FedRAMP Security Assessment Plan (SAP) Template



Third Party Assessment Organization (3PAO)
<3PAO Name>

for

Cloud Service Provider (CSP)
<CSP Name>

Information System Name

Version #.#

Version Date

Controlled Unclassified Information

Instruction: This template contains a number of features to facilitate data entry. As you go through the template entering data, you will see prompts for you to enter different types of data.

Repeatable Field

Some multiple-occurring data fields have been linked together, and you need only enter the data once. Enter the data once; then click outside the data entry field, and all occurrences of that field will be populated. For example, when you see “Information System Abbreviation” and replace it with your system abbreviation, all instances of the abbreviation throughout the document will be replaced with the value you entered. This document contains the following repeatable fields:

 3PAO Name

 CSP Name

Information System Name

 Version Number

 Version Date

 Information System Abbreviation

If you find a data field from the above list that has not populated, then press the F9 key to refresh the data. If you make a change to one of the above data fields, you may also have to press the F9 key to refresh the data throughout the document. Remember to save the document after refreshes.

Date Selection

Data fields that must contain a date will present a date selection menu.

Item Choice

Data fields that have a limited number of value choices will present a selection list.

Number Entry

Data fields that must have numeric values display “number”.

Text Entry

Many data fields, particularly in tables, that can contain any text display “Enter text” or “Click here to enter text”.

Delete this instruction from your final version of this document.

System Assessment Plan

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 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 Zip Code> |

Record of Changes for Template

| Date | Description | Version | Author |
| --- | --- | --- | --- |
| 6/6/2014 | Major revision for Special Publication (SP) 800-53 Revision 4. Includes new template and formatting changes.  | 2.0 | FedRAMP PMO |
| 1/20/2016 | 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. | 3.0 | FedRAMP PMO |
| 10/21/16 | Converted to standard document templateRemoved Acronyms and referenced FedRAMP Glossary and Acronyms resource documentClarity edits, and instructions for the new Integrated Inventory Template Section 2.2 | 3.1 | FedRAMP PMO |
| 3/9/2017 | Renamed document from "Security Assessment Plan (SAP) Template to "FedRAMP Security Assessment Plan (SAP) Template” | 3.2 | FedRAMP PMO |
| 6/6/2017 | Updated logo | 3.2 | FedRAMP PMO |

Revision History

| Date | Description | Version of SSP | Author |
| --- | --- | --- | --- |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |

How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact *info@FedRAMP.gov*

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

Table of Contents

[1 Introduction 1](#_Toc464807194)

[1.1 Laws, Regulations, Standards, and Guidance 1](#_Toc464807195)

[1.2 Purpose 1](#_Toc464807196)

[2 Scope 2](#_Toc464807197)

[2.1 Information System Name/Title 2](#_Toc464807198)

[2.2 Internet Protocol (IP) Addresses, WeB APPLICATIONS, and DATABASES Slated for Testing 2](#_Toc464807199)

[2.3 Roles Slated for Testing 3](#_Toc464807200)

[3 Assumptions 3](#_Toc464807201)

[4 Methodology 4](#_Toc464807202)

[5 Test Plan 5](#_Toc464807203)

[5.1 Security Assessment Team 5](#_Toc464807204)

[5.2 <CSP Name> Provider Testing Points of Contact 5](#_Toc464807205)

[5.3 Testing Performed Using Automated Tools 6](#_Toc464807206)

[5.4 Testing Performed Through Manual Methods 6](#_Toc464807207)

[5.5 Schedule 7](#_Toc464807208)

[6 Rules of Engagement 8](#_Toc464807209)

[6.1 End of Testing 9](#_Toc464807210)

[6.2 Communication of Test Results 9](#_Toc464807211)

[6.3 Limitation of Liability 9](#_Toc464807212)

[6.4 Signatures 11](#_Toc464807213)

[7 Acronyms 12](#_Toc464807214)

[A Appendix A – Test Case Procedures 13](#_Toc464807215)

[B Appendix B – Penetration Testing Plan and Methodology 13](#_Toc464807216)

[C Appendix C – Attachments 13](#_Toc464807217)

List of Tables

[Table 2‑1 Information System Name and Title 2](#_Toc464807218)

[Table 2‑2 Location of Components 2](#_Toc464807219)

[Table 2‑6 Role Based Testing 3](#_Toc464807220)

[Table 5‑1 Security Testing Team 5](#_Toc464807221)

[Table 5‑2 <CSP Name> Service Provider Points of Contact 6](#_Toc464807222)

[Table 5‑3 Tools Used for Security Testing 6](#_Toc464807223)

[Table 5‑4 Testing Performed through Manual Methods 7](#_Toc464807224)

[Table 5‑5 Testing Schedule 7](#_Toc464807225)

[Table 6‑1 Individuals at <CSP Name> Receiving Test Results 9](#_Toc464807226)

# Introduction

Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for <CSP Name>. Testing security controls is an integral part of the FedRAMP security authorization requirements. Providing a plan for security control ensures that the process runs smoothly.

The Information System Name (Information System Abbreviation) will be assessed by an Independent Assessor (IA) <3PAO Name>. The use of an independent assessment team 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.

## Laws, Regulations, Standards, and Guidance

A summary of the FedRAMP Laws and Regulations and the FedRAMP Standards and Guidance is included in the System Security Plan (SSP) Attachment 12 – FedRAMP Laws and Regulations.

SSP Section 12 Laws, Regulations, Standards, and Guidance contains the following two tables that are system specific:

* Table 12 1 Information System Name Laws and Regulations includes additional laws and regulations specific to Information System Name.
* Table 12 2 Information System Name Standards and Guidance includes any additional standards and guidance specific to Information System Name.

## Purpose

Instruction: A goal of the kick-off meeting is to obtain the necessary information to populate this plan. The 3PAO must obtain the requisite information on the CSP system at the kick-off meeting so that this plan can be completed. After this plan has been completed, the 3PAO must meet again with the CSP, present the Draft Security Assessment Plan, and make any necessary changes before finalizing the plan. Both the Draft plan and Final plan must be submitted to the Authorizing Official (AO) for review. Delete this instruction from your final version of this document.

This document consists of a test plan to test the security controls for Information System Abbreviation. It has been completed by <3PAO Name> for the benefit of <CSP Name>. NIST SP 800-39, Managing Information Security Risk states:

The information system owner and common control provider rely on the security expertise and the technical judgment of the assessor to: (i) assess the security controls employed within and inherited by the information system using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the controls and address identified vulnerabilities.

# Scope

## Information System Name/Title

Instruction: Name the system that that is slated for testing and include the geographic location of all components that will be tested. Put in a brief description of the system components that is a direct copy/paste from the description in the System Security Plan. Delete this instruction from your final version of this document.

The Information System Abbreviation.is undergoing testing as described in this Security Assessment Plan named in Table 2-1.

Table 2‑1 Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| <Enter FedRAMP Application Number> | Information System Name | Information System Abbreviation |

The physical locations of all the different components that will be tested are described in Table 2‑2 Location of Components.

Table 2‑2 Location of Components

| Login URL\* Data Center Site Name | Address | Description of Components |
| --- | --- | --- |
| Enter Data Center Site Name | Enter Data Center Address | Description of Components |
| Enter Data Center Site Name | Enter Data Center Address | Description of Components |
| Enter Data Center Site Name | Enter Data Center Address | Description of Components |

\*uniform resource locator (URL)

## Internet Protocol (IP) Addresses, WeB APPLICATIONS, and DATABASES Slated for Testing

Instruction: This section should simply reference the system’s Integrated Inventory Workbook, which should be maintained and updated monthly by the CSP. If additional IP addresses are discovered that were not included in the Integrated Inventory Workbook, advise the CSP to update the Inventory Workbook as well as the boundary information in the SSP and obtain new approval on the SSP from the ISSO before moving forward. If the network is a large network (Class B or larger), test a subset of the IP addresses. If a sampling methodology is to be used, ensure the approach is documented in Section 4 and Appendix C of this SAP. All scans must be fully authenticated. CSPs must ensure that the inventory is current before testing, and that the inventory and components to be tested are in agreement. Instructions for completing the Integrated Inventory Workbook are provided within the Integrated Inventory Workbook, itself.

The Integrated Inventory Workbook, also provided as Attachment 13 of the <*System Name*> System Security Plan, provides the complete listing of system components within the scope of testing for this Security Assessment Plan.

## Roles Slated for Testing

Role testing will be performed to test the authorizations restrictions for each role. <3PAO Name> will access the system while logged in as different user types and attempt to perform restricted functions as unprivileged users. Functions and roles that will be tested are noted in Table 2‑6 Role Based Testing. Roles slated for testing correspond to those roles listed in the Information System Abbreviation SSP.

Table 2‑6 Role Based Testing

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

# Assumptions

Instruction: The assumptions listed are default assumptions. The IA must edit these assumptions as necessary for each unique engagement.

Delete this instruction from your final version of this document.

The following assumptions were used when developing this SAP:

* <CSP Name> resources, including documentation and individuals with knowledge of the <CSP Name> systems and infrastructure and their contact information, will be available to <3PAO Name> staff during the time necessary to complete assessments.
* The <CSP Name> will provide login account information/credentials necessary for <3PAO Name> to use its testing devices to perform authenticated scans of devices and applications.
* The <CSP Name> will permit <3PAO Name> to connect its testing laptops to the <CSP Name> networks defined within the scope of this assessment.
* The <CSP Name> will permit communication from Third Party Assessment Organization testing appliances to an internet hosted vulnerability management service to permit the analysis of vulnerability data.
* Security controls that have been identified as “Not Applicable” in the SSP will be verified as such and further testing will not be performed on these security controls
* 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, <CSP Name> personnel will be available should the <3PAO Name> staff determine that either after hours work, or weekend work, is necessary to support the security assessment.

# Methodology

Instruction: FedRAMP provides a documented methodology to describe the process for testing the security controls. The IAs may edit this section to add additional information.

Delete this instruction from your final version of this document.

<3PAO Name> will perform an assessment of the Information System Abbreviation security controls using the methodology described in NIST SP 800-53A. <3PAO Name> will use FedRAMP test procedures 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 worksheets (provided in Appendix B) along with information that notes whether the control (or control enhancement) is satisfied or not.

<3PAO Name> data gathering activities will consist of the following:

* Request <CSP Name> provide FedRAMP required documentation
* Request any follow-up documentation, files, or information needed that is not provided in FedRAMP required documentation
* Travel to the <CSP Name> sites as necessary to inspect systems and meet with <CSP Name> staff
* Obtain information through the use of security testing tools

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

* Examine: the IA will review, analyze, inspect, or observe one or more assessment artifacts as specified in the attached test cases
* Interview: the IA will conduct discussions with individuals within the organization to facilitate assessor understanding, achieve clarification, or obtain evidence
* Technical Tests: the IA will perform technical tests, including penetration testing, on system components using automated and manual methods

<3PAO Name> Choose response use sampling when performing this assessment.

Instruction: If sampling methodology is used, attach the sampling methodology in Appendix C.

Delete this instruction from your final version of this document.

Penetration testing methodology is attached in Appendix B.

# Test Plan

## Security Assessment Team

Instruction: List the members of the risk assessment team and the role each member will play. Include team members contact information.

Delete this instruction from your final version of this document.

The security assessment team consists of individuals from <3PAO Name> which are located at the following address: <3PAO Name> Enter Address of 3PAO.Information about <3PAO Name> can be found at the following URL: Third Party Assessment Organization Enter 3PAO URL.

Security control assessors play a unique role in testing system security controls. NIST SP 800-39, Managing Information Security Risk states:

*The security control assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system).*

The members of the IA security testing team are found in Table 5‑1 Security Testing Team.

Table 5‑1 Security Testing Team

| Name | Role | Contact Information |
| --- | --- | --- |
| Enter Test Team POC Name | Enter Test Team POC Role | Enter Test Team Contract Information |
| Enter Test Team POC Name | Enter Test Team POC Role | Enter Test Team Contract Information |
| Enter Test Team POC Name | Enter Test Team POC Role | Enter Test Team Contract Information |

## <CSP Name> Provider Testing Points of Contact

Instruction: The IA must obtain at least three points of contact from the CSP to use for testing communications. One of the contacts must be available 24 x 7 and must include an operations center (e.g., NOC, SOC).

Delete this instruction from your final version of this document.

The <CSP Name> points of contact that the testing team will use are found in Table 5‑2 <CSP Name> Service Provider Points of Contact (POCs).

Table 5‑2 <CSP Name> Service Provider Points of Contact

| Name | Role | Contact Information |
| --- | --- | --- |
| Enter CSP POC Name | Enter CSP POC Role | Enter CSP Contact Information |
| Enter CSP POC Name | Enter CSP POC Role | Enter CSP Contact Information |
| Enter CSP POC Name | Enter CSP POC Role | Enter CSP Contact Information |

## Testing Performed Using Automated Tools

Instruction: Describe what tools will be used for testing security controls. Include all product names and names of open source tools and include version numbers. If open source tools are used, name the organization (or individuals) who developed the tools. Additionally, describe the function and purpose of the tool (e.g., file integrity checking, web application scanning). For scanners, indicate what the scanner’s capability is, e.g., database scanning, web application scanning, infrastructure scanning, code scanning/analysis). For more information see the Guide to Understanding FedRAMP.

Delete this instruction from your final version of this document.

<3PAO Name> plans to use the following tools noted in Table 5‑3 Tools Used for Security Testing to perform testing of the Information System Abbreviation.

Table 5‑3 Tools Used for Security Testing

| Tool Name | Vendor/Organization Name & Version | Purpose of Tool |
| --- | --- | --- |
| Enter Tool Name | Enter Vendor and Version | Enter Tool Purpose |
| Enter Tool Name | Enter Vendor and Version | Enter Tool Purpose |
| Enter Tool Name | Enter Vendor and Version | Enter Tool Purpose |
| Enter Tool Name | Enter Vendor and Version | Enter Tool Purpose |

## Testing Performed Through 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 Security Assessment Report (SAR). Examples are listed in the first four rows. Delete the examples, and put in the real tests. Add additional rows as necessary. Identifiers must be in the format MT-1, MT-2 which would indicate “Manual Test 1” and “Manual Test 2” etc.

Example MT-1
Example Forceful Browsing
Example Description: We will login as a customer and try to see if we can gain access to the Network Administrator and Database Administrator privileges and authorizations by navigating to different views and manually forcing the browser to various URLs.
Example MT-2
Example Structured Query Language (SQL) Injection
Example Description: We will perform some manual SQL injection attacks using fake names and 0 OR '1'='1' statements.
Example MT-3 C
Example Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)
Example Description: We will test the CAPTCHA function on the web form manually.
Example MT-4
Example Online Certificate Status Protocol (OCSP)
Example Description: We will manually test to see if OCSP is validating certificates.

Penetration tests must be included in this section.

Delete these instructions from your final version of this document.

Table 5‑4 Testing Performed through Manual Methods describes the technical test that were performed through manual methods without automated tools.

Table 5‑4 Testing Performed through Manual Methods

| Test ID | Test Name | Description |
| --- | --- | --- |
| Test ID | Test Name | Enter Test Description |
| Test ID | Test Name | Enter Test Description |
| Test ID | Test Name | Enter Test Description |

## Schedule

Instruction: Insert the security assessment testing schedule. This schedule must be presented to the CSP by the 3PAO at the kick-off meeting. The ISSO must be invited to the meeting that presents the schedule to the CSP. After being presented to the CSP at the kick-off meeting, the IA must make any necessary updates to the schedule and this document and send an updated version of the CSP, copying the ISSO.

Delete this instruction from your final version of this document.

The security assessment testing schedule can be found in Table 5‑5 Testing Schedule below.

Table 5‑5 Testing Schedule

| Task Name | Start Date | Finish Date |
| --- | --- | --- |
| Kick-off Meeting | Select start date. | Select end date. |
| Develop Draft SAP | Select start date. | Select end date. |
| Meeting to Review SAP | Select start date. | Select end date. |
| Finalize SAP | Select start date. | Select end date. |
| Review <CSP Name> Documentation | Select start date. | Select end date. |
| Conduct Interviews of <CSP Name> Staff | Select start date. | Select end date. |
| Perform Testing | Select start date. | Select end date. |
| Develop Risk Exposure Table  | Select start date. | Select end date. |
| Develop Draft SAR | Select start date. | Select end date. |
| Draft SAR Delivered to CSP | Select start date. | Select end date. |
| Issue Resolution Meeting | Select start date. | Select end date. |
| Finalize SAR | Select start date. | Select end date. |
| Send Final Version of SAR <CSP Name> Provider and ISSO | Select start date. | Select end date. |

# Rules of Engagement

Instruction: FedRAMP provides a Rules of Engagement template. The IAs must edit this RoE as necessary. The final version of the RoE must be signed by both the IA and CSP.

Delete this instruction from your final version of this document.

A Rules of Engagement (RoE) document is designed to describe proper notifications and disclosures between the owner of a tested systems and an independent assessor. 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

Instruction: Edit and modify the disclosures as necessary. If testing is to be conducted from an internal location, identify at least one network port with access to all subnets/segments to be tested. The purpose of identifying the IP addresses from where the security testing will be performed is so that when the IAs are performing scans, the CSP will understand that the rapid and high volume network traffic is not an attack and is part of the testing.

Delete this instruction from your final version of this document.

Any testing will be performed according to terms and conditions designed to minimize risk exposure that could occur during security testing. All scans will originate from the following IP address(es): List IP addresses for Scan Test.

Security Testing May Include

Instruction: The IA must edit the bullets in this default list to make it consistent with each unique system tested.

Delete this instruction from your final version of this document.

Security testing may include the following activities:

* 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/password
* Attempted structured query language (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

Security Testing Will Not Include

Instruction: The 3PAO must edit the bullets in this default list to make it consistent with each unique system tested.

Delete this instruction from your final version of this document.

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 <CSP Name> 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 (viruses, Trojans, worms, etc.)

## End of Testing

<3PAO Name> will notify <End Testing POC> at <CSP Name> when security testing has been completed.

## Communication of Test Results

Email and reports on all security testing will be encrypted according to <CSP Name> requirements. Security testing results will be sent and disclosed to the individuals at <CSP Name> noted in Table 6‑1 Individuals at <CSP Name> Receiving Test Results within <Enter number of days> days after security testing has been completed.

Table 6‑1 Individuals at <CSP Name> Receiving Test Results

| Name | Role | Contact Information |
| --- | --- | --- |
| Enter CSP Name | Enter CSP Role | Enter CSP Contact Information |
| Enter CSP Name | Enter CSP Role | Enter CSP Contact Information |
| Enter CSP Name | Enter CSP Role | Enter CSP Contact Information |

## 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 instruction from your final version of this document.

<3PAO Name>, and its stated partners, shall not be held liable to <CSP Name> 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.

<CSP Name> 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 the IA and <CSP Name> have been identified as having the authority to agree to security testing of Information System Abbreviation.

|  |
| --- |
| ACCEPTANCE AND SIGNATURE |
|  | I have read the above Security Assessment Plan and Rules of Engagement and I acknowledge and agree to the tests and terms set forth in the plan. |  |
|  |
| <3PAO Name> Representative: | Enter 3PAO Representative Name. | (printed) |  |  |
| <3PAO Name> Representative: |  | (signature) | Click here to enter a date. | (date) |
|  |
| <CSP Name> Representative: | Enter CSP Representative Name | (printed) |  |  |
| <CSP Name> Representative: |  | (signature) | Click here to enter a date. | (date) |
|  |  |  |

# Acronyms

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website [Documents](https://www.fedramp.gov/resources/documents-2016/) page under Program Overview Documents.

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.

# Appendix A – Test Case Procedures

Results of the security test case procedures shall be recorded directly in each respective workbook. The workbook must be attached.

# Appendix B – Penetration Testing Plan and Methodology

Instruction: CSPs must attach a file containing the plan or include the plan in this Appendix.

Delete this instruction from your final version of this document.

# Appendix C – Attachments

Instruction: If applicable, attachments must include penetration testing rules of engagement, penetration testing methodology, and the sampling methodology used in testing.

Delete this instruction from your final version of this document.

List of Attachments: