StateRAMP Overview

SPRING 2021

stateramp.org

StateRAMP

Why StateRAMP?

PROBLEM STATEMENT

How to provide state and local government procurement and security officials assurance that their contractors have the processes and capabilities necessary to meet state and local government policy requirements.

GOALS

- Standardized approach
- Meet minimum requirements
- Consistency in RFPs
- Best value

OUTCOME

- Improve security for state and local government
- Streamline and reduce costs for government and its vendors

Verification of vendor cybersecurity is a requirement in the federal system. Through the creation of Federal Risk and Authorization Management Program (FedRAMP), the federal government requires all service providers to meet their cyber policies by independent 3rd party verification. FedRAMP Authorization is only eligible for providers doing business with the federal government, eliminating it as a source for common verification for state and local government and their providers.

Because there is no common standard for state and local governments, states and locals are left to either contract with federal government contractors who are FedRAMP authorized or develop their own approach. Without a common method for verification, each agency struggles separately to secure budget, attract/retain experts, and develop policies to validate their contractors have appropriate security and data controls in place.

The National Association of State Chief Information Officers (NASCIO) listed cybersecurity and managing third party risk as their #1 2021 priority for the 8th consecutive year. StateRAMP was created to assist state and local governments in managing the third-party risk with service providers.

StateRAMP

What is StateRAMP?

In 2020, a Steering Committee comprised of dozens of current and former State Chief Information Officers, Chief Information Security Officers, Procurement and Privacy Officials joined private industry leaders and cyber assessing organizations to charter StateRAMP.

StateRAMP creates a **framework that can be implemented by procurement and security officials** for continuous improvement in cybersecurity for state & local governments, providers, and the constituents they serve.

- Shared Services Model for States and Local Government
- "Verify Once, Use Many" Approach for Providers
- Centralized Resources for Government & Providers
- Path for Procurement to Verify Controls Required
- Ongoing Commitment to Education and Best Practice
- State and Local Government Led Governance and Collaboration

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 required data, including personally identifiable information (PII), personal health information (PHI) and payment card industry (PCI) information.

StateRAMP launched in 2021 and is organizing as a 501c6 non-profit organization, governed by a majority of state and local government officials, with minority representation from private industry and subject matter experts.

Like FedRAMP, StateRAMP's process for verification relies on FedRAMP Authorized Third Party Assessing Organizations (3PAOs) to conduct independent audits and assessments. The requirements are built on the widely accepted National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 4 framework, modeled in part after FedRAMP.

With StateRAMP, Procurement Officials, Privacy Officers, and Information Security Officers can be confident in knowing government-selected service providers meet and maintain published cybersecurity policies.

Secure service providers have the ability to grow their government business at scale through transferrable cybersecurity verifications published on StateRAMP's Approved Vendor List.

StateRAMP formalizes processes that allow third party assessment organizations to validate IaaS, SaaS, and PaaS solutions to ensure service providers meet government-published cybersecurity policies.

StateRAMP

How the Process for Vendor Verification Works

1. The process begins with a state or local government adopting a cyber policy that requires independent verification of their vendor's cyber posture and may be verified by StateRAMP.

2. Providers who wish to do business with that state or local government engage a Third Party Assessing Organization (3PAO) for the required assessments. Any FedRAMP 3PAO is eligible to conduct the assessments but must register with StateRAMP.

3. The 3PAO conducts a Readiness Assessment Report or Security Assessment Report and submits the security package to StateRAMP.

4. StateRAMP manages the Program Management Office (PMO), whose security professionals review the security package and verifies security status based on the policies adopted by the StateRAMP Board. The StateRAMP PMO also maintains responsibility for continuous monitoring.

5. StateRAMP will publish and maintain a publicly available Authorized Vendor List (AVL) on stateramp.org that will include information about the service providers' products, including impact level, provider type, and security status.

STATE OR LOCAL GOVERNMENT

Policy defines cyber requirements for Service Providers

PROVIDER

Engages accredited and approved Third Party Assessment Organization (3PAO) to complete assessments & audit

→

3PAO

Completes audit of Provider's security and submits Security Package to StateRAMP for review

→

StateRAMP

Reviews 3PAO-submitted Security Package and assigns Security Status of Provider, publishing status

Data Classification and Categorization Guide Impact

Once a service provider has made the decision to verify cloud security with StateRAMP, the first step is to identify at which impact level.

StateRAMP recognizes three impact levels, including:

1

CATEGORY 1- FEDRAMP LOW CONTROL BASELINES

Category 1, which aligns with FedRAMP Low, generally maps to data or systems that involve publicly available data.

2

CATEGORY 2- FEDRAMP LOW + SELECT MODERATE CONTROLS

Category 2 was a response to requests from stakeholders for a Low + option. Category 2 will be further developed and validated in 2021.

3

CATEGORY 3- FEDRAMP MODERATE CONTROL BASELINES

Category 3 aligns with FedRAMP Moderate, and generally maps to data or systems that involve confidential data or involve systems that are of high criticality to the continuity of government.

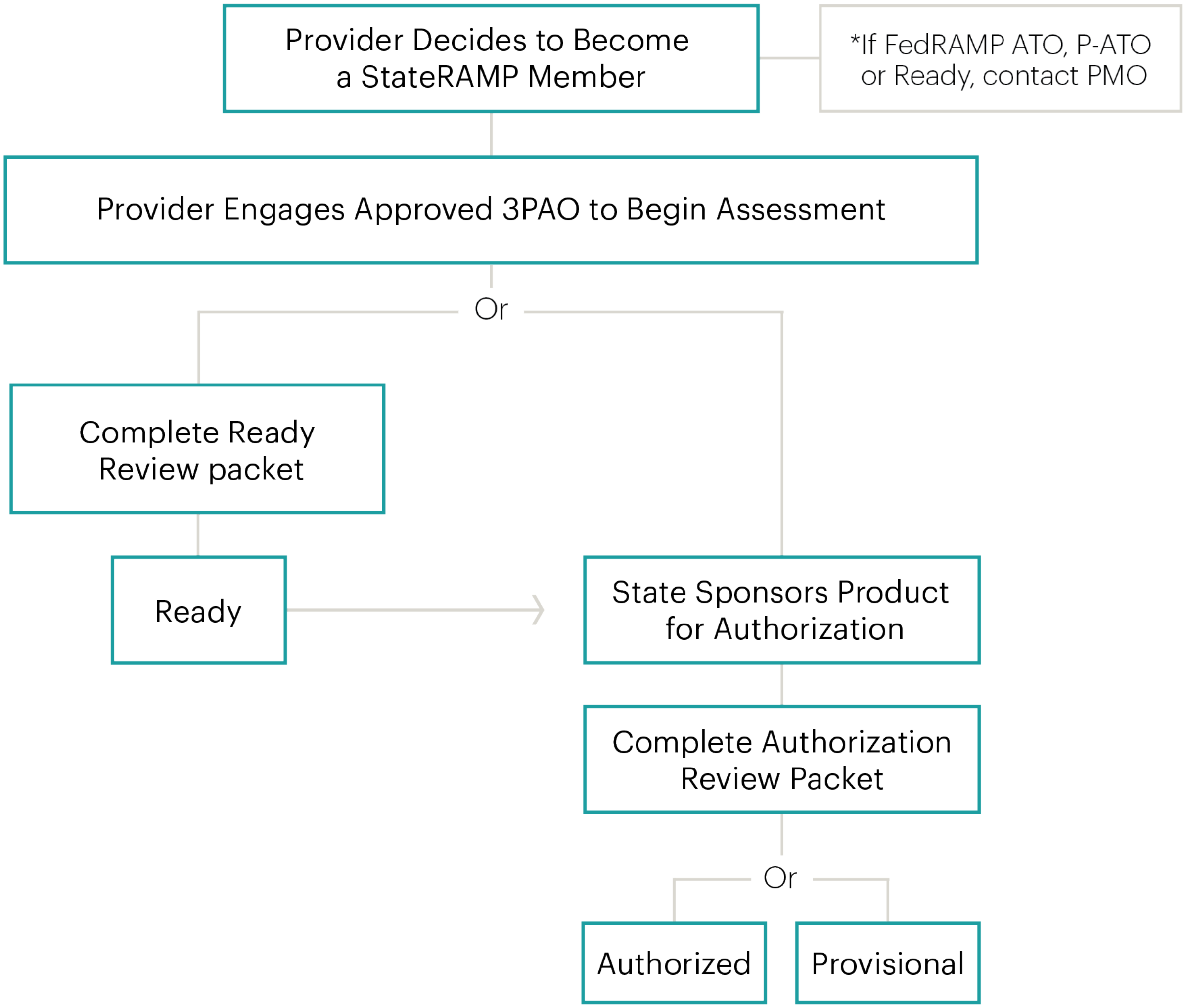
Government entity defines required procurement/contract security impact level. StateRAMP Impact Levels include 3 categories. All categories align to NIST 800-53 Rev. 4.

The StateRAMP Data Classification Tool is available for government and procurement officials and service providers to help guide impact level selection. View the Data Classification Tool at **www.stateramp.org/documents.**

Security Status Progression

There are three milestone statuses recognized by StateRAMP that include: Ready, Authorized and Provisional. Ready does not require a Government Sponsor. Authorized and Provisional statuses require a Government Sponsor.

DECISION TREE


Provider Decides to Become a StateRAMP Member
*If FedRAMP ATO, P-ATO or Ready, contact PMO
Provider Engages Approved 3PAO to Begin Assessment
Or
Complete Ready Review packet
Ready
State Sponsors Product for Authorization
Complete Authorization Review Packet
Or
Authorized
Provisional

StateRAMP Security Milestone Statuses

READY is a status that is attained by meeting the Minimum Mandatory Requirements demonstrated by a Readiness Assessment Report that is conducted by a Third Party Assessing Organization (3PAO). No contract or government sponsor is required for Ready Status. A provider that is StateRAMP Ready indicates this is an offering that meets the minimum requirements and is likely well positioned to be able to comply with the full authorization requirements.

While StateRAMP's vendor verification process is modeled after FedRAMP, StateRAMP's mission is education. StateRAMP will provide proactive education, sample policies & resources for its members. The goal with documentation is to provide clear guidance with a focus on intent and purpose. An example StateRAMP's approach can be found in the published Minimum Mandatory Requirements for Ready status, which are available at www.stateramp.org/documents.

AUTHORIZED is a status that indicates the product or offering meets all the required NIST controls by impact level and the provider has completed the necessary documentation, including a 3PAO Security Assessment Report. A government sponsor is required to be listed as Authorized or Provisional.

To be Authorized, both the StateRAMP PMO and "sponsoring government" must agree the product meets the requirements to listed as Authorized. Note: You do not need to be "Ready" before "Authorized." These steps for security statuses are provided as options.

If there is a provider who meets the minimum requirements and most critical controls, but not all, a Sponsoring Government may choose to list the status as **PROVISIONAL**. The goal would be for the provider listed with a Provisional Status to work toward Authorized.

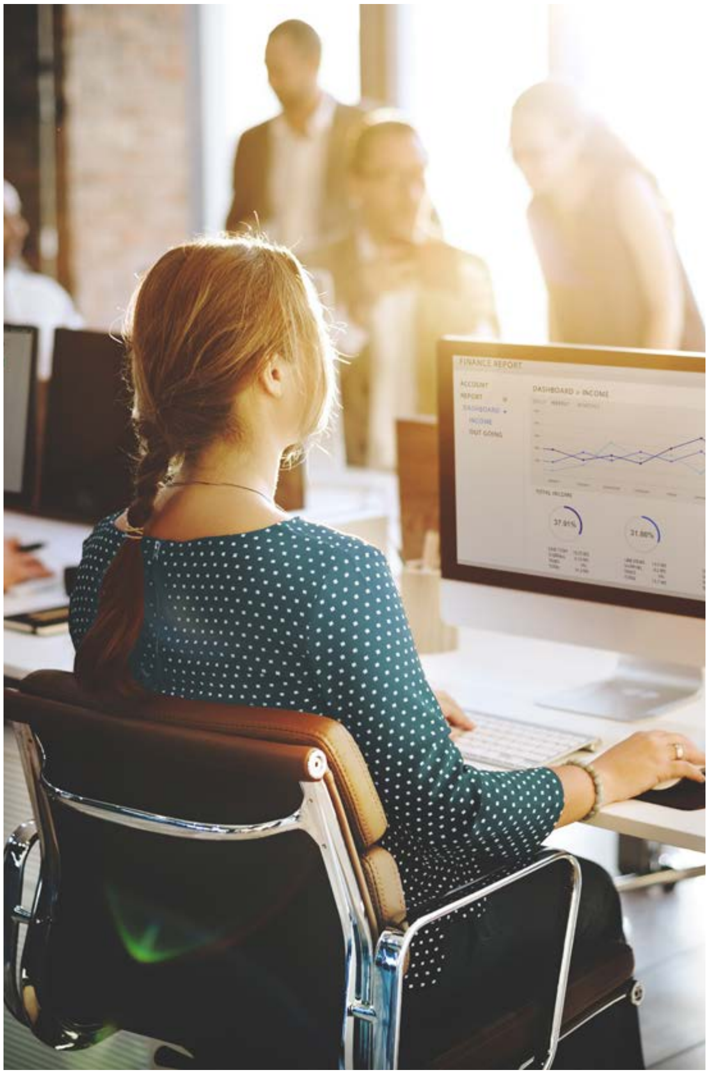
There are fees for reviewing security packages that are paid by the service provider to the StateRAMP Program Management Office (PMO) based on the security status listing that is being requested, including: $2,500 for a Ready Review, $5,000 for a Security Assessment Review, and $5,000 annually for Continuous Monitoring to maintain the listing.

StateRAMP

What does it mean to be a Sponsoring Government for a Provider?

For a vendor's offering to be listed as StateRAMP Authorized on StateRAMP's Authorized Vendor List (AVL), a government sponsor is required. Eligible government sponsors include: Any SLED (state, local, education, tribal/territorial) government official or employee with responsibility for information security may serve as a government sponsor.

Government sponsors agree to the following:



INITIAL AUTHORIZATION REVIEW

- Review the StateRAMP Program Management Office's (PMO) summary and recommendation of the service provider's security package submission.
- Make a recommendation to approve or deny authorization status. If an authorization status is denied and the provider's offering meets the minimum mandatory requirements, the sponsor may recommend Provisional status.

ONGOING

- Review and respond to the Program Management Office's (PMO) summary and recommendations for remediation as necessary.

ANNUALLY

- Review the StateRAMP PMO's summary and recommendation of the service provider's annual audit for continued authorization status.
- Make a recommendation to approve or deny continued authorization status.

FedRAMP Reciprocity

StateRAMP has developed a fast-track process for products or offerings with a FedRAMP authorization to be list on StateRAMP's Authorized Vendor List (AVL). The process for reciprocity does not require an additional audit. However, providers will need to work with the StateRAMP Program Management Office (PMO) to authenticate and provide documentation in a way that is usable by state and local governments. Additionally, the PMO will provide options to assist with the transfer of FedRAMP documentation to StateRAMP templates. Whether a provider has a FedRAMP ATO, the fees are the same for the PMO review, which include a Ready Review fee of $2500, an Authorization Review Fee of $5000 and then ongoing, annually $5000 for Continuous Monitoring.

The reciprocity for FedRAMP only applies to offerings that have a FedRAMP Ready, ATO or P-ATO status. If a provider has multiple offerings, including some that are FedRAMP Authorized and some that are not, the process for reciprocity only applies for the offerings with a FedRAMP authorization. For offerings without a FedRAMP authorization, providers will need to engage a Third Party Assessment Organization for an audit.

STEPS FOR FEDRAMP RECIPROCITY

ACCEPTED FEDRAMP STATUS

- FedRAMP Ready
- FedRAMP ATO
- FedRAMP P-ATO

REQUIRED DOCUMENTATION

- Security Packet as submitted and approved by FedRAMP
- Prior 90 days of Continuous Monitoring
- *StateRAMP Templates required

PMO REVIEW

- Call to Review Boundary and Architecture
- Review Submission
- Review Fee

Continuous Monitoring Requirements

To maintain a listing of Ready, Authorized or Provisional, the provider must comply with the Continuous Monitoring requirements, which can be found in the Continuous Monitoring Guide, published on **www.stateramp.org/documents.**

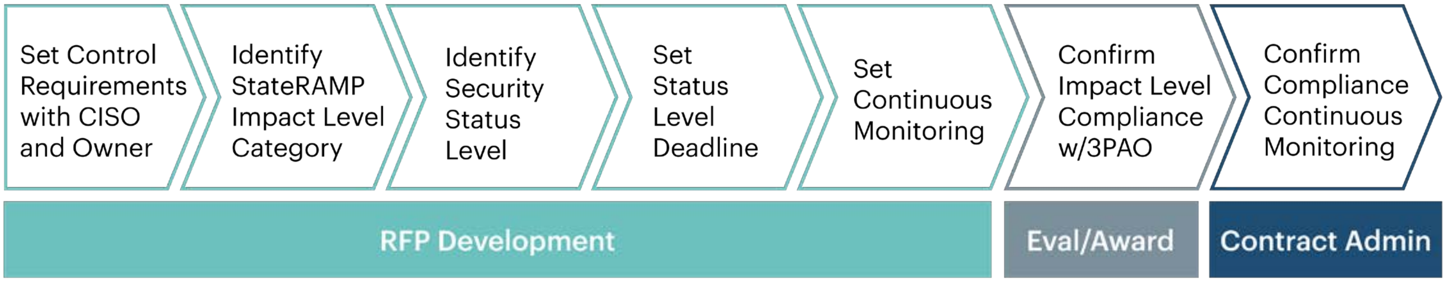
Continuous monitoring activity is centralized through the StateRAMP Program Management Office (PMO). This centralization gives service providers and governments a single point of reference. Additionally, having the PMO involved in all status reviews and in continuous monitoring ensures consistent application of standards.

StateRAMP Certified Members, who include any state or agency that requires StateRAMP verification and who has a membership agreement with StateRAMP, must assign an authorized security official to receive an account in the StateRAMP PMO secure portal to view continuous monitoring reporting for all StateRAMP listed providers with whom the state/agency has a contract, so long as the provider(s) consents. The authorized security official will also receive notification when a breach or problem arises from the StateRAMP PMO.

STATERAMP & PROCUREMENT PROCESS

StateRAMP has emphasized the need to give sufficient time for providers to attain a listing of Ready or Authorized. Some states or local governments may wish to require a provider's product be listed as StateRAMP Ready at the time of executing a contract for services. Then, they may require the provider's product be StateRAMP Authorized within 12 months of contract initiation.

See an example of how a state or agency may incorporate StateRAMP/cloud security requirements into the procurement process:


Set Control Requirements with CISO and Owner
Identify StateRAMP Impact Level Category
Identify Security Status Level
Set Status Level Deadline
Set Continuous Monitoring
Confirm Impact Level Compliance w/3PAO
Confirm Compliance Continuous Monitoring
RFP Development
Eval/Award
Contract Admin

StateRAMP

StateRAMP Membership

StateRAMP is a membership organization, with membership options for both governments and private industry.

GOVERNMENT MEMBERS

Individuals

Any SLED (state, local, education, tribal/territorial) government official or employee with responsibility for information security, information technology, privacy and/or procurement may become a member of StateRAMP. There is no fee to join. Members may join by emailing the Executive Director to indicate their interest (**leah@stateramp.org**) or completing a form at **www.stateramp.org.**

States & Agencies

States or Agencies interested in becoming a StateRAMP Certified Member at the agency or enterprise level should contact Leah McGrath at **leah@stateramp.org.**

SERVICE PROVIDERS

Service Providers and supporting organizations may join StateRAMP as a Subscriber Member for a membership fee of $500. Membership provides access to templates and resources, and the ability to list verified cloud products on the StateRAMP Authorized Vendor List (AVL). To list products on the StateRAMP Authorized Vendor List (AVL), the products must meet verification requirements that are adopted by the Board of Directors and recommended by the Standards and Technical Committee.

StateRAMP Leadership

STATERAMP LEADERSHIP

Board of Directors:

J. R. Sloan
StateRAMP President

Chief Information Officer,
State of Arizona

Ted Cotterill
StateRAMP Secr./Treas.

Chief Privacy Officer &
MPH General Counsel,
State of Indiana

Joe Bielawski
Past President

President,
Knowledge Services

STEERING COMMITTEE:

Tony Bai, Federal Practice Lead, A-LIGN

Paul Baltzell, VP of Strategy & Business Development, Salesforce

Rich Banta, Chief Information Security Officer & Data Center Architect, Lifeline Data Centers, L.L.C.

Thomas Considine, Sr., Sr. Information Security Engineer, AZRamp, State of Arizona

Curtis Dukes, Executive VP & General Manager for Security Best Practices, Center for Internet Security

Dan Lohrmann, Chief Strategist & Chief Information Security Officer, Security Mentor

Steve Nettles, Statewide Procurement Group Manager, State of Arizona

Jason Oksenhendler, Sr. Manager Cyber Risk Advisory, Coalfire

Dugan Petty, Cooperative Contract Coordinator ICT, NASPO ValuePoint

Doug Robinson, Executive Director, NASCIO

Tim Roemer, Chief Information Security Officer, State of Arizona

Jaime Schorr, Chief Procurement Officer, State of Maine

Teri Takai, Executive Director Center for Digital Government

Paul Toomey, Founder & CEO, Geographic Solutions

Jay White, Chief Information Security Officer, State of Mississippi

Owen Zorge, State Compliance & Privacy Officer, State of Arizona

Executive Director:

Leah McGrath, StateRAMP

info@stateramp.org

LEARN MORE ABOUT STATERAMP

StateRAMP will strive to continuously improve how StateRAMP meets the needs of all stakeholder to improve the cyber posture for states and local governments and the citizens they serve.

Sign up to receive updates at **www.stateramp.org** and visit **www.stateramp.org/events** for information about future events.

stateramp.org