

template

StateRAMP Security assessment plan

(SR-sap)

[3PAO Name]

for

[Service Provider Name]

[Information System Name]

**Version:**

X.X

**Date:**

YYYYMMDD

TABLE OF CONTENTS

[1. Introduction 6](#_Toc96593357)

[1.1 Laws, Regulations, Standards, and Guidance 6](#_Toc96593358)

[1.2 PURPOSE 6](#_Toc96593359)

[2. scope 6](#_Toc96593360)

[2.1 INFORMATION system name/title 6](#_Toc96593361)

[2.2 IP Addresses, Web Applications, and Databases Slated for Testing 7](#_Toc96593362)

[2.3 Roles Slated for Testing 7](#_Toc96593363)

[3. Assumptions 9](#_Toc96593364)

[4. methodology 9](#_Toc96593365)

[5. Test plan 10](#_Toc96593366)

[6. RULES OF ENGAGEMENT 10](#_Toc96593367)

List of Tables

[Table 2‑1 Information System Name and Title 6](#_Toc96427976)

[Table 2‑2 Location of Components 6](#_Toc96427977)

[Table 3‑1. System Information 9](#_Toc96427978)

[Table 3‑2. Leveraged StateRAMP Authorizations 10](#_Toc96427979)

[Table 3‑3. External Systems and Services 12](#_Toc96427980)

[Table 3‑4. APIs 13](#_Toc96427981)

[Table 4‑2. Cryptographic Modules 17](#_Toc96427982)

[Table 4‑3. Transport Layer Security 17](#_Toc96427983)

[Table 4‑4. Identification, Authentication, and Access Control 18](#_Toc96427984)

[Table 4‑5. Audit, Alerting, Malware, and Incident Response 19](#_Toc96427985)

[Table 4‑6. Contingency Planning and Disaster Recovery 20](#_Toc96427986)

[Table 4‑7. Configuration and Risk Management 21](#_Toc96427987)

[Table 4‑8. Data Center Security 23](#_Toc96427988)

[Table 4‑9. Policies, Procedures, and Documentation 23](#_Toc96427989)

[Table 4‑10. Missing Policy and Procedure Elements 25](#_Toc96427990)

[Table 4‑11. Security Awareness Training 25](#_Toc96427991)

[Table 4‑12. Staffing Levels 25](#_Toc96427992)

[Table 4‑13. Change Management 26](#_Toc96427993)

[Table 4‑14. Vendor Dependencies and Agreements 26](#_Toc96427994)

[Table 4‑15. Vendor Dependency Details 26](#_Toc96427995)

[Table 4‑16. Formal Agreements Details 27](#_Toc96427996)

[Table 4‑17. Continuous Monitoring Capabilities 27](#_Toc96427997)

[Table 4‑18. Continuous Monitoring Capabilities– Additional Details 27](#_Toc96427998)

[Table 4‑19. Maturity of the System Security Plan 28](#_Toc96427999)

[Table 4‑20. Controls Designated “Not Applicable” 28](#_Toc96428000)

[Table 4‑21. Controls with an Alternative Implementation 28](#_Toc96428001)

Security Assessment Plan

Prepared by

| Identification of Organization that Prepared this Document |
| --- |
| Shape  Description automatically generated with low confidence | 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 |
| --- |
| Shape  Description automatically generated with low confidence | 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 |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

Revision History

| Date | Description | Version of SAP | Author |
| --- | --- | --- | --- |
| 03/03/2022 | Initial Draft | 1.0 | StateRAMP PMO |
|  |  |  |  |

How to contact us

For questions about StateRAMP, how to become a member, or how to list your product on the Authorized Vendor List, contact info@stateramp.org. For technical questions about this document including how to use it, contact pmo@stateramp.org.

For more information about StateRAMP, see [www.stateramp.org](http://www.stateramp.org)

# Introduction

StateRAMP represents the shared interests of state and local governments, education institutions, state and local agencies, other public institutions, and service providers (SP) with IaaS, SaaS, and PaaS solutions. Testing security controls is an integral part of the StateRAMP security authorization requirements. Providing a plan for security control helps the process go more smoothly.

The **<Information System Name>** (**<Information System Abbreviation>**) will be assessed by an independent assessor, **<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.

## Laws, Regulations, Standards, and Guidance

A summary of the StateRAMP Laws and Regulations and the StateRAMP Standards and Guidance is included in the StateRAMP-Controls-Matrix, Section 5, Laws and Regulations.

## PURPOSE

Instructions: The 3PAO must obtain the required information on the SP 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 SP, present the draft Security Assessment Plan, and make any necessary changes before finalizing the plan. The finalized plan must be provided to the StateRAMP PMO.

Delete these instructions from the final version of this document.

This document consists of a test plan for testing the security controls for **<Information System Abbreviation>**. It has been completed by **<3PAO Name>** for the benefit of **<SP name>**.

# scope

This SAP must specifically address all the security controls required for the impact level of **<Impact Level>** for **<Information System Abbreviation>**. Tests on systems and interfaces that are outside the boundary of the SP’s service offering are not included in this plan.

In the space below, provide a one-paragraph description of the system that includes all the information provided in Table 2-1, System Information.

## INFORMATION system name/title

Instructions: Name the system that that is slated for testing and state the geographic location of all components that will be tested (if applicable). Include a brief description of the system components that is a direct copy/paste from the description in the StateRAMP System Security Plan (SR-SSP). Contact info@stateramp.org if you need help determining your StateRAMP ID. Delete these instructions from your final version of this document.

Table ‑ Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| **<Enter StateRAMP ID>** | **<Information System Name>** | **<Information System Abbreviation>** |

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

Table ‑ Physical Location of Components

| Data Center Site Name | Address | Description of Components |
| --- | --- | --- |
| **<Data Center Site Name>** | **<Data Center Address>** | **<Description of Components>** |
| **<Data Center Site Name>** | **<Data Center Address>** | **<Description of Components>** |
| **<Data Center Site Name>** | **<Data Center Address>** | **<Description of Components>** |

## IP Addresses, Web Applications, and Databases Slated for Testing

Instructions: This section should reference the system’s Inventory Workbook, which should be maintained and updated monthly by the SP. If additional IP addresses are discovered that were not included in the Integrated Inventory Workbook, the 3PAO should advise the SP to update the Inventory Workbook, as well as the boundary information in the SSP. If the network is a Class B or C, 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 B of this SAP. All scans must be fully authenticated. SPs must ensure that the inventory is current before testing, and that the inventory and components to be tested match. Instructions for completing the StateRAMP Inventory Workbook are provided within the StateRAMP Inventory Workbook itself.

The StateRAMP Inventory Workbook, provided as Attachment B of this document, 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 authorization controls for each system 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 2-3: Role-Based Testing. Roles slated for testing correspond to those roles listed in the **<Information System Abbreviation>** SR-SSP.

Table ‑3 Role-Based Testing

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

# Assumptions

Instructions: This section is where the 3PAO lists assumptions as necessary for each unique engagement. Examples of assumptions include the following:

 - Dependencies on resources (documentation, personnel with requisite knowledge required to complete testing, etc.)

 - Appropriate login account info and credentials

 - Access to HW, systems and networks

 - Identifying the process of how to test controls marked as "N/A"

 - Situational testing of significant upgrades or changes to the infrastructure and/or components of the system

The assumptions included below are statements referring to the examples above and should be altered by the assessor(s).

Delete these instructions from the final version of this document.

The following assumptions were used when developing this SAP:

* **<SP name>** resources, including documentation and individuals with knowledge of the **<SP name>** systems and infrastructure and their contact information, will be available to **<3PAO name>** staff during the time necessary to complete assessments.
* **<SP name>** will provide login account information and credentials necessary for **<3PAO name>** to perform authenticated scans of devices and applications.
* **<SP name>** will permit **<3PAO name>** to connect testing equipment to **<SP name>** networks defined within the scope of this assessment.
* **<SP name>** will permit communication from 3PAO testing equipment 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 SR-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, **<SP name>** personnel will be available should the **<3PAO name>** staff determine that after-hours work or weekend work is necessary to support the security assessment.

# methodology

Instructions: StateRAMP provides a documented methodology to describe the process for testing the security controls as outlined in the StateRAMP Test Case Workbooks. The 3PAO may edit this section to add additional information.

Delete these instructions from the 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 StateRAMP 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 along with information that notes whether the control (or control enhancement) is satisfied or not. The completed test case workbook will be included in the SAR submission.

**<3PAO name>** data-gathering activities will consist of the following:

* Request <SP name> provide StateRAMP-required documentation
* Request any follow-up documentation, files, or information needed that is not provided in StateRAMP required documentation
* Travel to <SP name> sites as necessary to inspect systems and meet with <SP name> staff
* Obtain information using security testing tools

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

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

**<3PAO name>** **<will/will not>** use sampling when performing this assessment.

Instruction: If sampling methodology is used, submit the sampling methodology as part of Appendix B.

Delete this instruction from your final version of this document.

# 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> <3PAO Address>.** Information about **<3PAO name>** can be found at the following URL: **<3PAO URL>.**

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

Table - Security Testing Team

| Name | Role | Contact Information |
| --- | --- | --- |
| **<Test Team POC Name>** | **<Test Team POC’s Role>** | **<Test Team POC’s Contact Info>** |
| **<Test Team POC Name>** | **<Test Team POC’s Role>** | **<Test Team POC’s Contact Info>** |
| **<Test Team POC Name>** | **<Test Team POC’s Role>** | **<Test Team POC’s Contact Info>** |

## <SP NAME> Testing Points of Contact

Instruction: The assessment team must obtain a primary and alternate point of contact from the SP to use for testing communications. One of the contacts must be available 24 x 7.

Delete this instruction from your final version of this document.

The **<SP Name>** points of contact that the testing team will use are found in Table 5-2: **<SP Name>** Points of Contact.

Table - **<SP Name>** Service Provider Points of Contact

| Name | Role | Contact Information |
| --- | --- | --- |
| **<SP POC Name>** | **<SP POC Role>** | **<SP POC Contact Info>** |
| **<SP POC Name>** | **<SP POC Role>** | **<SP POC Contact Info>** |
| **<SP POC Name>** | **<SP POC Role>** | **<SP POC Contact Info>** |

##

## 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).

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 - Tools Used for Security Testing

| Tool Name | Vendor/Organization Name & Version | Purpose of Tool |
| --- | --- | --- |
| **<Tool Name>** | **<Vender Name & Tool Version>** | **<Tool Purpose>** |
| **<Tool Name>** | **<Vender Name & Tool Version>** | **<Tool Purpose>** |
| **<Tool Name>** | **<Vender Name & Tool Version>** | **<Tool Purpose>** |
| **<Tool Name>** | **<Vender Name & Tool Version>** | **<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 log in as a customer and try to see if we can gain access to the Network Administrator and Database Administrator roles’ privileges and authorizations by navigating to different views and manually forcing the browser to various URLs.
Example MT-2
Example SQL Injection
Example Description: We will perform some manual SQL injection attacks using fake names and 0 OR '1'='1' statements.
Example MT-3
Example Spear Phishing
Example Description: We will conduct an unannounced spear phishing exercise against system administrators.

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 - Testing Performed through Manual Methods

| Test ID | Test Name | Description |
| --- | --- | --- |
| **<Test ID>** | **<Test Name>** | **<Test Description>** |
| **<Test ID>** | **<Test Name>** | **<Test Description>** |
| **<Test ID>** | **<Test Name>** | **<Test Description>** |

## Schedule

Instructions: Insert the security assessment testing schedule. This schedule must be presented to the SP by the 3PAO at the kick-off meeting. After being presented to the SP at the kick-off meeting, the 3PAO must make any necessary updates to the schedule and this document and send an updated version to the SP.

Delete these instructions from the final version of this document.

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

Table - Testing Schedule

| Task Name | Start Date | Finish Date |
| --- | --- | --- |
| Kick-off Meeting | **<Start Date>** | **<End Date>** |
| Develop Draft SAP | **<Start Date>** | **<End Date>** |
| Meeting to Review SAP | **<Start Date>** | **<End Date>** |
| Finalize SAP | **<Start Date>** | **<End Date>** |
| Review **<Service Provider Name>** Documentation | **<Start Date>** | **<End Date>** |
| Conduct Interviews of **<Service Provider Name>** Staff | **<Start Date>** | **<End Date>** |
| Perform Testing | **<Start Date>** | **<End Date>** |
| Develop Risk Exposure Table  | **<Start Date>** | **<End Date>** |
| Develop Draft SAR | **<Start Date>** | **<End Date>** |
| Draft SAR Delivered to SP | **<Start Date>** | **<End Date>** |
| Issue Resolution Meeting | **<Start Date>** | **<End Date>** |
| Finalize SAR | **<Start Date>** | **<End Date>** |
| Send Final Version of SAR to **<Service Provider Name>** and StateRAMP PMO | **<Start Date>** | **<End Date>** |

# RULES OF ENGAGEMENT

Instruction: Below is a Rules of Engagement (RoE) template. The 3PAO must edit this RoE as necessary. The final version of the RoE must be signed by both the 3PAO and SP.

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. An 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

Instructions: 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 assessors are performing scans, the SP will understand that the rapid and high-volume network traffic is not an attack and is part of the testing.

Delete these instructions 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>**

Security Testing May 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 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 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 **<SP 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 **<SP Contact>** at **<SP Name>** when security testing has been completed.

## Communication of Test Results

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

Table - Individuals at **<SP Name>** Receiving Test Results

| Name | Role | Contact Information |
| --- | --- | --- |
| **<Name of individual>** | **<Role of Individual>** | **<Contact Info of Individual>** |
| **<Name of individual>** | **<Role of Individual>** | **<Contact Info of Individual>** |
| **<Name of individual>** | **<Role of Individual>** | **<Contact Info of Individual>** |

## 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 **<SP 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.

**<SP 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 **<3PAO Name>** and **<SP 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: | **<Representative’s Name>** | (printed) |  |  |
| **<3PAO Name>** Representative: |  | (signature) | **<Date>** | (date) |
|  |
| **<SP Name>** Representative: | **<Representative’s Name>** | (printed) |  |  |
| **<SP Name>** Representative: |  | (signature) | **<Date>** | (date) |
|  |  |  |

Appendix A – Security Test Case Procedures Template

Results shall be recorded in the StateRAMP Security Test Case Procedures Template. Submit the applicable StateRAMP Test Case Procedures Template as a separate Excel file. Do not embed the document.

Name of file: **<File Name>**

Appendix B – Attachments

Note the attachments to the SAP. Do not embed any documents.

* IP Addresses Slated for Testing – Name of file: **<File name>**
* Web Applications Slated for Testing – Name of file: **<File name>**
* Databases Slated for Testing – Name of file: **<File name>**
* Sampling Methodology – Name of file: **<File name>**