STATERAMP CONTINUOUS MONITORING AND IMPROVEMENT GUIDE

VERSION:
1.1

DATE:
January 2021

TABLE OF CONTENTS

1. DOCUMENT REVISION HISTORY

Date	Description	Version	Governance Body
10/29/2020	Original Publication	1.0	StateRAMP Steering Committee
1/08/2021	Language updates	1.1	StateRAMP Staff

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

2. PURPOSE

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and analyze security controls and information security related risks at a frequency sufficient to support organizational risk-based decisions.

Monitoring security controls is part of the overall risk management framework for information security and the service provider is required to maintain a security authorization that meets the StateRAMP requirements. Performing ongoing security assessments determines whether the set of deployed security controls in a cloud system remains effective considering new exploits and attacks and planned and unplanned changes that occur in the system and its environment over time.

To maintain an authorization that meets StateRAMP requirements, the service 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 assessment of security controls results in greater control over the security posture of the service provider's system and enables timely risk-management decisions. Security-related information collected through continuous monitoring is used to make recurring updates to the security assessment package.

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

3. ROLES AND RESPONSIBILITIES

3.1 SERVICE PROVIDER

When a service provider has achieved a StateRAMP Authorized status, the service provider's security posture is monitored according to the assessment and authorization process. It is the responsibility of the service provider to partner with a StateRAMP certified third party assessment organization (3PAO) to allow for required monitoring requirements.

3.2 STATERAMP PMO

StateRAMP oversees and conducts analysis on the service provider's continuous monitoring activities and provides information and may advise the State Authorizing Body, who maintains the responsibility on behalf of the State for continuous monitoring in relation to their contract.

3.3 GOVERNMENT AUTHORIZING BODY

State refers to state or local government bodies contracting with service providers who provide and/or use a SaaS, PaaS, or IaaS solution involving the storage, processing, and/or transmitting of government data including PII, PHI, and/or PCI.

The State Authorizing Body manages the review and approval of all continuous monitoring artifacts submitted by the service provider on behalf of the State. The State must review all security artifacts

provided by the service provider, 3PAO, or StateRAMP PMO to ensure the service provider's security posture meets requirements for the State's use of the system.

State Authorizing Bodies should ensure their State is monitoring the Plan of Action & Milestones (POA&M) and reporting artifacts as well as any significant changes associated with the service provider's service offering. States should use this information to make risk-based decisions about ongoing authorization of the system for the State.

3.4 THIRD PARTY ASSESSMENT ORGANIZATION (3PAO)

3PAOs are responsible for independently verifying and validating the control implementation and test results for service providers for continuous monitoring. 3PAOs are responsible for:

- Submitting the assessment report to StateRAMP one year after the service provider's authorization date and each year thereafter
- Perform announced penetration testing annually
- Perform annual scans of web applications, databases, and operating systems
- Assess change controls on an ad hoc basis as requested by StateRAMP or the State authorizing body for any changes made to the system by the service provider
- Conduct an annual review of subset of security controls

To be effective in this role, 3PAOs are responsible for ensuring that the chain of custody is maintained for any 3PAO-authored documentation. 3PAOs must also be able to vouch for the veracity and integrity of data provided by the service provider for inclusion in 3PAO-authored documentation.

- If scans are performed by the service provider, the 3PAO must either be on site and observe the service provider performing the scans or be able to monitor or verify the results of the scans through other means documented and approved by the State Authorizing Body.

3.5 STANDARDS AND TECHNICAL COMMITTEE

As outlined in the StateRAMP Bylaws Article VI Section 9, the Standards and Technical Committee will consult the PMO on policies, security standards, etc. This committee will have the following responsibilities regarding continuous monitoring:

- Review policy framework for continuous monitoring and security artifacts on a regular basis
- Set minimum requirements for the PMO to provide the State authorizing body regularly scheduled summary reporting of the service provider's continuous monitoring statuses and changes
- Ensure the StateRAMP PMO is providing artifacts to all relevant State authorizing bodies in a timely manner
- StateRAMP Standards and Framework will undergo periodic and regular review to address current trends and concerns in cybersecurity. Notice will be provided with reasonable time frame for implementation.

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

4. CONTINUOUS MONITORING

The StateRAMP continuous monitoring program is based on the continuous monitoring process described in NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organization, and the FedRAMP Continuous Monitoring Strategy Guide on the FedRAMP document assets. StateRAMP has attempted to create a process that will meet the diverse needs of state and local governments.

StateRAMP recognizes that cybersecurity verification is not a "one size fits all" implementation. In order to meet each State's specific needs, the StateRAMP PMO will partner with the State authorizing body, service provider, 3PAO, and the StateRAMP Board to make reasonable accommodations, recommendations, and/or modifications to the standard StateRAMP continuous monitoring processes. Image 1 provides a visual representation of the continuous monitoring process cycle.

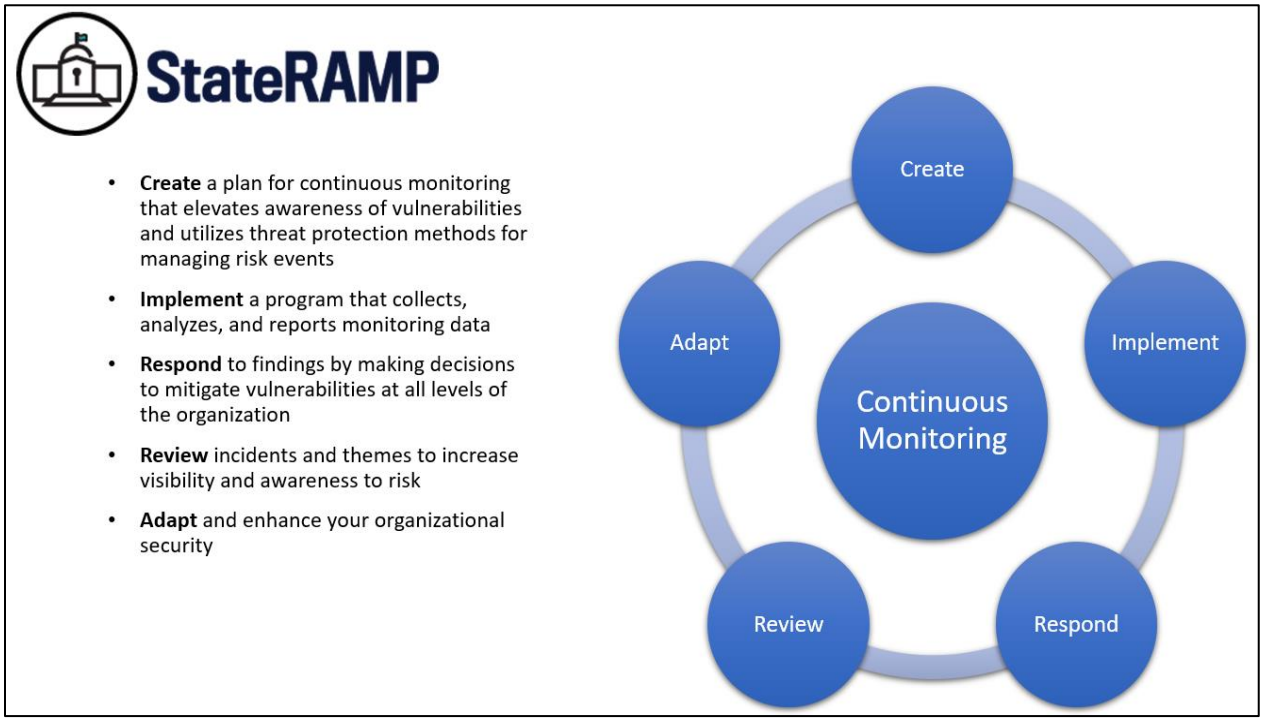

Image 1

4.1 CONTINUOUS MONITORING PROCESS

1. Continuous monitoring begins when a service provider with a StateRAMP Authorized status who is listed on the Marketplace enters into a contract with a state or local government
2. The service provider will partner with the 3PAO to create a continuous monitoring plan that meets the minimum StateRAMP continuous monitoring standards including all specific requirements provided by the State authorizing body
3. It is the service provider's responsibility to implement the continuous monitoring plan as agreed upon by StateRAMP and the State authorizing body
4. The service provider sends StateRAMP all continuous monitoring and significant change artifacts at regular intervals

a. The service provider provides all monthly and quarterly reporting
b. The 3PAO provides all annual and penetration testing reporting

5. The PMO conducts an analysis of all submitted artifacts and creates an executive summary to accompany all submitted artifacts submitted
    a. StateRAMP PMO will provide the State authorizing body access to view and approve the service provider's reporting and PMO comments and States may review raw evidence upon request
6. The State authorizing body reviews the service provider's continuous monitoring artifacts and accompanying executive summary
    a. If any party is not satisfied with the findings, the State Authorizing Body, the StateRAMP PMO, and service provider will meet to define corrective actions which will be incorporated into the POA&M
    b. Additional continuous monitoring requirements are at the discretion of the State Authorizing Body
7. The State Authorizing Body approves all continuous monitoring documentation
    a. Any concerns by the State will be addressed on a case by case basis and could affect the authorization status
8. The PMO receives notification of the State Authorizing Body's approval
9. The PMO updates the service provider's public profile with documentation and most recent State approval as needed

5. FREQUENCY OF MONITORING ACTIVITIES

Upon obtaining Authorized Status, the service provider is required to maintain a continuous monitoring program. The StateRAMP PMOs review and analysis of the service provider's continuous monitoring deliverables is required for service providers to retain their Authorized Status. Failure to implement or comply with the continuous monitoring activities required by the State Authorizing Body can result in a change or loss of the Status.

5.1 MONTHLY ACTIVITIES

Service providers must provide a monthly vulnerability and compliance scan, including raw results, and report to the StateRAMP PMO. The service provider's preferred 3PAO is responsible for providing annual vulnerability and compliance scan reports.

Service providers must mitigate all discovered high-risk vulnerabilities within 30 days, moderate vulnerability risks within 90 days, and low vulnerability risks within 180 days.

- All activities related to mitigation must be tracked at least monthly in the StateRAMP secure system, and will be reviewed by the PMO to ensure compliance
- Service providers must show evidence that outstanding vulnerabilities have been mitigated
- If vulnerabilities are not mitigated within the prescribed timelines, StateRAMP PMO and the State Authorizing Body may request greater frequency of continuous monitoring activities and reserves the right to conduct an impromptu request for evidence regarding most recent assessment

- Failure to comply with the agreed upon continuous monitoring plan and requirements may result in corrective action or revocation of status
- StateRAMP and/or the State Authorizing Body may require additional controls be added to annual 3PAO assessment based on the service providers continuous monitoring activity

5.2 QUARTERLY ACTIVITIES

Service providers must regularly update their POA&M and must submit the updated document to the StateRAMP PMO at least quarterly.

5.3 ANNUAL ACTIVITIES

The following activities must take place on an annual basis for the service provider to retain their Authorized Status and remain in good standing with the StateRAMP PMO and the State Authorizing Body.

5.3.1 SERVICE PROVIDER ANNUAL ACTIVITIES

The service provider is directly responsible for conducting the following activities on an annual basis:

- The Information Security Policies and Procedures for high-risk systems must be reviewed and updated
    - For moderate and low-risk systems, the service provider must review procedures annually and policies every three years
    - The service provider must insert the updated policy document as an attachment to the StateRAMP System Security Plan (SR-SSP) and submit the updated plan to the StateRAMP PMO one year after the initial authorization date and each year thereafter
- Service providers must contract with a 3PAO to assess a subset of their security controls
    - The 3PAO will determine which subset of controls are to be assessed, with approximately 1/3 of controls reviewed annually, with all controls reviewed every three years
    - The StateRAMP PMO and/or State Authorizing Body may require specific security controls for annual review
    - The resulting assessment report must be submitted to the StateRAMP PMO one year after the initial authorization date and each year thereafter
- Service providers must conduct penetration testing to ensure compliance with all vulnerability mitigation procedures
    - Penetration testing must be performed by a 3PAO and all penetration testing reports must be sent to the StateRAMP PMO
    - Additional penetration testing is required when the service provider has made a significant change in their product
        - In the case of a significant change, the service provider shall report a self-attestation of penetration testing focused on the specific change
        - Unless required by the State Authorizing Body, this testing does not have to be conducted by a 3PAO but shall be included in the required annual testing by the 3PAO

- The Configuration Management Plan must be reviewed and updated
    - The new plan must be submitted to the StateRAMP PMO one year after the initial authorization date and each year thereafter
- The IT Contingency Plan must be reviewed and updated
    - The new plan must be submitted to the StateRAMP PMO one year after the initial authorization date and each year thereafter
- An incident response plan test must be conducted, and the corresponding Incident Response Plan must be reviewed and updated
    - Record the results of the incident response testing in the SR-SSP in the appropriate control description field indicating when the testing took place, testing materials, who participated, and who conducted the testing
    - Insert the updated Incident Response Plan as an attachment to the SR-SSP
- The SR-SSP must be reviewed and updated
    - The new plan must be submitted to the StateRAMP PMO one year after the initial authorization date and each year thereafter

5.3.2 3PAO ANNUAL ACTIVITIES

The 3PAO is directly responsible for conducting the following activities on an annual basis:

- The development of a security assessment plan that describes the scope of the assessment including:
    - Security controls and control enhancements under assessment
    - Assessment procedures to be used to determine security control effectiveness
    - Assessment environment, assessment team, and assessment roles and responsibilities
- Conduct an assessment of the security controls in the service providers information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements
- Provide a report of vulnerability and compliance scanning to the service provider and the StateRAMP PMO
- Produce a security assessment summary that documents the results of the assessment
- Provide the results of the security control assessment to StateRAMP
    - Security control assessments include in-depth monitoring, vulnerability scanning, malicious user testing, and insider threat assessment
    - Security control assessments for performance and load testing must occur once every three years unless the State Authorizing Body specifically requires more frequent testing