STATERAMP SECURITY ASSESSMENT FRAMEWORK

VERSION:
1.3

DATE:
May 2021

Table of 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

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 the 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 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.

1. 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 LAUNCH

StateRAMP will open membership in early 2021 with operations to include:

- Approved and published policies, complete list of Board Members, and relevant documents made available on www.stateramp.org
- Priority for education and stakeholder communication
- Security requirements aligned with NIST 800-53 rev. 4
- A focus on Low and Moderate Impact Level security controls
- A maintained Marketplace with reciprocity for FedRAMP Authorization
- Knowledge Services to serve as Project Management Office (PMO)

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. 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 a 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 and is comprised of seven members at all times. 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 practice, 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 and is comprised of five members at all times. 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 CORPORATE COMMUNITY COMMITTEE

The Corporate Community Committee is a StateRAMP standing committee and is open to all vendors, providers, 3PAOs, and other non-governmental organizations.

Committee members will meet in person or virtually biannually to discuss and provide feedback on StateRAMP policies, documentation, and public strategic initiatives.

Information on meetings and opportunities for feedback and participation are published and maintained on www.stateramp.org.

For the duration of Pilot Program, the Corporate Community Committee will meet ad hoc as opportunities for feedback and input arise.

1.4.5 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 objectives. The PMO is also responsible for maintaining the StateRAMP Marketplace, a public website listing of StateRAMP authorized providers.

1.4.6 STATE AND LOCAL GOVERNMENTS

StateRAMP seeks to bring together states 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 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.

1.4.7 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.

1.4.8 SERVICE PROVIDERS

Service providers offering cloud computing services that have transformed business operations across state and local governments 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:

- Transferable certificates and credentials
- 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 StateRAMP Marketplace found at www.stateramp.org. Providers who have achieved FedRAMP Authorization will be inherited and recognized at the appropriate security impact level by StateRAMP.

2. STATERAMP REQUIREMENTS

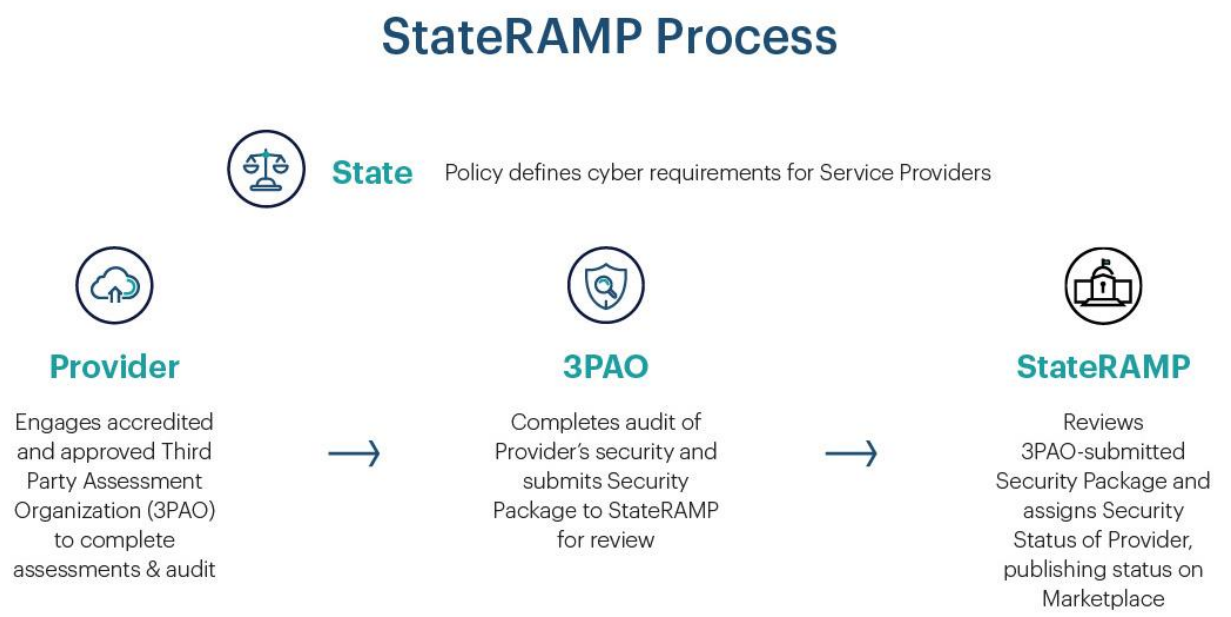
As more state and local governments have transitioned to cloud computing environments, data protection and cybersecurity remain top priorities.

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.

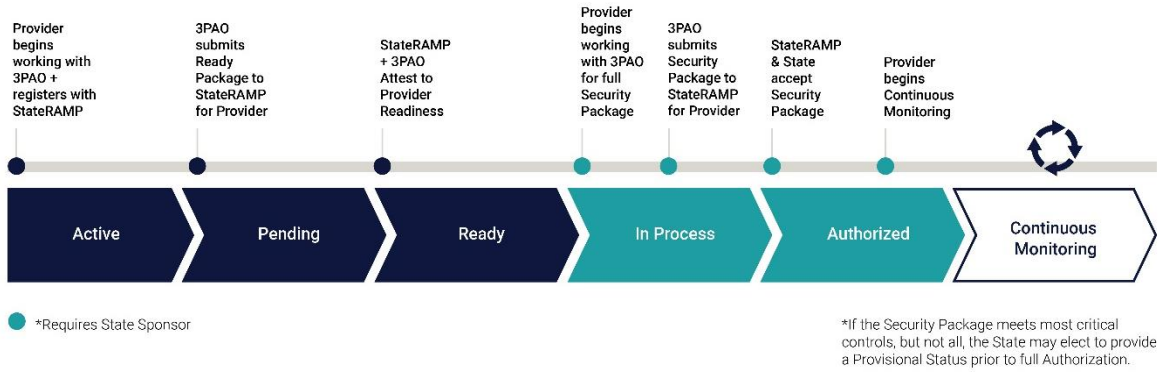


Throughout the duration of the Pilot Program, StateRAMP will work with cybersecurity experts, States, and providers to identify the most applicable impact levels for state and local governments.

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.

2.1 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 state or local government 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) State and StateRAMP PMO can attest the provider meets minimum security controls. Once a provider achieves authorization, continuous monitoring is required to maintain the status. Continuous monitoring begins upon authorization. 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.

State and local governments may choose to require StateRAMP or FedRAMP Authorizations upon issuing RFPs that involved cloud solutions when issuing direct contracts or may choose to require authorization for current vendors as desired.

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 Marketplace at www.stateramp.org. FedRAMP Authorization will be inherited and recognized at the appropriate security impact level by StateRAMP. While StateRAMP will recognize FedRAMP Authorizations at the similar appropriate security impact level, FedRAMP does not recognize StateRAMP Authorizations.

2.2 AUTHORIZED VENDOR LIST

The StateRAMP Authorized Vendor List displaying a provider's impact level and status will be maintained and published at www.stateramp.org. FedRAMP Authorization will be inherited and recognized at the appropriate security impact level by StateRAMP.

2.3 USING A PROVIDER NOT LISTED ON THE AUTHORIZED VENDOR LIST

Best practice when using cloud providers is to assess risk up front and with continuous monitoring. Using a provider on the StateRAMP Authorized Vendor List or FedRAMP Marketplace ensures 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.

3. STATERAMP SECURITY ASSESSMENT FRAMEWORK

StateRAMP's Security Assessment Framework process is modeled after the NIST Risk Framework Management, upon which FedRAMP is also modeled. Figure 1 below can be found in NIST SP 800-60 Vol. 1 Rev. 1.

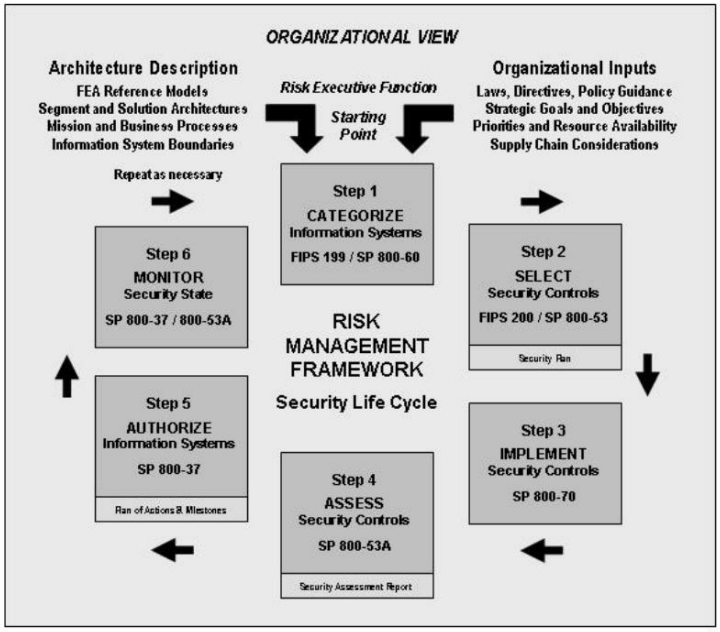


Figure 1: NIST Risk Management Framework

3.1 DOCUMENT

3.1.1 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:

Category 1: Aligned with Low Impact, based on FedRAMP Low Control Baselines
Category 2: Aligned with Low/Moderate Impact, adapted from FedRAMP Low and Moderate Control Baselines
Category 3: 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 Marketplace so that providers can benefit from the higher authorization indicating an ability to comply with more rigorous standards.

StateRAMP will provide a Data Classification Tool to 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 will be published and maintained on www.stateramp.org.

3.1.2 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 alternative implementations that demonstrate the implementation satisfies the intent of the control requirement. For any control that cannot be met, providers must provide justification for not being able to implement the control.

3.1.3 SYSTEM SECURITY PLAN

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

3.2 ASSESS

3.2.1 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. A listing of FedRAMP Authorized 3PAOs can be found at www.fedramp.gov.

3.2.2 COMPLETE THE READINESS ASSESSMENT PLAN

The StateRAMP SR-RAR is developed by the 3PAO. The StateRAMP Ready Status indicates that a 3PAO attests to a provider's readiness for the authorization process, and that a StateRAMP SR-RAR has been reviewed and approved by the StateRAMP PMO. 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.

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.

3.2.3 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 will be published at www.stateramp.org.

3.3 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.

3.3.1 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.

3.3.2 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.

3.3.3 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
- Security Controls Template 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 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.

3.3.4 RECOGNITION OF STATUS

A provider's security status will be published and maintained on the StateRAMP Marketplace at www.stateramp.org. StateRAMP will provide a badge to providers for marketing use when a milestone status is obtained, including Ready, Provisional and Authorized. FedRAMP Authorization will be inherited and recognized at the appropriate security impact level by StateRAMP. Conversely, FedRAMP does not recognize StateRAMP Authorizations.

3.3.5 LEVERAGING 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 providers 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.

3.3.6 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, the PMO will notify all relevant stakeholders and update the Marketplace accordingly.

3.4 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.

3.4.1 OPERATIONAL VISIBILITY

The StateRAMP Continuous Monitoring Plan will be published at www.stateramp.org, including:

- Monthly mitigation response
- Quarterly update to the POA&M
- Annual 3PAO audit and testing

The StateRAMP PMO will provide all submitted reports and artifacts, 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.

3.4.2 CHANGE CONTROLS

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 audit by the 3PAO should note any other changes and affected security controls.

3.4.3 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 providers 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

STATERAMP SECURITY CONTROLS BASELINE SUMMARY

StateRAMP developed the baseline with input from government and private industry stakeholders and security experts. It is the goal of the StateRAMP to help mature and grow the provider community and in doing so, improve the security profile for state and local government. StateRAMP will verify along with third party assessment organization reports that the providers meets the intent of the security requirements as appropriate and fit for purpose.

All of the security controls listed in the table below are listed in NIST 800-53 Rev. 4. StateRAMP's Category 1 aligns with the controls required for FedRAMP Low Impact. StateRAMP's Category 3 aligns with the controls required for FedRAMP Moderate Impact. Category 2 is in development stages and once launched, is intended to provide flexibility for states and local governments.

ID	Control Description	Sensitivity Level			
		Low / Cat. 1	Low + / Cat. 2	Mod. / Cat. 3	High (FedRAMP)
AC	**Access Control**				
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1	AC-1
AC-2	Account Management *Only required for privileged accounts	AC-2	AC-2 (1) (4 (12) (7*)	AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12)	AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (11) (12) (13)
AC-3	Access Enforcement	AC-3	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4 (21)	AC-4 (8) (21)
AC-5	Separation of Duties	Not Selected	AC-5	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (7) (8) (9) (10)
AC-7	Unsuccessful Logon Attempts	AC-7	AC-7	AC-7	AC-7 (2)
AC-8	System Use Notification	AC-8	AC-8	AC-8	AC-8
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11 (1)	AC-11 (1)
AC-12	Session Termination *Only required for admin. back-end access	Not Selected	AC-12*	AC-12	AC-12 (1)
AC-14	Permitted Actions Without Identification or Authentication	AC-14	AC-14	AC-14	AC-14
AC-17	Remote Access	AC-17	AC-17 (1) (2) (9)	AC-17 (1) (2) (3) (4) (9)	AC-17 (1) (2) (3) (4) (9)
AC-18	Wireless Access *Only required for on-	AC-18*	AC-18	AC-18 (1)	AC-18 (1) (3) (4) (5)

ID	Control Description	Sensitivity Level			
		Low / Cat. 1	Low + / Cat. 2	Mod. / Cat. 3	High (FedRAMP)
	premise solutions, so long as SaaS/PaaS host meets requirements				
AC-19	Access Control For Mobile Devices	AC-19	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	AC-20	AC-20 (1)	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	Not Selected	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content *FedRAMP requires AC-22 for Low Impact. It is not required as a baseline control for StateRAMP.	Not Selected*	Not Selected	AC-22	AC-22
AT	**Awareness and Training**				
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	AT-2	AT-2 (2)	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	AT-3	AT-3	AT-3	AT-3 (3) (4)
AT-4	Security Training Records	AT-4	AT-4	AT-4	AT-4
AU	**Audit and Accountability**				
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1	AU-1
AU-2	Audit Events	AU-2	AU-2 (3)	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	AU-3	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis and Reporting	AU-6	AU-6 (1)	AU-6 (1) (3)	AU-6 (1) (3) (4) (5) (6) (7) (10)
AU-7	Audit Reduction and Report Generation	Not Selected	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8 (rec. (1))	AU-8 (1)	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9 (2) (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	Not Selected	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	AU-11	AU-11	AU-11	AU-11

ID	Control Description	Sensitivity Level			
		Low / Cat. 1	Low + / Cat. 2	Mod. / Cat. 3	High (FedRAMP)
AU-12	Audit Generation *AU-12 is required by FedRAMP for Low and Moderate Impact Levels. It is not required as a baseline control for StateRAMP.	Not Selected*	Not Selected	Not Selected *	AU-12 (1) (3)
CA	**Security Assessment and Authorization**				
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2 (1)	CA-2 (1)	CA-2 (1) (2) (3)	CA-2 (1) (2) (3)
CA-3	System Interconnections	CA-3	CA-3	CA-3 (3) (5)	CA-3 (3) (5)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5	CA-5
CA-6	Security Authorization	CA-6	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7 (1)	CA-7 (1)	CA-7 (1) (3)
CA-8	Penetration Testing *Note: Recommend CA-8 (1) every 2 years or when a significant change occurs.	Not Selected	CA-8 (1)*	CA-8 (1)	CA-8 (1)
CA-9	Internal System Connections	CA-9	CA-9	CA-9	CA-9
CM	**Configuration Management**				
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1) (3)	CM-2 (1) (2) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	Not Selected	CM-3 (2)	CM-3 (2)	CM-3 (1) (2) (4) (6)
CM-4	Security Impact Analysis	CM-4	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions For Change	Not Selected	CM-5	CM-5 (1) (3) (5)	CM-5 (1) (2) (3) (5)
CM-6	Configuration Settings	CM-6	CM-6 (1)	CM-6 (1)	CM-6 (1) (2)
CM-7	Least Functionality	CM-7	CM-7	CM-7 (1) (2) (5)*	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	CM-8	CM-8 (1)	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration	Not Selected	CM-9	CM-9	CM-9

ID	Control Description	Sensitivity Level			
		Low / Cat. 1	Low + / Cat. 2	Mod. / Cat. 3	High (FedRAMP)
	Management Plan				
CM-10	Software Usage Restrictions *Note: CM-10 is required by FedRAMP for Low Impact. It is not required as a baseline control for StateRAMP.	Not Selected*	CM-10	CM-10 (1)	CM-10 (1)
CM-11	User-Installed Software	CM-11	CM-11	CM-11	CM-11 (1)
CP	**Contingency Planning**				
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (8)	CP-2 (1) (2) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	CP-3	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	CP-4	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-6	Alternate Storage Site	Not Selected	CP-6	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	CP-8	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1)	CP-9 (1) (3)	CP-9 (1) (2) (3) (5)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10 (2)	CP-10 (2)	CP-10 (2) (4)
IA	**Identification and Authentication**				
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users) *Note: IA-2 (12) is required by FedRAMP for Low Impact. It is not required as a baseline control for StateRAMP.	IA-2 (1)*	IA-2 (1) (11) (i.e. for (11) make it text message, etc.)	IA-2 (1) (2) (3) (5) (8) (11) (12)	IA-2 (1) (2) (3) (4) (5) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	Not Selected	Not Selected	IA-3	IA-3

ID	Control Description	Sensitivity Level			
		Low / Cat. 1	Low + / Cat. 2	Mod. / Cat. 3	High (FedRAMP)
IA-4	Identifier Management	IA-4	IA-4	IA-4 (4)	IA-4 (4)
IA-5	Authenticator Management	IA-5 (1) (11)	IA-5 (1) (11)	IA-5 (1) (2) (3) (4) (6) (7) (11)	IA-5 (1) (2) (3) (4) (6) (7) (8) (11) (13)
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users) *Optional for states to require IA-8 (1) (2) (3) (4) when applicable	Not Selected*	Not Selected*	Not Selected*	IA-8 (1) (2) (3) (4)
IR	**Incident Response**				
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	IR-2	IR-2	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing *Recommend Tabletop Exercise for Cat. 1 and Small Scale Functional Exercise for Category 2.	Not Selected*	Not Selected*	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	IR-4	IR-4	IR-4 (1)	IR-4 (1) (2) (3) (4) (6) (8)
IR-5	Incident Monitoring	IR-5	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (2)	IR-7 (1) (2)	IR-7 (1) (2)
IR-8	Incident Response Plan	IR-8	IR-8	IR-8	IR-8
IR-9	Information Spillage Response *Recommend a modified requirement for IR-9	Not Selected*	IR-9 (1)	IR-9 (1) (2) (3) (4)	IR-9 (1) (2) (3) (4)
MA	**Maintenance** Note: Many of these controls are inherited if the system resides on public IaaS				
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1	MA-1

ID	Control Description	Sensitivity Level			
		Low / Cat. 1	Low + / Cat. 2	Mod. / Cat. 3	High (FedRAMP)
MA-2	Controlled Maintenance	MA-2	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools		MA-3 (1)	MA-3 (1) (2) (3)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	MA-4	MA-4	MA-4 (2)	MA-4 (2) (3) (6)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5 (1)	MA-5 (1)
MA-6	Timely Maintenance *MA-6 recommended for all categories if on-premise solution	Not Selected*	MA-6*	MA-6	MA-6
MP	**Media Protection** Note: Many of these controls are inherited if the system resides on public IaaS				
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2	MP-2	MP-2
MP-3	Media Marking *MP-3 is recommended for all categories if on-premise solution	Not Selected*	MP-3*	MP-3	MP-3
MP-4	Media Storage *MP-4 is recommended for all categories if on-premise solution	Not Selected*	MP-4*	MP-4	MP-4
MP-5	Media Transport *MP-5 is recommended for all categories if on-premise solution	Not Selected*	MP-5*	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization *MP-6 (2) is required by FedRAMP for Moderate Impact	MP-6	MP-6 (1)	MP-6 (1)*	MP-6 (1) (2) (3)
MP-7	Media Use *Optional for states to require MP-7.	Not Selected*	Not Selected*	Not Selected*	MP-7 (1)

ID	Control Description	Sensitivity Level			
		Low / Cat. 1	Low + / Cat. 2	Mod. / Cat. 3	High (FedRAMP)
	FedRAMP requires MP-7 for Low Impact and MP-7 (1) for Moderate Impact				
PE	**Physical and Environmental Protection** Note: Many of these controls are inherited if the system resides on public IaaS. Additionally, the goal is to ensure service providers meet the intent of the requirements. For example, a fire extinguisher on site would suffice for PE-13.				
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3	PE-3 (1)
PE-4	Access Control For Transmission Medium *Note: this is a shared responsibility between the government and service provider.	Not Selected	PE-4	PE-4	PE-4
PE-5	Access Control For Output Devices	Not Selected	PE-5	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6	PE-6 (1)	PE-6 (1) (4)
PE-8	Visitor Access Records	PE-8	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and Cabling	Not Selected	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	Not Selected	PE-10	PE-10
PE-11	Emergency Power	Not Selected	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting *PE-12 is required by FedRAMP for Low Impact. It is not required as a baseline control for StateRAMP.	Not Selected*	Not Selected	PE-12	PE-12
PE-13	Fire Protection	PE-13*	PE-13*	PE-13 (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14*	PE-14*	PE-14 (2)	PE-14 (2)

ID	Control Description	Sensitivity Level			
		Low / Cat. 1	Low + / Cat. 2	Mod. / Cat. 3	High (FedRAMP)
	*Evaluation will ensure it meets the intent of the requirements				
PE-15	Water Damage Protection *Evaluation will ensure it meets the intent of the requirements	PE-15*	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal (i.e. loading dock areas) *Focus of this intent is to verify the service provider is process-oriented and identified authorized personnel.	PE-16*	PE-16*	PE-16	PE-16
PE-17	Alternate Work Site (i.e. secure VPN)	Not Selected	PE-17	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	Not Selected	Not Selected	PE-18
PL	**Planning**				
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2	PL-2 (3)	PL-2 (3)
PL-4	Rules of Behavior	PL-4	PL-4	PL-4 (1)	PL-4 (1)
PL-8	Information Security Architecture	Not Selected	PL-8	PL-8	PL-8
PS	**Personnel Security (combining HR with IT)**				
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1	PS-1
PS-2	Position Risk Designation *PS-2 is required by FedRAMP for Low / Moderate Impact Levels. It is not required as a baseline control for StateRAMP.	Not Included*	Not Included	Not Included*	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3	PS-3 (3)
PS-4	Personnel Termination	PS-4	PS-4	PS-4	PS-4 (2)
PS-5	Personnel Transfer	PS-5	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel	PS-7	PS-7	PS-7	PS-7

ID	Control Description	Sensitivity Level			
		Low / Cat. 1	Low + / Cat. 2	Mod. / Cat. 3	High (FedRAMP)
	Security				
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8	PS-8
RA	**Risk Assessment**				
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3	RA-3
RA-5	Vulnerability Scanning	RA-5	RA-5	RA-5 (1) (2) (3) (5) (6) (8)	RA-5 (1) (2) (3) (4) (5) (6) (8) (10)
SA	**System and Services Acquisition**				
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	SA-3	SA-3	SA-3	SA-3
SA-4	Acquisition Process *SA-4 (1) is required by FedRAMP for Low Impact. SA-4 (2) (8) (9) (10) are required by FedRAMP for Moderate Impact. They not required as a baseline control for StateRAMP.	Not Selected *	Not Selected *	SA-4 (1)*	SA-4 (1) (2) (8) (9) (10)
SA-5	Information System Documentation	SA-5	SA-5	SA-5	SA-5
SA-8	Security Engineering Principles	Not Selected	Not Selected	SA-8	SA-8
SA-9	External Information System Services *SA-9 (4) (5) are required by FedRAMP for Moderate Impact. They are not required as a baseline control for StateRAMP.	SA-9	SA-9 (1) (2)	SA-9 (1) (2)*	SA-9 (1) (2) (4) (5)
SA-10	Developer Configuration Management	Not Selected	Not Selected	SA-10 (1)	SA-10 (1)
SA-11	Developer Security Testing and Evaluation	Not Selected	SA-11	SA-11 (1) (2) (8)	SA-11 (1) (2) (8)
SA-12	Supply Chain	Not Selected	Not Selected	Not Selected	SA-12

ID	Control Description	Sensitivity Level			
		Low / Cat. 1	Low + / Cat. 2	Mod. / Cat. 3	High (FedRAMP)
	Protection				
SA-15	Development Process, Standards and Tools	Not Selected	Not Selected	Not Selected	SA-15
SA-16	Developer-Provided Training	Not Selected	Not Selected	Not Selected	SA-16
SA-17	Developer Security Architecture and Design	Not Selected	Not Selected	Not Selected	SA-17
SC	**System and Communications Protection**				
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected	Not Selected	SC-3
SC-4	Information In Shared Resources	Not Selected	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5	SC-5
SC-6	Resource Availability	Not Selected	Not Selected	SC-6	SC-6
SC-7	Boundary Protection	SC-7	SC-7 (5) (7) (12) (13)	SC-7 (3) (4) (5) (7) (8) (12) (13) (18)	SC-7 (3) (4) (5) (7) (8) (10) (12) (13) (18) (20) (21)
SC-8	Transmission Confidentiality and Integrity	Not Selected	SC-8	SC-8 (1)	SC-8 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10	SC-10
SC-12	Cryptographic Key Establishment and Management	SC-12	SC-12	SC-12 (2) (3)	SC-12 (1) (2) (3)
SC-13	Cryptographic Protection	SC-13	SC-13	SC-13	SC-13
SC-15	Collaborative Computing Devices *SC-15 is required by FedRAMP for Low and Moderate Impact Levels. It is not required as a baseline control for StateRAMP.	Not Selected*	Not Selected	Not Selected*	SC-15
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17	SC-17

ID	Control Description	Sensitivity Level			
		Low / Cat. 1	Low + / Cat. 2	Mod. / Cat. 3	High (FedRAMP)
SC-18	Mobile Code	Not Selected	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	Not Selected	SC-19	SC-19
SC-20	Secure Name / Address Resolution Service (Authoritative Source)	SC-20	SC-20	SC-20	SC-20
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	SC-21	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name / Address Resolution Service	SC-22	SC-22	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	Not Selected	SC-23	SC-23 (1)
SC-24	Fail in Known State	Not Selected	Not Selected	Not Selected	SC-24
SC-28	Protection of Information At Rest	Not Selected	SC-28	SC-28 (1)	SC-28 (1)
SC-39	Process Isolation	SC-39	SC-39	SC-39	SC-39
SI	**System and Information Integrity**				
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2	SI-2 (2) (3)	SI-2 (1) (2) (3)
SI-3	Malicious Code Protection	SI-3	SI-3	SI-3 (1) (2) (7)	SI-3 (1) (2) (7)
SI-4	Information System Monitoring	SI-4	SI-4	SI-4 (1) (2) (4) (5) (14) (16) (23)	SI-4 (1) (2) (4) (5) (11) (14) (16) (18) (19) (20) (22) (23) (24)
SI-5	Security Alerts, Advisories and Directives	SI-5	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	Not Selected	Not Selected	SI-6	SI-6
SI-7	Software, Firmware and Information Integrity	Not Selected	SI-7	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Spam Protection *If email is in boundary, SI-8 is not required	Not Selected	SI-8*	SI-8 (1) (2)	SI-8 (1) (2)
SI-10	Information Input Validation	Not Selected	SI-10	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11	SI-11
SI-12	Information Handling	SI-12	SI-12	SI-12	SI-12

ID	Control Description	Sensitivity Level			
		Low / Cat. 1	Low + / Cat. 2	Mod. / Cat. 3	High (FedRAMP)
	and Retention				
SI-16	Memory Protection	SI-16	SI-16	SI-16	SI-16

Find the StateRAMP Security Controls Baseline Summary at www.stateramp.org/documents.

APPENDIX B

MINIMUM MANDATORY REQUIREMENTS FOR READY STATUS

Achieving Ready Status

To achieve Ready Status, a Service Provider must meet the minimum mandatory requirements outlined in this document. The minimum mandates are the same across all impact levels.

Templates and Guidance will be maintained and published on www.stateramp.org.

#	StateRAMP Ready Minimum Mandates	Compliant?		
		Yes	No	N/A
1	Are modern cryptographic modules consistently used where cryptography is required? Data at Rest [SC-28] Transmission [SC-8 (1), SC-12, SC-12(2, 3)] Remote Access [AC-17 (2)] Authentication [IA-5 (1)] Digital Signatures/Hash [CM-5 (3)] AES-256 AES-128 TLS 1.1 (Compliant) TLS 1.2 (Compliant)			
2	Can the system support Single Sign On (SSO/SAML)? [IA-08]			
3	Does the service provider scan for and consistently remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days, and Low vulnerabilities within 180 days? [RA-5] Required: Credentialed scan shall be used on all devices and validated that credentials work properly.			
4	Do you scan for configuration settings on systems in the environment? [CM-6]			
5	Does the service provider's system utilize and audit and event monitoring solution (SIEM) that can support 90 days of online storage and 365 days of event/log data? [AU-2, AU-3, AU-8, AU-11] SIEM is preferred, but some form of log aggregation is required			
6	Does the system's external DNS solution support DNS Security (DNSSEC) to provide origin authentication and integrity verification assurances? [SC-20, SC-21]			
7	Does the system ensure secure separation of customer data? [SC-4]			
8	Does the system have the capability to detect, contain, and eradicate malicious software? [SI-3, SI-3 (1), SI-3 (2), SI-3 (7), MA-3 (2)]			

#	StateRAMP Ready Minimum Mandates	Compliant?		
		Yes	No	N/A
9	Does the system protect audit information from unauthorized access, modification, and deletion? [AU-7, AU-9]			
10	Does the service provider have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? [CP-2, CP-2 (2), CP-2 (3), CP-9, CP-10]			
11	Does the service provider maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8]			
12	Does the service provider follow a formal change control process that includes a security impact assessment? [CM-3, CM-4] Expectation: Automated Include examples of acceptable criteria – SharePoint, excel			
13	Does the service provider employ automated mechanisms to detect inventory and configuration changes? [CM-2(2), CM-6(1), CM-8(3)]			
14	Does the service provider prevent unauthorized changes to the system? [CM-5, CM-5(1), CM-5(5)]			
15	Does the system require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2(1), IA-2(3)]			
16	Does the service provider have an Incident Response Plan and Incident Response Testing Plan [IR-3] [IR-8] (SR Template)			
17	Does the service provider have a Configuration Management Plan? [CM-9, CM-11]			
18	Does the service provider have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with NIST Special Publication 800-34? [CP-2, CP-8]			
19	Do you conduct code analysis for internally-developed code? [SA-11]			
20	Does the service provider restrict physical system access to only authorized personnel? [PE-2 through PE-6, PE-8]			
21	Does the service provider monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8]			
22	Does the service provider monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6 (1)]			
23	Does the system have or use alternate telecommunications providers? [CP-8, CP-8 (2)] If on SR/FR IaaS (N/A), if in non-authorized IaaS, they will have to gather this info from the IaaS			
24	Does the system have backup power generation or other redundancy? [PE-11]			
25	Does the service provider have service level agreements (SLAs) in place with all telecommunications providers? [CP-8 (1)]			

To achieve Ready Status, a Service Provider must have the required Ready Documentation.

#	StateRAMP Required Ready Documentation	Completed?		
		Yes	No	N/A
1	Boundary Diagram			
2	StateRAMP Inventory Worksheet			
3	Roles & Permissions Matrix			

To achieve Ready Status, a Service Provider must complete, at minimum, 50% or 21 of the StateRAMP Documents.

#	StateRAMP Documentation (Minimum of 50% Documents Must be Completed for Ready)	Compliant?		
		Yes	No	N/A
1	System Security Plan (SSP)			
2	Incident Response Plan			
3	Information System Contingency Plan			
4	Configuration Management Plan			
5	Rules of Behavior			
6	Control Implementation Summary			
7	Continuous Monitoring Plan			
8	Security Policy – Access Control (AC)			
9	Security Policy – Awareness & Training (AT)			
10	Security Policy – Audit & Accountability (AU)			
11	Security Policy – Security Assessment & Authorization (CA)			
12	Security Policy – Configuration Management (CM)			
13	Security Policy – Contingency Planning (CP)			
14	Security Policy – Identification & Authentication (IA)			
15	Security Policy – Incident Response (IR)			
16	Security Policy – Maintenance (MA)			
17	Security Policy – Media Protection (MP)			
18	Security Policy – Personnel Security (PS)			
19	Security Policy – Physical & Environmental (PE)			
20	Security Policy – Planning (PL)			
21	Security Policy – Risk Assessment (RA)			

#	StateRAMP Documentation (Minimum of 50% Documents Must be Completed for Ready)	Compliant?		
		Yes	No	N/A
22	Security Policy – Systems & Services Acquisition (SA)			
23	Security Policy – Systems & Communications Protection (SC)			
24	Security Policy – Systems & Information Integrity (SI)			
25	Security Procedure – Access Control (AC)			
26	Security Procedure – Awareness & Training (AT)			
27	Security Procedure – Audit & Accountability (AU)			
28	Security Procedure – Security Assessment & Authorization (CA)			
29	Security Procedure – Configuration Management (CM)			
30	Security Procedure – Contingency Planning (CP)			
31	Security Procedure – Identification & Authentication (IA)			
32	Security Procedure – Incident Response (IR)			
33	Security Procedure – Maintenance (MA)			
34	Security Procedure – Media Protection (MP)			
35	Security Procedure – Personnel Security (PS)			
36	Security Procedure – Physical & Environmental (PE)			
37	Security Procedure – Planning (PL)			
38	Security Procedure – Risk Assessment (RA)			
39	Security Procedure – Systems & Services Acquisition (SA)			
40	Security Procedure – Systems & Communications Protection (SC)			
41	Security Procedure – Systems & Information Integrity (SI)			

APPENDIX C

SAMPLE RFP OR CONTRACTUAL LANGUAGE FOR STATES

State and local governments may incorporate the following or similar language into RFPs and/or contracts with providers or vendors using a cloud system that processes, stores and/or transmits government data.)

SECURITY FRAMEWORK & CONTRACTOR REQUIREMENTS

The State information security policies and standards adhere to the National Institute of Standards and Technology (NIST) 800-53 revision 4.

A contract will not be executed with a contractor that utilizes a cloud system to process, store and/or transmit government data, unless and until the service provider has achieved FedRAMP or StateRAMP Ready Status. The Ready Status serves as an attestation to the providers capabilities to achieve full authorization.

The State requires all cloud systems that process, store and/or transmit government data must demonstrate compliance with NIST 800-53 revision 4 by achieving FedRAMP or StateRAMP authorization within 12 months of contract execution for the appropriate data classification.

Once a contract is issued, the provider must achieve full FedRAMP or StateRAMP authorization within 12 months. All contractors must comply with required continuous monitoring to maintain FedRAMP and StateRAMP authorizations.

The State reserves the right to request and review all Third Party Assessment Organization (3PAO) audits, risk assessments, vulnerability assessments, penetration tests, of the contractor's environment. The contractor shall respond to all serious flaws discovered by providing an acceptable timeframe to resolve the issue and/or implement a compensating control.

Any deviation from these requirements must be approved by the Chief Information Officer. Information about FedRAMP can be found at www.fedramp.gov. Information about StateRAMP can be found at www.stateramp.org.

APPENDIX D

DATA CLASSIFICATION TOOL

This document can be found at www.stateramp.org/documents and is intended to be used by state governments and procurement officials as a tool for determining the appropriate StateRAMP or FedRAMP security requirements in a request for proposals (RFP) with the intent of procuring a service provider using or offering IaaS, SaaS, and/or PaaS solutions that processes, stores, and/or transmits government data including PII, PHI, and/or PCI.

According to the Federal Information Security Management Act (FISMA) requirements, there are three distinct security objectives for information and information systems: confidentiality, integrity, and availability. These standards are used as the foundation to ensure service providers are providing solutions that meet the minimum security requirements to process, store, and transmit certain types of government data.

It is necessary for States to accurately determine their required security baseline prior to publishing an RFP so that the State can select a service provider that meets the State's needs and provides the appropriate security controls to protect the State's data. This data classification self-assessment is based on the NIST 800-5 Revision 4 requirements and designed to help state and local governments easily identify the appropriate StateRAMP security category to include in an RFP.

INSTRUCTIONS

Answer the questions in the survey section to determine what StateRAMP security category requirements you need to include in your RFP to ensure your data is protected. Because of the level of reciprocity between StateRAMP and FedRAMP, a StateRAMP Category 1 requirement is equivalent to a FedRAMP Low Impact and a StateRAMP Category 3 requirement is equivalent to a FedRAMP Moderate Impact.

SURVEY QUESTIONS

1. Will the service provider process, transmit, and/or store non-sensitive State data, metadata, and/or data that may be released to the public that requires no additional levels of protection?
    a. If yes, StateRAMP Category 1 is required.
2. Will the service provider process, transmit, and/or store personally identifiable information (PII) as defined by the U.S. Department of Labor (DOL)?
    a. If yes, StateRAMP Category 3 is required.
3. Will the service provider process, transmit, and/or store protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA)?
    a. If yes, StateRAMP Category 3 is required.
4. Will the service provider process, transmit, and/or store payment card industry (PCI) data as defined by the PCI Security Standards Council (PCI SSC)?
    a. If yes, StateRAMP Category 3 is required.
5. Will the loss or unavailability of the data that is processed, transmitted, and/or stored by the service provider result in a disruption to government operations?

   a. If yes, StateRAMP Category 3 is required.

6. Will the loss or unavailability of the data that is processed, transmitted, and/or stored by the service provider result in a loss of confidence or trust in the government?
   a. If yes, StateRAMP Category 3 is required.
7. Will the service provider process, transmit, and/or store criminal justice information (CJI), foreign affairs information, federal critical infrastructure information, national security information, and/or global trade information?
   a. If yes, FedRAMP High Impact is required.

NEXT STEPS

Remember that data processed, transmitted, and/or stored by the service provider includes information shared inside and outside of the provider's cloud service application. Similarly, if state or local laws have identified any other data type not included in the survey above as confidential, a StateRAMP Category 3 is required. Once a determination has been made regarding the appropriate StateRAMP or FedRAMP security category that should be required from service providers, be sure to partner with the information security team, Chief Information Officer, and Chief Information Security Officer to ensure the appropriate standards have been met.

APPENDIX E

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
Marketplace	Directory of providers with StateRAMP Security Status, FedRAMP marketplace inherited

APPENDIX F

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.