STATERAMP SECURITY ASSESSMENT FRAMEWORK

VERSION:
3.0

DATE:
August 2024

Contents

DOCUMENT REVISION HISTORY

Date	Description	Version	Governance Body
9/24/2020	Original Publication	1.0	StateRAMP Steering Committee
12/17/2020	Amended with Updated Security Status Definitions	1.1	StateRAMP Steering Committee
01/08/2021	Updated definitions and language	1.2	StateRAMP Board of Directors
5/7/2021	Updated process descriptions	1.3	StateRAMP Board of Directors
4/29/2022	Updated	1.4	StateRAMP Standards and Technical Committee and Board
11/29/2023	Update framework to include StateRAMP Security Snapshot Program and other definitions, according to Rev. 5 updates and process descriptions	2.0	StateRAMP Standards & Technical Committee
11/30/2023	Adopted	2.0	StateRAMP Board of Directors
8/30/2024	Updated Provisional Status to Provisionally Authorized Status.	3.0	StateRAMP Board of Directors
11/11/2024	Updated Fee Schedule Section to reflect Board approved fees.	3.1	StateRAMP Staff

EXECUTIVE SUMMARY

This document describes a general Security Assessment Framework (SAF) for StateRAMP. The purpose of this document is to outline StateRAMP's key internal and external stakeholders; identify the security framework used for security assessments in StateRAMP; and outline the assessment process. This comprehensive security assessment framework document helps to provide a full-scale overview of StateRAMP for both public sector organizations and service providers alike.

StateRAMP Background

In April 2020, a steering committee of government and industry leaders chartered StateRAMP to bring public and private sector leaders together and create a common method to verify security through development of a streamlined approach to risk and authorization management (or RAMP). As a result of the steering committee's work, StateRAMP was formed as a partnership with state government Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Chief Privacy Officers, and Procurement Officials and private industries experts who serve state governments. StateRAMP operates as a 501(c)6 nonprofit.

StateRAMP's design was developed in line with RAMP best practices, namely:

- Third-party assessment and audit of the security posture of products
- Continuous monitoring of product vulnerabilities and patching, as well as any changes to an organization that may drive additional risk
- Annual reauthorization to ensure that the product is maintaining the necessary level of security required

As such, StateRAMP therefore works to help educate the public sector on the need for a comprehensive and streamlined risk and authorization management program and to also provide a service as a RAMP program that is easy to implement.

> *The StateRAMP mission is to support the public sector in defense against cyber threats through adoption of the most comprehensive, streamlined, and accessible cybersecurity assessment framework; and to support service providers in reducing burdens to cybersecurity compliance and improved cybersecurity posture.*
>
> *StateRAMP's vision is to see widespread adoption of the most robust and streamlined risk and authorization management programs across our public sector in the U.S. as part of the national strategy to better protect our country from cyber threats foreign and domestic.*

Like FedRAMP, a federal government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services, StateRAMP aims to promote cybersecurity standards, policies, and best practice so that public sector and critical infrastructure organizations, including private K-12 and higher education institutions, can validate the security of their third-party IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and/or SaaS (Software as a Service) solutions which process, transmit, store the organization's data or which could impact data security.

StateRAMP's security verification model is based on NIST 800-53 Rev. 5 published by the National Institute of Standards and Technology (NIST), which also serves as the framework for FedRAMP requirements. Additionally, NIST 800-53 Rev. 5 has been adopted as the security framework for several state and local governments. Many government officials, industry experts, and working groups participated in adopting standards for controls, policies, and procedures for StateRAMP. These documents and requirements, along with any future proposed amendments, are published on the StateRAMP website at www.stateramp.org.

1. STATERAMP OVERVIEW

1.1 KEY STAKEHOLDERS

StateRAMP exists to support both the public sector and service providers in tackling effective cyber risk management. Therefore, key stakeholders in the StateRAMP ecosystem include, but are not limited to:

Public Sector:

- State government
- Local government
- K-12 institutions
- Public higher education institutions
- Special districts
- Emergency Medical Services
- Critical infrastructure
- Non-profit & non-government organizations

In 2023, the Board adopted private K-12 and higher education institutions be included as a public sector stakeholder.

Private industry:

- Cloud service providers (CSPs) – Software as a Service (SaaS); Platform as a Service (PaaS); Infrastructure as a Service (IaaS); Security as a Service
- Third-Party Assessment Organizations (3PAOs)
- Resellers (aka VARs (Value Added Re), Channel Partners)
- Managed Service Providers (MSPs)
- Cybersecurity compliance consultants

Additionally, StateRAMP continues to work with federal agencies and federal and state elected officials to collaborate and advocate for better third-party risk management policies and standards.

1.2 GOVERNANCE

StateRAMP has developed a governance structure that reflects the public-private partnership necessary to address the challenges inherent to developing and maintaining an effective risk and authorization management program (RAMP) on the public sector side, and for achieving and maintaining robust compliance on the service provider side.

The StateRAMP By-Laws are available at www.stateramp.org.

BOARD OF DIRECTORS

StateRAMP is governed by a Board of Directors with a majority representation from government officials, and minor representation from private industry and subject matter experts. Board Members serve two-year terms and are nominated for service in the following categories of membership:

- **Government Members** are individuals working within a state or local government and are recommended by the Nominating Committee, per StateRAMP By-Laws. Government Members may include chief procurement officers, procurement officers, chief privacy officers, compliance officers, privacy managers, chief information officers, chief information security officers, and other internal privacy support positions within state or local government.
- **Professional, Business, and Non-Government Members** are recommended by the Nominating Committee and may include chief privacy officers, compliance officers, privacy managers, chief information security officers, and other support positions.

The Board of Directors is responsible for: appointing an Executive Director and Program Management Office (PMO) to carry out the duties of StateRAMP, adopting standards and policies to guide the organization and cloud security verification, and adopting and overseeing financial policies and budget.

Officers of the Board include President, Past President, and Secretary/Treasurer, who together with the executive staff, comprise the Executive Committee.

Board leadership and Committee membership are updated and available on www.stateramp.org.

NOMINATING COMMITTEE

The Nominating Committee is a standing committee formed according to the StateRAMP By-laws and is comprised of three to five members. Committee members are recommended by the Nominating Committee and appointed by the Board. The committee recommends qualified individuals for Board membership, committee membership, and officers. The committee also makes recommendations on best practices for governance. In accordance with the StateRAMP By-laws, the National Association of State Chief Information Officers (NASCIO) and National Association of State Procurement Officials (NASPO) may appoint a representative to serve as a member on the Nominating Committee.

STANDARDS & TECHNICAL COMMITTEE

The Standards and Technical Committee is a StateRAMP standing committee, established by the Standards and Technical Committee Charter. Committee members are appointed by the Board, who strive to include representation from all stakeholders, including at least one member of the Board of Directors. The Standards and Technical Committee conducts regular meetings and may call special ad hoc meetings as needed. The Standards and Technical Committee makes recommendations to the Board regarding PMO policies, security standards, best practices, and assessment processes.

APPEALS COMMITTEE

The Appeals Committee is a StateRAMP standing committee, established by the Appeals Committee Charter. Committee members are appointed by the Board, who strive to include representation from all stakeholders, including at least one member of the Board of Directors.

The Appeals Committee serves as the adjudication board for issues related to the PMO such as a conflict of interest claim, disagreements over status determination, or requests for exceptions. They conduct meetings as needed.

APPROVALS COMMITTEE

The Approvals Committee was established by the Approvals Committee Charter, and its members represent state and local government and higher education institutions. The Committee is responsible for serving as the sponsoring government body required for the StateRAMP Authorized security status. Approvals Committee members possess the necessary technical and government policy knowledge and capabilities to review and approve product security packages and ensure government industry verification needs are met.

PROVIDER LEADERSHIP COUNCIL

The Provider Leadership Council (PLC) is established by the StateRAMP PLC Charter and gives all service providers a voice in ensuring StateRAMP fulfills its mission. The PLC's founding purpose is to provide expertise and advice regarding provider challenges, and to foster conversations with governments that result in efficient and effective cyber practices. Any Provider Member may designate a person to serve on the Provider Leadership Council. The PLC Directory and Charter are available at www.stateramp.org.

3PAO & ADVISORY COUNCIL

The 3PAO & Advisory Council is established by the Council Charter and provides an opportunity for communication and input to the StateRAMP PMO and StateRAMP Standards & Technical Committee on technical requirements, assessment process, and frequently asked questions. The Council is comprised of representatives from Third Party Assessing Organizations (3PAOs) and consulting organizations who are dues-paying members of StateRAMP.

1.3 STATERAMP ORGANIZATION

NON-PROFIT MANAGEMENT TEAM

StateRAMP is led by the Executive Director and Chief of Operations who support overall operations and governance. Additional staff support partnerships, marketing, and government provider membership benefits and support.

GOVERNMENT ENGAGEMENT TEAM

The Government Engagement Team (GET) works with public sector organizations to help share information about building effective risk management and authorization programs, and how integrating or adopting StateRAMP can support their efforts to better manage third-party risk.

The GET also works with public sector organizations to adopt StateRAMP through general project management support, coordinating education and outreach opportunities, and ongoing general support.

PROGRAM MANAGEMENT OFFICE

StateRAMP has an agreement with Knowledge Services to serve as the StateRAMP Program Management Office (PMO), given authority to carry out their work through the PMO Charter. The StateRAMP PMO supports service providers as they work to achieve their required/necessary level of StateRAMP authorization, and includes the following services:

MEMBERSHIP ENGAGEMENT TEAM (MET)
The MET works primarily to reach out to the service provider community to educate them on the benefits of becoming a StateRAMP member and serves as a liaison throughout the process to gaining authorization status.

PMO SECURITY TEAM

The PMO Security Team conducts the assessments to provide scoring for StateRAMP Security Snapshots. The team also guides providers through the StateRAMP authorization process of their applicable products and partners with the StateRAMP Board of Directors and committees to recommend providers for security authorizations. The PMO team is directly responsible for reviewing authorization packages submitted by service providers to become authorized.

The PMO team is also responsible for maintaining the continuous monitoring portal that public sector organizations use to review and assess the security packages submitted to the PMO team. This responsibility includes ensuring that service providers authorize access to requesting public sector entities, as well as managing overall access to the continuous monitoring portal.

PMO CONSULTANT TEAM

The StateRAMP consultant team works with providers through their experience in the Progressing Snapshot Program (covered in section 1.1.10), as well as any remediation efforts covered in Continuous Monitoring. The consultant team also offers subject matter expertise support and recommendations to the StateRAMP board and committees.

1.4 SECURITY FRAMEWORK

StateRAMP has selected the NIST 800-53, Rev. 5 framework as the foundation for all applicable standards. This is in part due to the best practice demonstrated by FedRAMP, and given that many security frameworks used by state and local governments are generally tied to the NIST 800-53 framework. This framework is applied in the assessment of service provider's specific products that serve state and local governments and additional public sector organizations.

To allow for a transition from Rev. 4 to Rev. 5 requirements, all providers have until October 1, 2024, to update security packages, including annual 3PAO audits, to comply with Rev. 5 updated baseline control requirements.

STATERAMP STANDARDS

The following outlines StateRAMP policies that establish StateRAMP security standards and requirements. These policies are reviewed and updated annually by the Standards and Technical Committee and are published at www.stateramp.org.

- StateRAMP Security Snapshot Criteria and Scoring
- StateRAMP Data Classification Tool
- StateRAMP Ready Minimum Mandatory Requirements for Low Impact Level
- StateRAMP Ready Minimum Mandatory Requirements for Moderate and High Impact Levels
- StateRAMP Baseline Controls by Impact Level for Authorization
- StateRAMP Authorization Boundary Guidance
- StateRAMP Penetration Test Guidance
- StateRAMP Continuous Monitoring Guide

- StateRAMP Vulnerability Scan Requirements Guide
- StateRAMP Incident Communications Procedures
- StateRAMP Continuous Monitoring Escalation Process Guide

STATERAMP PROGRAM REFERENCES

The following explicitly outlines the various application standards, directives, and industry best practices that StateRAMP also integrates:

- NIST definitions of cloud computing (NIST Special Publication 800-145)
- Computer Security Incident Handling Guide (NIST 800-61, Rev 2)
- Contingency Planning Guide for Federal Information Systems (NIST SP 800-34, Rev 1)
- Federal information systems security control assessment guide (NIST SP 800-53A, Rev 4)
- Security plans for Federal information systems development guide (NIST SP 800-18)
- A guide for applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (NIST SP 800-37, Rev 2)
- Guide for Mapping Types of Information and Information Systems to Security Categories (NIST SP 800-60, Rev 1)
- Guide for Security-Focused Configuration Management of Information Systems (NIST SP 800-128)
- Information Security Continuous Monitoring for Federal Information Systems and Organizations (NIST SP 800-137)
- Managing Information Security Risk: Organization, Mission, and Information System View (NIST SP 800-39)
- Recommended Security Controls for Federal Information Systems (NIST SP 800-53, Rev 5)
- Security and Privacy Controls for Federal Information Systems and Organizations RA-5 Requirements (NIST SP 800-53 Rev. 5)
- Privacy Control Catalog (NIST Special Publication 800-53 Rev. 5, Appendix J)
- Technical Guide to Information Security Testing and Assessments (NIST Special Publication 800-115)
- Digital Identity Guidelines Enrollment and Identity Proofing; Authentication and Lifecycle Management, and Federation and Assertions (NIST SP 800-63-3, 63A, 63B, 63C)
- An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (NIST SP 800-66 Rev. 1)
- International Information Security Standards: Security Control Mappings for ISO/IEC 27001 and 14508 (NIST SP 800-53 Rev. 5, Appendix H)

- Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (NIST Special Publication 800-84)
- Center for Internet Security (CIS Control 15: Service Provider Management)

THIRD PARTY ASSESSMENT ORGANIZATIONS (3PAOS)

3PAOs play a critical role in both the FedRAMP and StateRAMP security assessment process by providing an independent assessment of a provider's security controls. StateRAMP requires 3PAOs to be accredited through the FedRAMP 3PAO program, and accreditation occurs through A2LA. The accreditation ensures 3PAOs have demonstrated independence and the technical competence required to test security implementations and collect representative evidence.

A listing of accredited 3PAOs can be found at www.stateramp.org.

3PAOs participating in the StateRAMP program must:

- Plan and perform security assessments of provider systems
- Review security package artifacts in accordance with StateRAMP requirements

The StateRAMP Readiness Assessment Report (SR-RAR) and StateRAMP Security Assessment Report (SR-SAR) created by the 3PAO are key deliverables for consideration of a StateRAMP Ready or StateRAMP Authorized status. The SR-RAR and SR-SAR provide consistency in security audits upon which verification status is granted by StateRAMP. This consistent, repeatable model establishes confidence in authorizations that can be reciprocated and recognized by other state and local governments.

While States, local governments, and providers are free to use non-FedRAMP certified 3PAOs as independent assessors, use of an independent assessor may not be recognized by StateRAMP.

3PAOs do not need to be members of StateRAMP to be registered as a StateRAMP 3PAO. However, the organization does need to be a dues-paying member to participate in member activities, including on committees and on the 3PAO & Advisory Council.

1.5 STATERAMP ASSESSMENT PROCESS OVERVIEW

StateRAMP has worked to establish a streamlined, comprehensive authorization process that:

- Reduces barriers to security for all sizes of service providers
- Minimizes the cost of security compliance for all service providers
- Reflects the various risk levels for public sector organizations

Specifically, service providers may pursue the following opportunities for security status and review:

1.5.1 STATERAMP SECURITY SNAPSHOT

The StateRAMP Security Snapshot is a security maturity assessment for cloud products. The Security Snapshot helps service providers begin their cybersecurity journey while offering governments an initial level of insight into the risk maturity of suppliers' cloud products by providing an analysis that validates a product's current maturity utilizing the first top 40 most impactful controls as determined by the MITRE ATT&CK® Framework. The Security Snapshot is valid for a period of 12 months from the date of issuance and may be leveraged by multiple organizations during that time period. Please note: the StateRAMP Security Snapshot is different from a Single Use StateRAMP Security Snapshot as defined under Section

1.5.2 StateRAMP Provisionally Authorized in that there is no limitation on reuse. The Program includes quarterly assessments (Snapshots) and monthly, hour-long advisory calls with the PMO Consultant Team. Providers gain insight into their products' gaps in achieving NIST-based security controls and guidance on how to best address those gaps, with a focus on what matters most for improved security outcomes.

1.5.2 STATERAMP PROGRESSING SECURITY SNAPSHOT PROGRAM

The StateRAMP Progressing Security Snapshot Program is an ongoing security maturity assessment for cloud products. The Progressing Security Snapshot Program helps service providers begin their cybersecurity journey while offering governments an initial level of insight into the risk maturity of suppliers' cloud products on an ongoing basis. Enrollment in the Progressing Snapshot program includes quarterly assessments (Snapshots) and monthly, hour-long advisory calls with the PMO Advisory Team. Service providers gain insight into their products' gaps in achieving NIST-based security controls and guidance on how to best address those gaps, with a focus on what matters most for improved security outcomes. The criteria were designed to provide an analysis that validates a product's current maturity beginning with the top 40 most impactful controls as determined by the MITRE ATT&CK® Framework, while also allowing a Cloud Service Provider to continue their cyber security maturity journey to their desired verification status of StateRAMP Ready, Provisionally Authorized, or Authorized.

1.5.3 DATA CLASSIFICATION FOR AUTHORIZATION STATUS LEVEL

While a Snapshot can be used independently for risk insight and guidance on a product's gaps in achieving NIST-based security controls, the additional authorization status levels may be required or pursued to demonstrate a comprehensive adherence to NIST-800 53, Rev. 5 controls.

However, to determine which impact level is most appropriate for a product, service providers and public sector individuals can use the Data Classification Tool, which will be updated and published at www.stateramp.org to help identify the type of data that is being used, transmitted, or stored and its criticality level.

StateRAMP Security Controls are defined in three categories of impact levels:

- Low: Aligned with Low Impact, based on FedRAMP Low Control Baselines
- Moderate: Aligned with Moderate Impact, based on FedRAMP Moderate Control Baselines
- High: StateRAMP recognizes FedRAMP High Control Baselines

1.5.4 STATERAMP READY STATUS

A Ready status indicates that the product meets StateRAMP's Minimum Mandatory Requirements and most critical controls. The Ready requirements are published here and vary by Impact Level for Low, Moderate, or High. The security package for Ready includes a Readiness Assessment Report (RAR) submitted by a StateRAMP 3PAO, attesting to the minimum mandates. The required Ready documentation, including boundary diagram, inventory worksheet, roles, and permissions matrix, must be included in the security package provided to our Security Team through the StateRAMP Program Management Office (PMO). The StateRAMP PMO provides independent validation and verification that the security package and RAR comply with the standards established by the StateRAMP governing board and committees.

1.5.5 STATERAMP PROVISIONALLY AUTHORIZED STATUS

Provisionally Authorized status may be assigned by a sponsoring government or Approvals Committee to a package submitted for Authorized Status, as defined in Section 1.5.6 below, if the product meets the Authorization requirements, but one of the product's interconnected technologies is not StateRAMP or FedRAMP Authorized. To achieve a Provisionally Authorized Status, the interconnected technology must leverage a current StateRAMP Security Snapshot. The interconnected technology Provider(s) may obtain a single-use StateRAMP Security Snapshot without becoming a StateRAMP member. Read more about StateRAMP's Boundary Guidance at www.stateramp.org/templates-resources. The StateRAMP PMO provides independent validation and verification that the security package and SAR comply with the standards established by the StateRAMP governing board and committees.

1.5.6 STATERAMP AUTHORIZED STATUS

Authorized is the highest verification level. An Authorized status shows the product has a proven and complete security package that includes a System Security Plan (SSP) and Boundary Diagram, for example, along with all required documentation and policies and procedures. The provider has also completed and submitted an independent audit called a Security Assessment Report (SAR) that is conducted by one of our StateRAMP Third Party Assessing Organizations (3PAOs). The audit evaluates compliance with the NIST 800-53 required controls by impact level, in addition to penetration testing and other reviews. A SAR Template for the Audit report can be found on the StateRAMP resources page. The StateRAMP PMO provides independent validation and verification that the security package and SAR comply with the standards established by the StateRAMP governing board and committees. The PMO provides an executive summary and recommendation for status award to the Sponsoring body for Authorized Status. The final step in attaining an Authorized Status is approval by the Sponsoring body, the Approvals Committee or a Government Sponsor, who affirm the security package meets the requirements for Government.

Penetration tests are required by the Third-Party Assessment Organizations (3PAOs) and Providers for initial review for StateRAMP Ready or StateRAMP Authorized statuses and to comply with Continuous Monitoring reporting requirements, outline in the Continuous Monitoring Guide.

The Penetration Test Guidance policy can be found on www.stateramp.org as a reference for planning, executing, and reporting on StateRAMP penetration testing activities.

PLAN OF ACTION AND MILESTONES

After receiving the StateRAMP SR-SAR, the provider shall develop a POA&M (Plan of Action and Milestones) that addresses specific vulnerabilities noted in the StateRAMP SR-SAR. The provider must demonstrate its capacity, capabilities, and a schedule to correct each weakness. The POA&M serves as a tracking system for the provider, StateRAMP PMO and authorizing bodies. The implementation of the POA&M will be tracked during continuous monitoring, which begins upon authorization.

SUBMISSION OF A SECURITY PACKAGE FOR REVIEW

Following the conclusion of the 3PAO audit for Ready or Authorized, the provider must assemble a final package and submit the package for security review to the StateRAMP PMO. A final package will include:

- StateRAMP SR-SSP (StateRAMP System Security Plan) completed by the provider
- StateRAMP SR-SAP completed by the 3PAO
- StateRAMP SR-RAR completed by the 3PAO [only for Ready Status]

- StateRAMP SR-SAR completed by the 3PAO [only for Authorized Status]
- POA&M completed by the provider

View templates on StateRAMP website at www.stateramp.org.

PROGRESSING STATUS DEFINITIONS

StateRAMP recognizes cloud service offerings in the process of working toward a verified offering. To have a product listed as in progress, the Service Provider must be 1) enrolled in the StateRAMP Progressing Snapshot Program or 2) engaged with a Third-Party Assessment Organization (3PAO) to conduct an independent audit. The progressing statuses include Progressing, Active, In Process, Pending.

Progressing – A Progressing status indicates the product is enrolled in the Progressing Snapshot program, executed by the StateRAMP PMO.

Active - An Active status signals that a provider is working toward StateRAMP Ready. To be Active, the Service Provider must demonstrate an engagement with a 3PAO for a Readiness Assessment Report (RAR). Products may be listed with an Active status for a maximum of 90 days. The Executive Director may grant a 30-day extension.

In Process - An In Process status shows a service provider is working toward Authorized. This status may be assigned before a product passes the minimum requirements for Ready, if the Service Provider has engaged with a 3PAO for a Security Assessment Report (SAR). Products may be listed with an In Process status for a maximum of 90 days. The Executive Director may grant a 30-day extension.

Pending - A Pending status is used to describe a Service Provider who has submitted a product's security package to the StateRAMP PMO and is awaiting a determination for a verified status. Their 3PAO audit is completed, and they have completed their initial intake call with the StateRAMP PMO team.

AUTHORIZED PRODUCT LIST

Verified offerings with a security status of Ready, Provisionally Authorized, or Authorized are listed on the Authorized Product List (APL).

To be verified, the product must meet minimum security requirements and provide an independent audit conducted by a Third-Party Assessment Organization (3PAO). StateRAMP recognizes three verified statuses, including Ready, Provisionally Authorized, and Authorized. Ready products meet minimum requirements; Provisionally Authorized products exceed minimum requirements and have a government sponsor; Authorized products satisfy all requirements and have a government sponsor. To ensure ongoing security compliance and risk mitigation, providers must comply with continuous monitoring requirements to maintain a verified security status.

1.6 FEE SCHEDULE FOR SERVICE PROVIDERS

The fee schedule for the PMO to review security packages is adopted by the StateRAMP Board. You can view the current Fee Schedule on the StateRAMP website at the following link: StateRAMP Fee Schedule

1.7 CONTINUOUS MONITORING

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. Monitoring security controls is part of the overall risk management framework for information security.

To maintain an authorization that meets the StateRAMP requirements, the provider must monitor their security controls, assess them on a regular basis, and demonstrate that the security posture of their service offering is continuously acceptable.

Ongoing due diligence and review of security controls enables the security authorization package to remain current which allows state and local governments to make informed risk management decisions as they use a cloud solution.

Providers have the option to provision access to their government customers to the limited executive summary of monthly continuous monitoring or full details.

1.7.1 OPERATIONAL VISIBILITY

The StateRAMP Continuous Monitoring Guide is published at www.stateramp.org, including:

- Monthly Executive Summary
- Monthly update to the POA&M
- Annual 3PAO assessment of roughly 1/3 of the security controls

The StateRAMP PMO will provide a high-level summary of activity to the government authorizing body for review. Providers may also approve access to the summary of activities through a secure portal to participating governments.

1.7.2 VULNERABILITY SCAN REQUIREMENTS GUIDE

The StateRAMP Vulnerability Scan Requirements Guide, published on the StateRAMP website, describes the requirements for all vulnerability scans provided by service providers to StateRAMP for products with a Ready, Provisionally Authorized, or Authorized status. Service providers are required to perform vulnerability scanning of their information systems monthly (at a minimum).

INCIDENT RESPONSE

Providers must have incident response plans in place for all StateRAMP compliant systems, and document it as part of the StateRAMP SR-SSP. In the event of a security incident, a provider must follow the process and procedures found in the system Incident Response Plan. Based on the severity and outcome of security incidents and the impact they have on the security posture of a provider environment, the StateRAMP PMO and/or authorizing government body may initiate a review of a provider's authorization. Failure to report incidents may also trigger a review of a provider's authorization. StateRAMP has published guidance for incident response communications in the StateRAMP Incident Communications Procedures.

1.7.4 CONTINUOUS MONITORING ESCALATION PROCESS

The StateRAMP Continuous Monitoring Escalation Process document explains the actions taken when a Service Provider with a verified status of Ready, Provisionally Authorized and/or Authorized fails to maintain an adequate continuous monitoring program. Should a risk become a concern, the PMO and government authorizing body will work with the provider to identify a correction plan and timeline. Failure to comply with the correction plan may result in revocation of status, governed by the StateRAMP Continuous Monitoring Escalation Process policy, available on the StateRAMP website.

REVOKING A STATUS

StateRAMP has published a process for revoking a Status in the Continuous Monitoring Escalation Process Guide. Should a provider fail to comply with continuous monitoring requirements, the government authorizing body and/or StateRAMP PMO may revoke a status using the process defined in the Continuous Monitoring Escalation Process Guide. In the case of revocation, StateRAMP will update the APL accordingly.

1.8 FAST TRACK FOR READY, PROVISIONALLY AUTHORIZED, AND AUTHORIZED STATUSES

StateRAMP recognizes that many service providers have worked to establish compliance with other security frameworks, and therefore continues to expand 'fast track' options by which service providers can demonstrate compliance of a majority of the similar controls and work towards a faster review of any outstanding requirements.

The primary Fast Track option as of this version is for products that have a FedRAMP Ready or Authorized status.

1.8.1 FAST TRACK OPTIONS

StateRAMP Fast Track requires no new audit for products with a FedRAMP Ready, ATO (Authority to Operate), or P-ATO status. Providers who have completed a FedRAMP audit may submit the same audit and security package to the StateRAMP PMO, even before they have completed their FedRAMP Review Process.

Providers can begin the Fast Track process by completing a Security Review Request Form at www.stateramp.org.

1.9 CONCLUDING STATEMENT

StateRAMP leadership will continue to explore options for harmonization of compliance frameworks, with a focus on the Criminal Justice Information Systems (CJIS) framework in 2024. Additionally, the StateRAMP PMO is conducting a Pilot Fast Track for HI-Trust products in 2023-2024.

With a commitment toward continuous improvement, the StateRAMP will continue to pursue other initiatives that will further broaden the applicability and utility of this effort for states and local entities.

APPENDIX A - DEFINITIONS

Term	Definition
3PAO/ Approved Assessor	Third party assessment organization. StateRAMP currently works with organizations who are A2LA-certified and FedRAMP-approved to provide independent, third-party assessments of service providers' cybersecurity maturity based on the NIST 800-53 Rev 5 (or updated) standards. Approved Assessors are listed on the StateRAMP website.
Approvals Committee	The Approvals Committee is charged with serving as the body for Government Sponsorship for StateRAMP Authorized and StateRAMP Provisionally Authorized Statuses. The Committee is comprised of leaders in government, education, and cybersecurity to bring proven experience and clear insight to the committee. Committee members serve as authorizing officials on behalf of government if a provider is unable to secure a government sponsor.
AO	An Authorizing Official is designated by a government sponsor to conduct a review of the StateRAMP PMO's assessment of a product. This individual is granted access to the secure portal to review documentation and connect with the PMO team on any questions.
AOO	Authority to Operate Order asserts that the supplier's internal security policies meet the minimum security policies/standards set by the public sector organization's security team.
ATO	An Authorization to Operate is a formal letter given to service providers whose product meets StateRAMP's security standards for Authorized.
APL	Authorized Product List
CSP	Cloud Service Provider; alternatively, service provider, provider, vendor
FedRAMP	Federal Risk and Authorization Management Program - The Federal Risk & Authorization Management Program was set up for federal agencies. StateRAMP has used the FedRAMP model to influence its approach to setting up a similar program for state and local governments
Government Engagement Team	StateRAMP team dedicated to supporting organizations effectively implement and integrate StateRAMP as part of their overall risk management strategy.
Government Member	Individuals representing state or local governments, tribal agencies, K-12, public higher education institutions or other public sector and critical infrastructure organizations who have signed up for free StateRAMP membership to gain access to ongoing news and insights on third-party risk management. Government organizations may also sign up as a member.

	Sign-up form
Government Sponsor	A government sponsor is any SLED (state, local, education, tribal/territorial) government official or employee who serves in the role of Chief Information Security Officer or designee and is a StateRAMP Member (Individual or Certified). Sponsors support the product authorization review.
IaaS	Infrastructure-as-a-Service. IaaS offers essential compute, storage, and networking resources on demand. It helps reduce maintenance costs and increases reliability while giving the flexibility to scale IT resources up or down with demand.
Member Engagement Team	The Membership Engagement Team is dedicated to supporting outreach, education, and engagement for service providers.
NIST 800-53	National Institute for Standards and Technology Special Publication for Security and Privacy Controls for Information Systems and Organizations on which the StateRAMP program is based.
Organization	Any state, local, education, tribal agency, critical infrastructure/utilities partner, or other public sector or critical infrastructure group that serves as a participating StateRAMP member.
PaaS	Platform as a Service provides a complete development and deployment environment in the cloud, with resources that enable organizations to deliver cloud-based apps, cloud-enabled enterprise applications, etc.
P-ATO	A Provisionally Authorized Authorization to Operate is a formal letter given to service providers whose product meets some, but not all, of StateRAMP's security standards for Authorized.
PMO	StateRAMP Program Management Office that oversees the authorization process and delivers the final authorization to service providers.
SaaS	Software as a Service is a software solution that is utilized on a pay-as-you-go basis. The use of an application is essentially 'rented' out, and users can connect to it over the internet – usually in a web browser. All of the underlying infrastructure and software are located in the service provider's data center. The service provider manages the hardware and software.
Security Status	Designations assigned to products that have successfully completed a security assessment conducted by a third-party assessment organization that has been reviewed by the PMO to validate security compliance; StateRAMP security statuses include Active, Ready, In Process, Provisionally Authorized, and Authorized

	An additional opportunity available to service providers and governments is the use of a Snapshot or enrollment in the Progressing Snapshot Program, which allows for a high-level capture of a service provider's overall risk level.
SLED	Also referred to as SLTT (State, Local, Tribal, and Territorial), includes state, local, education, tribal and territorial organizations
TPRM	Third-party risk management is the process of analyzing and minimizing risks associated with outsourcing to third-party service providers.

APPENDIX B: FREQUENTLY ASKED QUESTIONS

For a complete list of FAQs (Frequently Asked Questions), visit https://stateramp.org/faq/.

Policies and documentation will be reviewed no less than annually by the StateRAMP Board and maintained and made available on the StateRAMP website at www.stateramp.org.