STATERAMP SECURITY ASSESSMENT FRAMEWORK

VERSION:
1.4

DATE:
April 29, 2022

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

This document will be reviewed at the discretion of the StateRAMP Board at a frequency no less than annually.

EXECUTIVE SUMMARY

This document describes a general Security Assessment Framework (SAF) for StateRAMP. In April 2020, a steering committee of government and industry leaders chartered StateRAMP to bring States together and create a common method to verify security.

StateRAMP was formed in 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 and operates as a 501(c)6 nonprofit. The StateRAMP mission is to promote cybersecurity best practices through education, advocacy, and policy

development to support our members improve the cyber posture of state and local governments and the citizens they serve.

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 state and local governments, public education institutions and special districts can validate the security of their third-party IaaS, PaaS, and/or SaaS solutions which process, transmit, and/or store the government's data.

StateRAMP's security verification model is based on NIST 800-53 Rev. 4 published by the National Institute of Standards and Technology (NIST), which also serves as the framework for FedRAMP requirements. Additionally, NIST 800-53 Rev. 4 has been adopted as the security framework for several state governments. Many government officials, industry experts, and working groups participated in adopting standards for controls, policies, and procedures for StateRAMP. These policies and requirements, along with any future proposed amendments, will be published on www.stateramp.org.

STATERAMP OVERVIEW

1.1 GOVERNANCE

StateRAMP is governed by a Board of Directors with a majority representation from state and local government officials, and minor representation from private industry, and subject matter experts. StateRAMP is self-governing, non-commercial, non-sectarian, non-profit, and non-partisan.

1.2 PROGRAM OVERVIEW

StateRAMP provides a platform for state and local governments seeking simplified cloud security verification and for providers seeking clarity and consistency in security requirements along with business development opportunities, education, opportunities for committee membership, access to publications, and more.

Table 1 includes the list of fees to be paid by providers participating in the StateRAMP program and the milestones at which said fees are due. The fees listed below do not include any costs incurred by the provider when contracting with a Third-Party Assessment Organization (3PAO).

MILESTONE	SR-RAR Review conducted by PMO to determine Ready Status	SR-SAR Review conducted by PMO to determine Authorization Status	Annual Fee for Continuous Monitoring
FEE	$2,500	$5,000	$5,000

Table 1

Financial data will be transparent and documented to inform the Board of Directors for long-term decisions and best practices. The Board and PMO will work together to collect data throughout the inaugural year to track progress and to inform the long-term policies and procedures of StateRAMP.

1.3 APPLICABLE STANDARDS AND GUIDANCE

All applicable standards will be reviewed annually by Board of Directors. Generally, the standards will align with the NIST 800-53 framework, Rev. 4 and best practices outlined by FedRAMP. Current applicable standards, directives, and industry best practices include:

- NIST definitions of cloud computing (NIST SP 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 4)
- Security and Privacy Controls for Federal Information Systems and Organizations RA-5 Requirements (NIST SP 800-53 Rev. 4)
- Privacy Control Catalog (NIST Special Publication 800-53 Rev. 4, Appendix J)
- Technical Guide to Information Security Testing and Assessments (NIST SP 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. 4, Appendix H)
- Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (NIST SP 800-84)
- Security Requirements for Cryptographic Modules (FIPS 140-3)

Additional Helpful Resources:

- Engineering Principles for Information Technology Security (A Baseline for Achieving Security) (NIST SP 800-27, Rev A)
- Minimum Security Requirements for Federal Information and Information Systems (FIPS Publication 200)
- Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS Publication 201-1)
- Guide for Conducting Risk Assessments (NIST SP 800-30, Rev 1)
- Security Considerations in the System Development Life Cycle (NIST SP 800-64, Rev 2)
- Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (NIST SP 800-52 Rev. 2)
- Transitioning the Use of Cryptographic Algorithms and Key Lengths (NIST 800-131A Revision 2)
- Recommendation for Key Management: Part 1 (NIST SP 800-57 Part 1 Rev. 5)
- Center for Internet Security (CIS Benchmark Level 1)

1.4 GOVERNANCE & STAKEHOLDERS

1.4.1 BOARD OF DIRECTORS

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

- **NASCIO Delegates** are selected by the National Association of State and Chief Information Officers (NASCIO) to serve on the StateRAMP Board of Directors.
- **NASPO Delegates** are selected by the National Association of State Procurement Officials (NASPO) to serve on the StateRAMP Board of Directors.
- **Government Members** are individuals working within a state or local government and are recommended by the Nominations 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 Nominations Committee and may include chief privacy officers, compliance officers, privacy managers, chief information security officers, and other internal privacy support positions.

The Board of Directors is responsible for: appointing an Executive Director and Project Management Office 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 membership, schedule of regular meetings, bylaws, and adopted policies will be published and maintained on www.stateramp.org.

1.4.2 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.

Membership and a schedule of regular meetings of the Standards and Technical Committee are published and maintained on www.stateramp.org.

For the duration of Pilot Program, the Board of Directors may assume the roles and responsibilities of the Standards and Technical Committee.

1.4.3 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 regular meetings and may call special ad hoc meetings as needed.

In some cases, the Executive Committee, which includes Board Officers and executive staff, may appoint a subject matter expert to the committee to aid in a claim assessment as needed.

Membership and a schedule of regular meetings of the Appeals Committee are published and maintained on www.stateramp.org.

For the duration of Pilot Program, the Board of Directors may assume the roles and responsibilities of the Appeals Committee.

1.4.4 STATERAMP APPROVALS COMMITTEE

The Approvals Committee is established by the Approvals Committee Charter, and its members represent state and local government and higher education. 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.

1.4.5CORPORATE COMMUNITY COMMITTEE

The Corporate Community Committee will be established by the Board at a future date, is open to all vendors, providers, 3PAOs, and other non-governmental organizations. Before the committee is established, the Board shall ensure a mechanism for input from the corporate community into policies.

Information on meetings and opportunities for feedback and participation are published and maintained on www.stateramp.org and through the StateRAMP Members Website.

1.4.6 PROGRAM MANAGEMENT OFFICE

The StateRAMP Program Management Office (PMO) is established by the PMO Charter and adopted by the Board of Directors.

The StateRAMP PMO possesses the necessary technical knowledge and capabilities to provide States, agencies, and providers with a standard approach and guidance related to the security authorization process. Similarly, the PMO is responsible for the day-to-day operations of the StateRAMP program and maintain a secure credentialing repository to manage program participant data.

The repository will be a cloud-based system that processes, stores, and transmits sensitive provider data and therefore must be FedRAMP Authorized at the moderate impact level or higher. The solution must be hosted on a Gov or Commercial Cloud system that is FedRAMP Authorized at moderate impact level or higher. This requirement will be assessed by the Board of Directors on an ongoing basis.

The PMO will guide the providers through the StateRAMP authorization process and partner with the StateRAMP Board of Directors and committees to recommend providers for security authorizations. Additionally, the PMO will act as the central point of communication for all StateRAMP stakeholders and act in best practice to help States, agencies, and providers understand the StateRAMP process, goals, and objectives1.4.7 State and Local Governments, Public Education Institutions and Special Districts

StateRAMP seeks to bring together governments to create a common method to verify security and to provide a fair, repeatable, transparent, and affordable model for all. With StateRAMP, state and local governments, public education institutions and special districts do not have to carry the burden or the budget impact of provider cybersecurity verification. providers benefit from a “verify once, use many” streamlined authorization process.

StateRAMP complements existing state and local government cyber efforts and reduces the risk of a major data breach or malware attack by ensuring essential security controls are properly implemented on cloud systems that process, store, and/or transmit Government data.

With StateRAMP, state and local governments can trust but verify third party providers to:

- Reduce cyber risks and protect sensitive data
- Create an efficient and cost-effective verification model
- Simplify processes for procurement, IT, and providers

The federal government created FedRAMP, under the responsibility of the Office of Management and Budget (OMB), to verify the cloud security of its vendors based on NIST 800-53 Rev. 4 standards. To achieve and maintain FedRAMP Authorization, a provider must be an active vendor of the federal government. There are many providers who serve state and local government who do not, and will never, conduct business with the federal government.

Requiring FedRAMP Authorization for providers as a qualifier to work with state and local government would exclude entire communities of vendors and entrepreneurs. State and local governments have been left to create their own processes for security verification.

Like the federal government, most states also define NIST 800-53 Rev. 4 as their cybersecurity framework. As such, StateRAMP is built on NIST 800-53 Rev. 4.

Adopting StateRAMP for state and local government begins by the information security officer or authorizing body adopting the NIST 800-53 Rev. 4 and requiring third party StateRAMP verification for providers. Final determinations of risk acceptance and contracting decisions always remain with the state and local governments.

1.4.8 THIRD PARTY ASSESSMENT ORGANIZATIONS

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

Leveraging the marketplace and standards FedRAMP has created, StateRAMP also requires 3PAOs be accredited through the FedRAMP 3PAO program. A listing of accredited 3PAOs can be found at: https://marketplace.fedramp.gov/.

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.

1.4.5 1.4.9 SERVICE PROVIDERS

Service providers offering cloud computing services that have transformed business operations across state and local governments, public education institutions and special districts and have made remote work possible. Providers participating in StateRAMP can provide one or more of the following solutions: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and others storing, processing, and/or transmitting government data in environments outside the control of the respective government.

The same classification applies to contractors who utilize a SaaS, PaaS, or IaaS to provide services that involve the storage, processing, and/or transmitting of government data.

One challenge providers face in doing business across government agencies is the uncertain, changing, and differing security requirements that exist between state and local governments. Understanding what security requirements exist, and what needs to be done to achieve and maintain the appropriate security certification, significantly reduces the barriers to entry and provides businesses an opportunity to scale.

With StateRAMP, the expectations are clear, and providers can confidently bid on government projects knowing that they meet the security requirements set forth by information security officers and procurement officials. StateRAMP provides the following benefits for providers:

- Fewer barriers of entry and the opportunity to scale
- Focused, structured security requirements
- A level playing field for competition

A listing of providers who achieve a StateRAMP security status will be maintained and published on the Authorized Product List (APL) found at www.stateramp.org.

STATERAMP REQUIREMENTS

As more state and local governments, public institutions and special districts have transitioned to cloud computing environments, data protection and cybersecurity remain top priorities.

A key factor in the successful government adoption of cloud computing solutions, is ensuring essential controls are properly implemented on cloud systems. To do this, cloud systems must meet the level of security commensurate with the government data that is being processed, stored, and/or transmitted. NIST SP 800-60, Rev 4 maps data sensitivity to impact levels, including low impact (generally public

data), moderate impact (generally confidential data), and high impact (generally affecting national security). Most state and local government data will likely fit within low or moderate impact levels.

StateRAMP provides a standardized process to identify and assess risks and security compliance of providers by impact level. This gives state and local governments the ability to make informed, risk-based decisions on their use of cloud services.

Bringing state and local government together to utilize one standard approach for risk assessment saves taxpayer dollars, government resources and eliminates duplicative efforts for both government and the providers.

While StateRAMP defines security impact levels and requirements that are aligned with NIST 800-53 rev. 4 and will make recommendations for baseline security levels, the contracting government has final determination for requirements.

1.5 AUTHORIZATION PATH

The statuses recognized by the StateRAMP PMO, include Active, Pending, Ready, In-Process, Provisional and Authorized. Three milestone statuses are Ready, Provisional, and Authorized. These milestone statuses convey the provider has completed necessary 3PAO audits and a review by the sponsoring state and StateRAMP PMO and has been found to meet minimum requirements.

Active denotes a provider has begun working with a 3PAO and is registered with StateRAMP. Pending denotes that a provider has submitted required Ready Documentation.

To achieve a Ready Status, a provider must meet the Minimum Mandatory Requirements for Ready as attested to by a 3PAO in the Readiness Assessment Report (SR-RAR). As stated in section 1.4.7, the 3PAO must be an accredited FedRAMP 3PAO. The StateRAMP PMO will evaluate the SR-RAR and assess the readiness of the provider to achieve the desired impact level. If the PMO determines the provider meets minimum requirements, the provider will be awarded a Ready Status. This Ready Status indicates that both 3PAO and PMO attest to a provider's readiness for the authorization process. State and local governments may require providers responding to an RFP achieve Ready Status as a prerequisite for selection.

Once the notice to award a contract has been issued, the government entity may require the provider to move forward with full authorization. In-Process means the provider has engaged a 3PAO for a full StateRAMP SR-SAR. Once the SR-SAR has been completed, the 3PAO will provide the artifacts and reporting to StateRAMP PMO. The PMO will review the SR-SAR and the provider's System Security Plan (SSP) to ensure critical controls are met and a Plan of Action & Milestones (POA&M) is developed to address vulnerabilities for continuous monitoring.

Authorized is assigned when both the contracting (or sponsoring) Government and StateRAMP PMO can attest the provider meets minimum security controls. Alternatively, the StateRAMP Approvals Committee may serve in the capacity of the sponsoring government. Continuous monitoring begins upon award of Ready, Provisional, or Authorized status. Once a provider achieves Ready, Provisional, or Authorized status, continuous monitoring is required to maintain the status. If the provider is deemed to not meet all the controls for Authorized status but does meet the minimum mandatory requirements for

Ready and has demonstrated a plan for completion, the sponsoring State may assign a Provisional status.

The goal is for all state and local governments to recognize the validation of statuses. State and local governments have the ability to require additional controls as needed. Additional controls will be noted, along with the provider's status, and published on the StateRAMP APL at www.stateramp.org.

1.6 AUTHORIZED VENDOR LIST

The StateRAMP Authorized Vendor List displaying a provider's impact level and status will be maintained and published at stateramp.org.

1.6.1 USING A PROVIDER NOT LISTED ON THE AUTHORIZED VENDOR LIST SELECT SECURITY CONTROLS

It is a best practice when using cloud providers to assess risk up front and with continuous monitoring. Using a provider on the StateRAMP Authorized Product List validates essential controls are properly implemented and maintained on the cloud system.

Final determinations of risk acceptance and contracting decisions remain with the state and local governments.

STATERAMP SECURITY ASSESSMENT FRAMEWORK

StateRAMP's Security Assessment Framework process is modeled after the NIST Risk Framework Management, upon which FedRAMP is also modeled.

1.7 DOCUMENT

1.7.1 SELECT SECURITY CONTROLS

The first step for a state or local government and a provider is to identify the required impact level. NIST SP 800-60, Rev 1 maps data sensitivity to impact levels, including low impact (generally public data), moderate impact (generally confidential data), and high impact (generally affecting national security). Most state and local government data will likely fit within low or moderate impact levels.

StateRAMP Security Controls are defined in three categories:

Low: Aligned with Low Impact, based on FedRAMP Low Control Baselines
Low+: Aligned with Low/Moderate Impact, adapted from FedRAMP Low and Moderate Control Baselines
Moderate: Aligned with Moderate Impact, based on FedRAMP Moderate Control Baselines

It is StateRAMP's goal to provide the state or local government authorizing body flexibility to require additional controls as appropriate. For example, additional controls may be necessary to comply with CJIS or MARS-E 2.0 requirements. These additional controls would be noted as (+) on the StateRAMP

APL so that providers can benefit from the higher authorization indicating an ability to comply with more rigorous standards.

The Data Classification Tool help guide the determination of Security Impact Level. Final determination lies with the contracting government information security official.

The Data Classification Tool and StateRAMP Security Baseline Controls Templates are published and maintained on www.stateramp.org.

1.7.2 IMPLEMENT SECURITY CONTROLS

Once the provider has selected the appropriate impact level, the next step is to implement the security controls related to that impact level. Security baseline templates will be published at www.stateramp.org.

For most providers, many of the controls are already implemented but need to be described adequately within the templates. Some controls might require the implementation of new capabilities, and some controls might require a re-configuration of existing implementations.

The important part of implementing security controls is that the intent of a security control is met. Providers may provide alternate implementations that demonstrate the implementation satisfies the intent of the control requirement. For any control that cannot be met, providers must provide a satisfactory justification for not being able to implement the control and the justification must be approved by the StateRAMP PMO.

1.7.3 SYSTEM SECURITY PLAN

To document the system security and controls, providers must complete a StateRAMP System Security Plan (SR-SSP). SR-SSP Templates are published at www.stateramp.org.

1.8 ASSESS

1.8.1 THIRD PARTY ASSESSMENT ORGANIZATIONS

Providers must use a FedRAMP Authorized 3PAO as the independent assessor to test the information system and demonstrate the controls are effective and implemented as documented in the StateRAMP SR-SSP. Requirements for StateRAMP 3PAOs and a listing of registered StateRAMP 3PAOs can be found at www.stateramp.org.

1.8.2 COMPLETE THE READINESS ASSESSMENT REPORT

To achieve the Ready Status, a provider must partner with an accredited 3PAO to complete a readiness assessment of its service offering. At the conclusion of the assessment, the 3PAO delivers a SR-RAR attesting to the providers readiness for the authorization process. Once the SR-RAR is deemed satisfactory by the 3PAO and the PMO, the StateRAMP Marketplace will be updated to reflect the provider as Ready.

The StateRAMP SR-RAR is developed by the 3PAO. The SR-RAR documents the providers capability to meet the minimum security requirements and is intended to help vendors and agencies have a snapshot of the security posture of a cloud service without the full investment of time and resources needed to complete the full security process of testing and documentation.

1.8.3 COMPLETE THE SECURITY ASSESSMENT PLAN

The StateRAMP Security Assessment Plan (SR-SAP) is developed by the 3PAO. The 3PAO creates a testing plan using the SR-SAP template.

The SR-SAP contains the test plan to assess the security controls of a system. The test plan functions as a detailed roadmap of the approach and methodology for the assessment of a provider's cloud service.

The SR-SAP template is published at www.stateramp.org.

1.8.4 ANALYSIS OF RISKS FOR AUTHORIZATION

After testing the security controls, the 3PAO analyzes the risks and provides a StateRAMP SR-SAR. The provider submits the SR-SAR to the PMO for review.

The SR-SAR contains information about vulnerabilities, threats, and risks discovered during the testing process. Additionally, the SR-SAR provides guidance for providers in mitigating the security weaknesses. The PMO and state authorizing body will review the StateRAMP SR-SAR to determine the overall risk posture of the provider.

1.9 AUTHORIZE

Once testing has been completed, the next step is for the StateRAMP PMO and government authorizing body to make an authorization decision based on the completed package of documents and the risks identified during the testing phase.

1.9.1 PLAN OF ACTION AND MILESTONES

After receiving the StateRAMP SR-SAR, the provider shall develop a POA&M that address 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.

1.9.2 SUBMISSION OF A SECURITY PACKAGE FOR AUTHORIZATION

Following the development of the StateRAMP SR-SAR, the provider must assemble a final package and submit the package for authorization review to the StateRAMP PMO. A final package will include:

- StateRAMP SR-RAR completed by the 3PAO
- StateRAMP SR-SSP completed by the provider
- StateRAMP SR-SAP completed by the 3PAO
- StateRAMP SR-SAR completed by the 3PAO
- POA&M completed by the provider

The PMO and authorizing government or Approvals Committee will review the entire security package and make a risk-based decision on whether to award a status of authorization. Both the PMO and government body must agree on the determination of status for it to be listed on the StateRAMP Marketplace.

Final contracting decisions remain with the state and local governments.

1.9.3 RECOGNITION OF STATUS

A provider's security status will be published and maintained on the StateRAMP APL at www.stateramp.org. StateRAMP will provide a badge to providers for marketing use when a milestone status is obtained, including Ready, Provisional and AuthorizedLeveraging StateRAMP Security Packages

One of the primary benefits of StateRAMP is the ability for state and local governments to recognize and reuse authorizations to leverage the work already completed so provider can "do once, use many."

The StateRAMP PMO maintains all documentation and artifacts in a secure repository. State and local government bodies interested in viewing a provider's documentation can request access, which must be approved by the provider.

State and local governments can piggyback on StateRAMP Authorizations as an additional authorizing body. To benefit from continuous monitoring, governments should contact StateRAMP directly at info@stateramp.org.

1.9.4 REVOKING A STATUS

StateRAMP shall publish a process for revoking a Status. Should a provider fail to comply with continuous monitoring requirements, the government authorizing body and/or StateRAMP PMO may revoke a status after consultation with the Appeals Committee. In the case of revocation, StateRAMP will updates the APL accordingly. update the

1.10 MONITOR

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.

1.10.1 OPERATIONAL VISIBILITY

The StateRAMP Continuous Monitoring Plan will be 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 all submitted reports, along with a high-level summary of activity to the government authorizing body for review. 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.

1.10.2 CHANGE CONTROL

Significant changes, as defined by the government authorizing body, shall be reported by the provider to the StateRAMP PMO and authorizing body within 30 days of a change. After any change is made, the impacted security controls shall be documented.

The annual assessment by the 3PAO should note any other changes and affected security controls.

1.10.3 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 will publish templates and guidance for incident response plans at www.stateramp.org.

APPENDIX A

TERMINOLOGY

Providers	Providers who utilize a cloud-based system (IaaS, PaaS, SaaS) to process, transmit and/or store government data
3PAO	Third Party Assessment Organizations, 30+ accredited by FedRAMP
Security Packages	Documentation of a cloud system's security
Impact Levels	Based on sensitivity/integrity of data, Aligned with FedRAMP
Security Status	Status of security authorization, Active, Pending, Ready, In Process, Provisional & Authorized
PMO	Program Management Office, Reviews 3PAO audits and works with governance committee(s) to determine authorizations and recommends adjudication
APL	Authorized Product List: Directory of products with StateRAMP Security Status

APPENDIX B

FREQUENTLY ASKED QUESTIONS

For a complete list of FAQs, 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.