GETTING STARTED WITH STATERAMP

A Guide for Service Providers Pursuing StateRAMP Authorization

VERSION:
1.2
DATE:
October 2021

TABLE OF CONTENTS

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
December 2020	Initial Draft	1.0	StateRAMP Staff
April 2021	Updates to membership information	1.1	StateRAMP Staff
October 2021	Updated security categories	1.2	StateRAMP Staff
January 2022	Revamped verification status for continuous monitoring to align with Continuous Monitoring Guide.	1.3	StateRAMP PMO
December 2022	Added StateRAMP Security Snapshot and Authorization requirements	1.4	StateRAMP Staff

1. WHAT IS STATERAMP

StateRAMP brings State and local governments together to develop standards for cloud security, educate on best practices, and recognize a common method for verifying the cloud security of service providers who use or offer cloud solutions that process, store, and/or transmit government data including personally identifiable information (PII), personal health information (PHI), and payment card industry (PCI) information. StateRAMP is organized under the Indiana Nonprofit Corporations Act as a domestic nonprofit organization.

StateRAMP's purpose is (1) to help State and local governments protect citizen data; (2) save taxpayer and service provider dollars with a "verify once, serve many" model; (3) to lessen the burdens on government; and (4) promote education and best practices in cybersecurity among those it serves in industry and the government communities. StateRAMP's security verification model is based on the National Institute of Standards and Technology (NIST) publication 800-53—the same publication the Federal Government used to develop FedRAMP, a similar cybersecurity program for federal entities.

While the NIST 800-53 standards and requirements have been adopted outright as the security framework for several state governments, StateRAMP has partnered with government officials, industry experts, and cybersecurity professionals to develop a widely acceptable set of standards, controls, policies, and procedures which specifically meet the cybersecurity needs of state and local governments.

StateRAMP is here to serve governments by providing a simplified and standardized approach for validating the cybersecurity of the service providers who offer IaaS, PaaS, or SaaS solutions that may process, transmit, and/or store any government data including PII, PCI, and PHI. When partnering with StateRAMP, governments receive education, consultation, and ongoing support through all phases of the implementation, contract award, and continuous monitoring phases of the procurement cycle. Participating governments have access to StateRAMP's secure repository to view service provider security packages, security statuses, and monthly and annual reporting tailored to the government's specific cybersecurity needs.

2. GETTING STARTED

To get started, review the Implementation Checklist provided in the Appendix, or download a copy from the StateRAMP website. Partnering with the StateRAMP Project Management Office (PMO) and completing the milestones outlined in the Implementation Checklist is the quickest way for governments to verify cloud security of their vendors. This Getting Started Guide is intended to provide further details and best practice recommendations for completing each item in the Implementation Checklist.

For questions about how to adopt StateRAMP's best practices or to speak with a member of the StateRAMP PMO, please email pmo@stateramp.org.

3. COMPLETING THE IMPLEMENTATION CHECKLIST

Use the following sections to complete all tasks and milestones included in the StateRAMP Implementation Checklist.

3.1 COMMUNICATING WITH STATERAMP

If you need to contact StateRAMP for any reason, please use the information listed below and a member of the StateRAMP team will respond to your inquiry within 1-2 business days.

StateRAMP Office Hours:
Monday-Friday 8:00 a.m. to 5:00 p.m. EST

Contact Information:
info@stateramp.org

3.2 BECOME A STATERAMP MEMBER

Service providers must become a StateRAMP member before their IaaS, PaaS, or SaaS solutions can be validated by the PMO, obtain a StateRAMP Security Status, or be listed on the Authorized Product List (APL). Service provider membership is granted at the organizational level and there is no limit to the number of products an organization can validate and list on the APL.

The membership application is located on the StateRAMP website and once the provider has completed the membership process, the organization and organization's primary point of contact will be added to the StateRAMP Member Directory. If the organization has already engaged a third-party assessment organization (3PAO) and indicated such on the membership application, the organization will be listed as In Process on the APL during the daily afternoon update.

3.3 OPTIONAL: COMPLETE A STATERAMP SECURITY SNAPSHOT

As a first step toward achieving a verified StateRAMP Security Status, service providers have the option to complete a StateRAMP Security Snapshot. The snapshot serves as a "pre-Ready" measurement and the criteria are designed to provide a gap analysis to validate a product's current maturity in relation to meeting the Minimum Mandatory Requirements for StateRAMP Ready. StateRAMP Security Snapshot reviews will take around three weeks to complete. A letter is provided with the StateRAMP Security Snapshot Score. Scores are not posted on the Authorized Product List.

3.4 DETERMINE APPROPRIATE SECURITY CATEGORY

Before engaging a 3PAO and submitting any documentation to the StateRAMP PMO for review, the provider must determine the appropriate security category required by the state or local government or by using the Data Classification Tool. There are three StateRAMP security categories: Low, Low +, Moderate, and High. Each category represents a different set of data characteristics and corresponding security requirements ranging from non-private, generally accessible information to protected, personally identifiable information (PII) or classified data. It is important for providers to identify the security standards required for the security category at which they will be assessed.

If the provider is obtaining a StateRAMP Security Status in preparation for or in response to a State or local government RFP, sponsorship, or current contract, the provider should identify the StateRAMP security category required by the government. If the provider is seeking a StateRAMP Security Status independent of a state or local government RFP, sponsorship, or current contract, the provider should use the Data Classification Tool to determine the appropriate security category for the data being processed, stored, and/or transmitted by the provider's IaaS, PaaS, or SaaS solution.

3.5 SELECT A 3PAO TO CONDUCT AN AUTHORIZATION REVIEW

The provider should review the list of StateRAMP-approved 3PAOs on the StateRAMP website and engage with the 3PAO of their choice to complete the full security assessment required for an

Authorization Review. Once a 3PAO has been engaged, the provider must notify the StateRAMP PMO of the engagement so they can update the provider's StateRAMP security status to In Process.

3.6 COMPLETE AUTHORIZATION REVIEW DOCUMENTATION

Once the provider has engaged with a 3PAO to conduct their StateRAMP Authorization Review, the provider must complete a StateRAMP System Security Plan (SR-SSP) if not already submitted, the StateRAMP Security Controls Matrix (SR-SCM), the Plan of Action and Milestones (POA&M), and any other documentation required by the 3PAO so the 3PAO can complete a StateRAMP Security Assessment Plan (SR-SAP) and a Security Assessment Report (SR-SAR) to be submitted to the StateRAMP PMO.

3.7 SUBMIT A SECURITY REVIEW REQUEST FORM

Before the 3PAO can submit the provider's completed documentation and assessment report, the provider must complete the Security Review Request Form and pay the Authorization Review fee. Only providers who are already a StateRAMP member can submit a Security Review Request. Additionally, the PMO only accepts security assessments and documentation submitted by StateRAMP-approved 3PAOs.

3.8 STATERAMP APPROVALS COMMITTEE OR GOVERNMENT SPONSOR

If a provider is pursuing StateRAMP Authorization, they must have an authorizing official approve their security package. Providers can choose to secure a government sponsor on their own or leverage the StateRAMP Approvals Committee. The StateRAMP Approvals Committee, comprised of five government representatives, can serve as their appointed sponsor, and confirm the security package meets StateRAMP requirements.

Eligible government sponsors include any government official or designee, who represents State, local, tribal, or territorial government or public education institutions.

3.9 OBTAIN A STATERAMP AUTHORIZED STATUS

If the 3PAO attested that the provider meets all required security controls, the StateRAMP PMO verified the findings, the state or local government accepted the provider's security package, and all outstanding issues and/or inquiries have been resolved, the provider's security status on the StateRAMP APL will be changed to Authorized.

A Provisional status may be assigned by a sponsoring government if the provider has submitted a security package for Authorization consideration, but is found to meet most, but not all, security requirements. Providers with a Provisional status comply with continuous monitoring requirements and an additional assessment may be required to obtain Authorization.

3.10 BEGIN CONTINUOUS MONITORING ACTIVITIES

Once the provider has obtained an Authorized or Provisional status, the provider must begin submitting the required documentation for monthly continuous monitoring reporting to maintain their StateRAMP Security Status as detailed in the *StateRAMP Continuous Monitoring Guide*. The annual continuous monitoring fee can be paid upfront in full or by monthly installments at the beginning of each month.

4. GLOSSARY

TERM	DEFINITION
Continuous monitoring	Activities conducted by the CSP on a monthly, annual, and ad hoc basis to be provided to the State to ensure ongoing data protection and security standard compliance.
SP	A Service Provider is any organization who offers or uses IaaS, PaaS, or SaaS solutions that may process, transmit, and/or store any government data including PII, PCI, and PHI.
IaaS	Infrastructure as a Service
NIST 800-53	The National Institute of Standards and Technology Special Publication 800-53 Revision 4 provides the official requirements of security and privacy controls for information systems handling government information and is the adopted security baseline for StateRAMP and FedRAMP.
PaaS	Platform as a Service
PCI	Payment Card Industry (Data Security Standard)
PHI	Protected Health Information
PII	Personally Identifiable Information
PMO	Project Management Office
SaaS	Software as a Service
Security Category	The Security Category is the category or level of security compliance an SP must achieve in order to meet State security requirements.
Security Status	The Security Status indicates where the SP is in the StateRAMP process. Security Statuses include Ready, In Process, Provisional, and Authorized.
3PAO	Third Party Assessment Organization

5. APPENDIX

5.1 STATERAMP IMPLEMENTATION CHECKLIST

- □ **Become a StateRAMP member**
    - □ The provider must complete the StateRAMP membership application and pay the membership fee.
    - □ Once the payment is processed, the organization and the organization's primary point of contact will be listed on the StateRAMP Member Directory.
    - □ If the provider has already engaged a 3PAO to assess one or more of the organization's IaaS, PaaS, or SaaS solutions at the time of application submission, the eligible product will be published on the StateRAMP Progressing Product List during the next list update.
- □ **Complete an optional StateRAMP Security Snapshot.**
    - □ If the service provider prefers to see where their security posture currently stands in relation to meeting the Minimum Mandatory Requirements for Ready, they can complete a StateRAMP Security Snapshot.
    - □ Submit a Security Snapshot Request Form, and the PMO will provide you with a risk score within three weeks.
- □ **Determine an appropriate StateRAMP Impact Level**
    - □ If the provider is obtaining a StateRAMP security status independent of a State or local government RFP, sponsorship, or current contract, the provider should use the Data Classification Tool to determine the appropriate impact level for the data being processed, stored, and/or transmitted by the provider's IaaS, PaaS, or SaaS solution.
    - □ If the provider is obtaining a StateRAMP security status in preparation for or in response to a State or local government RFP, sponsorship, or current contract, the provider should identify the StateRAMP impact level required by the government.
    - □ The provider may contact the StateRAMP PMO for a free, one-time consulting session to learn more about impact levels and determine with level is appropriate for the provider's solution.
- □ **Select a Third-Party Assessment Organization (3PAO) for an Assessment**
    - □ If the provider has received an intent to award, contract award, or sponsorship from a State or local government, the provider should review the list of StateRAMP-approved 3PAOs on the StateRAMP website and engage with the 3PAO of their choice to complete the full security assessment required for an Authorization Review.
    - □ Once a 3PAO has been engaged, the provider must notify the StateRAMP PMO of the engagement and the intent to award, contract award, or government sponsorship in the StateRAMP portal to update the provider's StateRAMP security status to In Process.
- □ **Complete the required documentation for an Authorization Review**
    - □ The provider must complete the StateRAMP System Security Plan (SR-SSP), StateRAMP Security Controls Template (SR-SCT), and a Plan of Action and Milestones (POA&M).
    - □ The provider must complete all documentation required by the 3PAO so the 3PAO can complete the StateRAMP Security Assessment Plan (SR-SAP) and the StateRAMP Security Assessment Report (SR-SAR).

☐ **Submit a Security Review Request Form**

- ☐ The provider must complete the Security Review Request Form and submit the Authorization Review fee before the 3PAO is allowed to submit the provider's completed documentation and assessment report.
- ☐ The PMO only accepts security assessments and documentation submitted by StateRAMP-approved 3PAOs and all documentation must be in the appropriate StateRAMP templates.

☐ **Decide whether to leverage the StateRAMP Approvals Committee or secure a government sponsor.**

- ☐ Providers can choose to select a government sponsor on their own or leverage the Approvals Committee.
- ☐ To leverage the Approvals Committee, providers will need to select the option on the Security Review Request form. Once their package has been reviewed by the PMO, the package will be sent to the Approvals Committee for final approval.
- ☐ Providers can also select a government sponsor on their own. Eligible government sponsors include any government official or designee, who represents state, local, tribal, or territorial government or public education institutions.

☐ **Receive a StateRAMP Authorized or Provisional status**

- ☐ If the 3PAO attested that the provider meets all required security controls, the StateRAMP PMO verified the findings, the State or local government accepted the provider's security package, and all outstanding issues and/or inquiries have been resolved, the provider's security status on the StateRAMP APL will be changed to Authorized.
- ☐ A Provisional status may be assigned by a sponsoring government if the provider has submitted a security package for Authorization consideration, but is found to meet most, but not all, security requirements. Providers with a Provisional status comply with continuous monitoring requirements and an additional assessment may be required to obtain Authorization.

☐ **Begin continuous monitoring activities**

- ☐ Once the provider has obtained an Authorized status, the provider must begin providing the required documentation for monthly continuous monitoring reporting to maintain their StateRAMP security status as detailed in the StateRAMP Continuous Monitoring Guide.
- ☐ The annual continuous monitoring fee can be paid upfront in full or by monthly installments at the beginning of each month.