |
| --- |
| ***Instruction:*** |
| *Provide the full penetration test report with this SAR.*  Delete this and all other instructional text from your final version of this document. |

<Insert IA Name> conducted a penetration test of <Insert CSO Name> from the <Provide Location Information> via an attributable Internet connection on <Insert MM/DD/YYYY>.

1. All CSPs should be reminded that VDs exist when the CSP must rely on a downstream vendor to issue a fix or patch. With regards to container images, CSPs should choose container images from reputable sources that handle patching in a FedRAMP compliant manner. CSPs should realize that if they build their own containers “in house”, then the CSP is the vendor and cannot declare a VD on an identified vulnerability. [↑](#footnote-ref-2)