Continuous Monitoring Strategy & Guide



Version 2.0

June 6, 2014



Executive Summary

The OMB memorandum M-10-15, issued on April 21, 2010, changed from static point in time security authorization processes to Ongoing Assessment and Authorization throughout the system development life cycle. Consistent with this new direction favored by OMB and supported in NIST guidelines, FedRAMP developed an ongoing assessment and authorization program for the purpose of maintaining the authorization of Cloud Service Providers (CSP).

After a system receives a FedRAMP authorization, it is probable that the security posture of the system could change over time due to changes in the hardware or software on the cloud service offering, or also due to the discovery and provocation of new exploits. Ongoing assessment and authorization provides federal agencies using cloud services a method of detecting changes to the security posture of a system for the purpose of making risk-based decisions.

This guide describes the FedRAMP strategy for CSPs to use once they have received a FedRAMP Provisional Authorization. CSPs must continuously monitor the cloud service offering to detect changes in the security posture of the system to enable well-informed risk-based decision making. This guide instructs CSPs on the FedRAMP strategy to continuously monitor their systems.

Document Revision History

| **Date** | **Page(s)** | **Description** | **Author** |
| --- | --- | --- | --- |
| 06/06/2014 |  | Major revision for SP800-53 Revision 4. Includes new template and formatting changes. | FedRAMP PMO |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[About this document 7](#_Toc389813623)

[Who should use this document? 7](#_Toc389813624)

[How this document is organized 7](#_Toc389813625)

[How to contact us 7](#_Toc389813626)

[1. Overview 8](#_Toc389813627)

[1.1. Purpose of This Document 8](#_Toc389813628)

[1.2. Continuous Monitoring Process 8](#_Toc389813629)

[2. Continuous Monitoring Roles & Responsibilities 10](#_Toc389813630)

[2.1. Authorizing Official 10](#_Toc389813631)

[2.2. FedRAMP PMO 10](#_Toc389813632)

[2.3. Department of homeland security (DHS) 10](#_Toc389813633)

[2.4. Third Party Assessment Organization (3PAO) 11](#_Toc389813634)

[3. Continuous Monitoring Process Arease 11](#_Toc389813635)

[3.1. Operational Visibility 11](#_Toc389813636)

[3.2. Change Control 12](#_Toc389813637)

[3.3. Incident Response 13](#_Toc389813638)

[Appendix A – Control Frequencies 14](#_Toc389813639)

[Appendix B – Template Monthly Reporting Summary 34](#_Toc389813640)

[JAB P-ATO Continuous Monitoring Analysis 34](#_Toc389813641)

List of Tables

[Table 3-1 – Control Selection Criteria 13](#_Toc389738829)

[Table A-1 – Summary of Continuous Monitoring Activities & Deliverables 40](#_Toc389738830)

List of Figures

[Figure 1 – NIST Special Publication 800-137 Continuous Monitoring Process 10](#_Toc389738753)

# About this document

This document has been developed to provide guidance on continuous monitoring and ongoing authorization in support of maintaining a security authorization that meets the FedRAMP requirements. This document is not a FedRAMP template -- there is nothing to fill out in this document.

## Who should use this document?

This document is intended to be used by Cloud Service Providers (CSPs), Third Party Assessor Organizations (3PAOs), government contractors working on FedRAMP projects, and government employees working on FedRAMP projects. This document may also prove useful for other organizations that are developing a continuous monitoring program.

## How this document is organized

This document is divided into seven sections and one appendix.

|  |  |
| --- | --- |
| Section 1 | Provides an overview of the continuous monitoring process. |
| Section 2 | Describes roles and responsibilities for stakeholders other than CSPs. |
| Section 3 | Describes how operational visibility, change control and incident response support continuous monitoring. |
| Appendix A | Describes the security control frequencies. |

## How to contact us

Questions about FedRAMP or this document may be directed to [*info@fedramp.gov*](mailto:info@fedramp.gov)*.*

For more information about FedRAMP, visit the website at <http://www.fedramp.gov>.

1. Overview

Within the FedRAMP Security Assessment Framework, once an authorization has been granted, the CSP’s security posture is monitored according to the assessment and authorization process. Monitoring security controls is part of the overall risk management framework for information security and is a requirement for CSPs to maintain a security authorization that meets the FedRAMP requirements.

Traditionally, this process has been referred to as “Continuous Monitoring” as noted in *NIST SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations*. Other NIST documents such as NIST SP 800-37, Revision 1 refer to “ongoing assessment of security controls”. It is important to note that both the terms “Continuous Monitoring” and “Ongoing Security Assessments” mean essentially the same thing and should be interpreted as such.

Performing ongoing security assessments determines whether the set of deployed security controls in a cloud information system remains effective in light of 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 the FedRAMP requirements, CSPs 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 CSP 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 agencies to make informed risk management decisions as they use cloud services.

* 1. Purpose of This Document

This document is intended to provide CSPs with guidance and instructions on how to implement their continuous monitoring program. Certain deliverables and artifacts related to continuous monitoring that FedRAMP requires from CSP’s are discussed in this document

* 1. Continuous Monitoring Process

The FedRAMP 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*. The goal is to provide: (i) operational visibility; (ii) managed change control; (iii) and attendance to incident response duties. For more information on incident response, review the FedRAMP *Incident Communications Procedure*.

The effectiveness of a CSP’s continuous monitoring capability supports ongoing authorization and reauthorization decisions. Security-related information collected during continuous monitoring is used to make updates to the security authorization package. Updated documents provide evidence that FedRAMP baseline security controls continue to safeguard the system as originally planned.

As defined by the National Institute of Standards and Technology (NIST), the process for continuous monitoring includes the following initiatives:

* **Define** a continuous monitoring strategy based on risk tolerance that maintains clear visibility into assets and awareness of vulnerabilities and utilizes up-to-date threat information.
* **Establish** measures, metrics, and status monitoring and control assessments frequencies that make known organizational security status and detect changes to information system infrastructure and environments of operation, and status of security control effectiveness in a manner that supports continued operation within acceptable risk tolerances.
* **Implement** a continuous monitoring program to collect the data required for the defined measures and report on findings; automate collection, analysis and reporting of data where possible.
* **Analyze** the data gathered and **Report** findings accompanied by recommendations. It may become necessary to collect additional information to clarify or supplement existing monitoring data.
* **Respond** to assessment findings by making decisions to either mitigate technical, management and operational vulnerabilities; or accept the risk; or transfer it to another authority.
* **Review** and **Update** the monitoring program, revising the continuous monitoring strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities; further enhance data driven control of the security of an organization’s information infrastructure; and increase organizational flexibility.

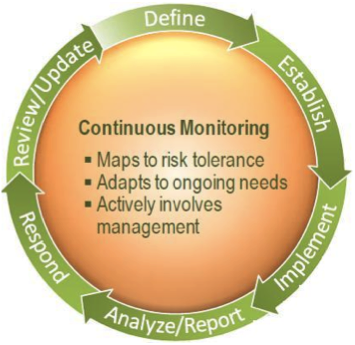


Figure 1 – NIST Special Publication 800-137 Continuous Monitoring Process

Security control assessments performed periodically validate whether stated security controls are implemented correctly, operating as intended, and meet FedRAMP baseline security controls. Security status reporting provides federal officials with information necessary to make risk-based decisions and provides assurance to existing customer agencies regarding the security posture of the system.

1. Continuous Monitoring Roles & Responsibilities
   1. Authorizing Official

Authorizing Officials and their teams (“AOs”) serve as the focal point for coordination of continuous monitoring activities for CSPs. CSPs must coordinate with their AOs to send security control artifacts at various points in time. The AOs monitor both the Plan of Action & Milestones (POA&M) and any major significant changes and reporting artifacts (such as vulnerability scan reports) associated with the CSP service offering. AOs use this information so that risk-based decisions can be made about ongoing authorization. Agency customers must perform the following tasks in support of CSP continuous monitoring:

* Notify CSP if the agency becomes aware of an incident that a CSP has not yet reported
* Provide a primary and secondary POC for CSPs and US-CERT as described in agency and CSP *Incident Response Plans*
* Notify US-CERT when a CSP reports an incident
* Work with CSPs to resolve incidents; provide coordination with US-CERT if necessary
* Notify FedRAMP ISSO of CSP incident activity
* Monitor security controls that are agency responsibilities.

During incident response, both CSPs and leveraging agencies are responsible for coordinating incident handling activities together, and with US-CERT. The team based approach to incident handling ensures that all parties are informed and enables incidents to be closed as quickly as possible.

* 1. FedRAMP PMO

The FedRAMP Program Management Office (PMO) acts as the liaison for the Joint Authorization Board for ensuring that CSPs with a JAB P-ATO strictly adhere to their established Continuous Monitoring Plan. The JAB and FedRAMP PMO only perform Continuous Monitoring activities for those CSPs that have a JAB P-ATO.

* 1. Department of homeland security (DHS)

The FedRAMP Policy Memo released by OMB defines the DHS FedRAMP responsibilities to include:

* Assisting government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity
* Coordinating cybersecurity operations and incident response and providing appropriate assistance
* Developing continuous monitoring standards for ongoing cybersecurity of Federal information systems to include real-time monitoring and continuously verified operating configurations
* Developing guidance on agency implementation of the Trusted Internet Connection (TIC) program for cloud services.

The FedRAMP PMO works with DHS to incorporate DHS’s guidance into the FedRAMP program guidance and documents.

* 1. Third Party Assessment Organization (3PAO)

Third Party Assessment Organizations (3PAO) are responsible for independently verifying and validating the control implementation and test results for CSPs in the continuous monitoring phase of the FedRAMP process. Specifically, 3PAOs are responsible for:

* Assessing a defined subset of the security controls annually.
* Submitting the assessment report to the ISSO one year after the CSP’s authorization date and each year thereafter.
* Performing announced penetration testing.
* Perform annual scans of web applications, databases, and operating systems.
* Assessing changed controls on an ad hoc basis as requested by the AOs for any changes made to the system by the CSP.

In order 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 CSP for inclusion in 3PAO authored documentation. As an example:

* If scans are performed by the CSP, the 3PAO must either be on site and observe the CSP performing the scans or be able to monitor or verify the results of the scans through other means documented and approved by the AO.
* Documentation provided to the CSP must be placed in a format that either the CSP cannot alter or that allows the 3PAO to verify the integrity of the document.

1. Continuous Monitoring Process Arease
   1. Operational Visibility

An important aspect of a CSP’s continuous monitoring program is to provide evidence that demonstrates the efficacy of its program. CSPs and its independent assessors are required to provide evidentiary information to AOs at a minimum of a monthly, annually, every 3 years, and on an as-needed frequency after authorization is granted. The submission of these deliverables allow AOs to evaluate the risk posture of the CSP’s service offering.

Table A-1 notes which deliverables are required as part of continuous monitoring activities. These deliverables include providing evidence, such as providing monthly vulnerability scans of CSPs operating systems/infrastructure, databases, and web applications.

As part of the continuous monitoring process CSPs are required to have a 3PAO perform an assessment on an annual basis for a subset of the overall controls implemented on the system. During the annual assessment the controls listed in Table A-1 are tested along with an additional number of controls selected by the AO. The AO has the option to vary the total number of controls tested to meet the desired level of effort for testing. The AO selects the additional controls for testing based on the following criteria in Table 3-1.

There are additional requirements for testing and control selection for CSPs that are transitioning to the FedRAMP 800-53 Revision 4 baseline. For additional guidance to on Revision 4 transition testing guidance, review the *FedRAMP Revision 4 Transition Guide*.

|  |  |  |
| --- | --- | --- |
| **Criteria** | | **Description** |
| 1. | Condition of previous assessment | Any conditions made by the authorizing official (AO) in the authorization letter or during a previous assessment. This would include the resolution of vulnerabilities within certain time-frames, implementation of new capabilities, etc. |
| 2. | Weakness identified since the last assessment | Any areas in which a cloud system has had known vulnerabilities or enhanced risk related to specific controls. Examples might include actual or suspected intrusion, compromise, malware event, loss of data, or DoS/DDoS attack. |
| 3. | Known or suspected testing/continuous monitoring failure | Any areas where the cloud system has demonstrated a weakness or vulnerability in continuous monitoring and testing related to specific security controls Examples might include those controls related to patch management, configuration management, or vulnerability scanning. |
| 4. | Control implementation that has changed since last assessment | Any control implementation s that have changed since the last assessment. These changes might not reach the level of a significant change but due to their change in implementation status would require an independent assessment of that implementation. |
| 5. | Newly discovered vulnerability, zero-day attack, or exploit | Select additional controls for testing when the system is affected by newly discovered vulnerabilities or zero-day exploits. Examples would include the Heartbleed vulnerability. |
| 6. | Recommendation of Authorizing Official or Organization | Based on direct knowledge and use of a cloud system, authorizing officials or organizations can require the CSP to test additional controls based on unique mission concerns or based on the CSP’s performance since their last assessment. |

Table 3-1 – Control Selection Criteria

* 1. Change Control

Systems are dynamic and FedRAMP anticipates that all systems are in a constant state of change. Configuration management and change control processes help maintain a secure baseline configuration of the CSP’s architecture. Routine day-to-day changes are managed through the CSP’s change management process described in their *Configuration Management Plan*.

However, before a planned major significant change takes place, CSP’s must perform a Security Impact Analysis to determine if the change will adversely affect the security of the system. The Security Impact Analysis is a standard part of a CSP’s change control process as described in the CSP’s *Configuration Management Plan*.

CSPs must notify their AO with a minimum of 30 days before implementing any planned major significant changes. The AOs might require more time based on the severity of the change being implemented so CSPs must work close with the AOs to understand how much time is needed in advance of major changes. CSPs must complete a *Significant Change Security Impact Analysis Form* and provide to the AO for their analysis. All plans for major significant changes must include rationale for making the change, and a Security Assessment Plan (SAP) for testing the change prior to and following implementation in the production system.

If any anticipated change adds residual risk, or creates other risk exposure that the AO finds unacceptable, the ATO could be revoked if the change is made without prior approval. The goal is for CSPs to make planned changes in a controlled manner so that the security posture of the system is not lowered.

After implementation the CSP must submit a new *Security Assessment Report* to the AO based on a security assessment performed by a 3PAO in accordance with the SAP and within the timeframe agreed between the CSP and AO. Additionally, the CSP will need to submit updated documentation pertaining to the newly implemented changes.

* 1. Incident Response

FedRAMP requires that CSPs demonstrate that they are able to adequately respond to security incidents. As part of the FedRAMP requirements, CSPs are required to submit and maintain an incident response guide, which is approved by the AO. CSPs are also required to follow the incident response and reporting guidance contained in the *FedRAMP Incident Communications Procedure*.

# Appendix A – Control Frequencies

Security controls have different frequencies for performance and review, and some controls require review more often than others. Table A-1 summarizes the minimally required frequencies required for the different continuous monitoring activities. Some continuous monitoring activities require that the CSP submits a deliverable to their AO. Note that CSPs are required to submit deliverables listed in Table A-1 if they have full or shared responsibility for the listed control. However, inherited controls do not require the submission of a deliverable. For example, in some cases, PaaS or SaaS offerings may inherit physical and environmental protection controls from an IaaS and would therefore not submit deliverables for those inherited controls.

Other continuous monitoring activities do not require a deliverable, and will be reviewed by 3PAOs during security assessments. CSPs must be able to demonstrate to 3PAOs that ongoing continuous monitoring activities are in place, and have been occurring as represented in the *System Security Plan*. For example, if a CSP has indicated in their *System Security Plan* that they monitor unsuccessful login attempts on an ongoing basis, the 3PAO may ask to see log files, along with the CSP analysis of the log files, for random dates over the course of prior authorization period (e.g., bi-annual, annual).

In Table A-1, refer to the “Description” column for information about what is required and when it is required to be submitted. A checkmark in either the CSP Authored Deliverable column or 3PAO Authored Deliverable column of Table A-1 indicates that a deliverable is required.

If concerns arise about the security posture of the CSP system, AOs may ask for a security artifact at any point in time. For example, if a CSP indicates in their *System Security Plan* that they actively monitor information system connections, the AO could ask the CSP to send them log file snippets for a particular connection at any point in time. If it becomes known that an entity that connects to a CSP has been compromised by an unauthorized user, the AO coordinate with the CSP to check in on the interconnection monitoring of the CSP. CSPs should anticipate that aside from scheduled continuous monitoring deliverables, and aside from testing performed by 3PAOs, that the AOs may request certain system artifacts on an ad hoc basis if there are concerns.

CSPs are required to submit a schedule of activities within 15 days from the date of their authorization to their AOs and annually thereafter. This schedule assists CSPs in managing continuous monitoring activities.

**Note:** For controls that do not have a check in either the CSP authored deliverable or 3PAO authored deliverable in Table A-1, CSPs will be required to provide evidence of compliance minimally during annual assessment and upon request.

| **Row #** | **Control Name** | **Control ID** | **Description** | **CSP Authored Deliverable** | **3PAO Authored Deliverable** | **Notes** |
| --- | --- | --- | --- | --- | --- | --- |
| **Continuous and Ongoing** | | | | | | |
| 1 | Information System Monitoring | SI-4 | The organization: a. Monitors the information system to detect:  1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and  2. Unauthorized local, network, and remote connections;  b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];  c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;  (continued) |  |  |  |
|  | Information System Monitoring | SI-4 (continued) | (continued)  d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;  e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;  f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and  g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]]. |  |  |  |
| 2 | Auditable Events | AU-2a, AU-2d | Certain events must be continuously monitored.  AU-2a auditable events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes |  |  | AU-2d Frequency: continually |
| 3 | Information System Component Inventory | CM-8(3)a | CSPs must be able to detect new assets continuously, using automated mechanisms with a maximum five-minute delay in detection. |  |  | This activity should be automated. |
| 4 | Incident Reporting | IR-6 | CSPs must report incidents in accordance with the FedRAMP Incident Communications Procedure. | ✓ |  | IR-6a. [US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)] |
| 5 | Temperature & Humidity Controls | PE-14b | CSPs must monitor temperature and humidity controls continuously. |  |  | Refer to ASHRAE *Thermal Guidelines for Data Processing Environments*.  Requirements: The service provider measures temperature at server inlets and humidity levels by dew point. |
| 6 | Vulnerability Scanning | RA-5(2) | CSPs must update the list of vulnerabilities scanned continuously, before each scan. |  |  | Before scans are run, signatures must be updated to the most current version. |
| 7 | Wireless Intrusion Detection | SI-4(14) | The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system. |  |  |  |
| **10 Days** | | | | | | |
| 8 | Contingency Training | CP-3a | CSPs must train personnel in their contingency roles and responsibilities within 10 days of assuming a contingency role or responsibility. Record the date of the training in the *System Security Plan*. |  |  |  |
| **Weekly** | | | | | | |
| 9 | Audit Review, Analysis, & Reporting | AU-6a | CSPs must review and analyze information system audit records for indications of inappropriate or unusual activity. |  |  | Report findings of inappropriate or unusual activity to incident response team. |
|  | **Monthly** | | | | | |
| 10 | Vulnerability Scanning | RA-5d | CSPs must mitigate all discovered high-risk vulnerabilities within 30 days and mitigate moderate vulnerability risks in 90 days. CSPs must send their ISSO updated artifacts every 30 days to show evidence that outstanding high-risk vulnerabilities have been mitigated. | ✓ |  |  |
| 11 | Continuous Monitoring Security State | CA-7g | CSPs must report the security state of the system to their own organizational officials on a monthly basis. |  |  |  |
| 12 | Access Records | PE-8b | CSPs must review visitor access records monthly. |  |  |  |
| 13 | Least Functionality | CM-7(1)a | CSPs must review the information system monthly to identify and eliminate unnecessary functions, ports, protocols, and/or services. If ports, protocols, and/or services are changed, Table 10-4 in the *System Security Plan* must be updated at the time of change. Changes must be made according to the CSP change management process that is described in the *Configuration Management Plan*. |  |  |  |
| 14 | Vulnerability Scanning | RA-5a | CSPs must scan operating systems, web applications and databases monthly. All scan reports must be sent to the ISSO monthly. | ✓ |  |  |
| 15 | Flaw Remediation | SI-2c | CSPs must install security-relevant software and firmware updates within 30 days of the release of the updates. |  |  |  |
| 16 | Flaw Remediation | SI-2(2) | CSPs must use an automated mechanism to look for system flaws at least once a month. |  |  | Examples of programs that look for system flaws could include program that: i) inspect log files looking for variances in normal behavior; ii) look for missing patches; iii) look for errors that indicate software bugs; iv) look for processing errors; v) look for indications for intrusions; vi) look for malware; vii) look for access control violations or attempted violations etc.. |
| 17 | Software & Information Integrity | SI-7(1) | CSPs must perform integrity scans monthly. |  |  | SI-7 (1). [Selection to include security relevant events and at least monthly] |
| 18 | Account Management | AC-2(2) | Automatic termination of temporary and emergency accounts after no more than 30 days. |  |  |  |
| 19 | Security Functionality Verification | SI-6 | System verifies correct operation of security functions monthly. |  |  | SI-6b [to include upon system startup and/or restart at least monthly]  SI-6c [to include system administrators and security personnel]  SI-6d [to include notification of system administrators and security personnel] |
| 20 | Plan of Action & Milestones | CA-5b | CSPs must update the POA&M at least monthly and must submit it to the ISSO at least monthly. | ✓ |  | Updates must be based on the findings from security assessments, security impact analyses, CSP risk assessments, continuous monitoring activities and any other indications of a security weakness. |
| 21 | Monitoring Physical Access | PE-6b | CSPs must review physical access logs at least monthly. Record the dates of review in the *System Security Plan*. |  |  |  |
|  | **60 Days** | | | | | |
| 22 | Authenticator Management | IA-5g | Change/refresh authenticators/passwords at least every sixty days. |  |  |  |
|  | **Quarterly (90 Days)** | | | | | |
| 23 | Account Management | AC-2(3) | AC-2(3) Disables user accounts after 90 days inactivity.  Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the Authorizing Official. |  |  |  |
| 24 | Identifier Management | IA-4e | IA-4e: Disables user IDs after 90 days of inactivity.  IA-4e. Requirement: The service provider defines time period of inactivity for device identifiers. |  |  |  |
| 25 | Publicly Accessible Content | AC-22d | CSPs must review content on publicly accessible system and look for non-public information. |  |  | This indicates data leaks and erroneous or unauthorized information disclosure. |
| 26 | Access Restrictions for Change | CM-5(5)b | CSPs must review and reevaluate their information system developer/integrator privileges quarterly. Record the date of the review in the *System Security Plan*. |  |  |  |
|  | **Annually** | | | | | |
| 27 | Information Security Policies | All “-1” Controls | CSPs must review Information Security Policies and Procedures annually. Insert the updated Policy document as an Attachment to the *System Security Plan* and submit the updated plan to the ISSO one year from the Provisional Authorization date and each year thereafter. | ✓ |  | All control families have “-1” controls (e.g. AC-1, SC-1). |
| 28 | Account Management | AC-2j | CSPs must perform an annual review and re-certification of user accounts to verify if the account holder requires continued access to the system. Record the date of annual user re-certification in the *System Security Plan*. |  |  | It is advisable to develop and document the annual user re-certification process and plan. |
| 29 | Security Awareness | AT-2 | CSPs must provide basic security awareness training to all users annually. Record the date that security awareness training last took place in the *System Security Plan*. |  |  | Security awareness training must include contractors, executives, and anyone who has access to the system. |
| 30 | Auditable Events | AU-2(3) | CSPs must review and update auditable events annually or whenever there is a change in the threat environment. Changes to the auditable event list must be recorded in the *System Security Plan*. CSPs must record the date that the auditable event review meeting takes place in the *System Security Plan*. Meeting notes with information about who attended the meeting must be archived. |  |  | Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the Authorizing Official. |
| 31 | Security Assessments | CA-2b | CSPs must have a 3PAO assess a subset of their security controls annually. Submit the assessment report to the ISSO one year from the Provisional Authorization date and each year thereafter. |  | ✓ | Consult with the ISSO to obtain information on which controls to assess during annual testing.  Deliverables produced by 3PAOs are always separate from deliverables produced by CSPs. |
| 32 | Security Assessments | CA-2 | The organization:  a. Develops a security assessment plan that describes the scope of the assessment including:  1 .Security controls and control enhancements under assessment;  2. Assessment procedures to be used to determine security control effectiveness; and  3.Assessment environment, assessment team, and assessment roles and responsibilities;  b. Assesses the security controls in the information system and its environment of operation [FedRAMP Assignment: at least annually] 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;  (continued) |  | ✓ |  |
|  | Security Assessments | CA-2 (continued) | (continued)  c. Produces a security assessment report that documents the results of the assessment; and  d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles]. |  | ✓ |  |
| 33 | Security Assessments - Specialized Assessments | CA-2 (2) | The organization includes as part of security control assessments, [FedRAMP Assignment: at least annually], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]].  . |  | ✓ | Requirement: To include 'announced', 'vulnerability scanning' at least annually  Deliverables produced by 3PAOs are always separate from deliverables produced by CSPs. |
| 34 | Penetration Testing | CA-8, CA-8 (1) | CSPs must conduct penetration testing at least annually or when there is a major significant change to ensure compliance with all vulnerability mitigation procedures. Penetration testing must be performed by a 3PAO. All penetration testing reports must be sent to the ISSO. |  | ✓ | Deliverables produced by 3PAOs are always separate from deliverables produced by CSPs. |
| 35 | Baseline Configuration | CM-2(1)a | CSPs must review and update the baseline configuration annually or during installations and updates. Changes and updates to the baseline configuration must be made in accordance with the change control process described in the CSP’s *Configuration Management Plan*. |  |  | This activity must also be performed whenever there is a major significant change to the system. |
| 36 | Configuration Management Plan | CM-9 | CSPs must review and update the *Configuration Management Plan* annually. Submit the new plan to the ISSO one year from the Provisional Authorization date (and each year thereafter). | ✓ |  |  |
| 37 | IT Contingency Plan | CP-2d | CSPs must review and update the *IT Contingency Plan* annually. Submit the new plan to the one year from the Provisional Authorization date (and each year thereafter). | ✓ |  | Requirement: For JAB authorizations the contingency lists include designated FedRAMP personnel. |
| 38 | Contingency Training | CP-3c | CSPs must train personnel in their contingency roles and responsibilities annually. Record the date of the training in the *System Security Plan*. |  |  |  |
| 39 | IT Contingency Plan Testing & Exercises (Moderate Systems) | CP-4a | CSPs must test and exercise the *IT Contingency Plan* (for Moderate systems) at least annually using functional exercises  Insert a new *IT Contingency Plan Test Report* into the proper Appendix of the *IT Contingency Plan* (which is submitted annually). | ✓ |  | Guidance: Plans for this test must be submitted at least 30 days prior to test to ISSO.  CP-4a. Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended); plans are approved by Risk-executive/Authorizing Official prior to initiating testing.  Moderate systems require functional testing and exercises. |
| 40 | Information System Backup | CP-9(1) | CSPs must test backups annually to verify integrity and reliability. When the *System Security Plan* is updated annually, this control description must indicate when (date) the last test took place and who performed the testing. |  |  |  |
| 41 | Incident Response Training | IR-2c | CSPs must conduct incident response training annually and when required by information system changes. When the *System Security Plan* is updated annually, this control description must indicate when training took place, training materials, who participated, and who conducted the training. |  |  |  |
| 42 | Incident Response Testing | IR-3 | CSPs must perform incident response testing annually. When the *System Security Plan* is updated annually, record the results of the incident response testing directly in the control description box indicating when testing took place, testing materials, who participated, and who conducted the testing. | ✓ |  | Guidance: Test plans must be delivered to ISSO at least 30 days prior to testing.  IR-3. Requirement: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). Requirement: For JAB Authorization, the service provider provides test plans to FedRAMP annually.  Test all contact information in the Appendices of the *Incident Response Plan* to make it is accurate. |
| 43 | Incident Response Plan | IR-8c | CSPs must review the *Incident Response Plan* annually and update it if necessary. Insert the updated Incident Response Plan as an attachment to the *System Security Plan*. | ✓ |  |  |
| 44 | Physical Access Authorizations | PE-2c | CSPs must review physical access authorization credentials annually and remove personnel from the access list who no longer require access. The date at which this review takes place, and who performed it, must be recorded in the *System Security Plan*. |  |  |  |
| 45 | Physical Access Control | PE-3f | CSPs must inventory physical access devices annually. The date of the inventory must be recorded in the *System Security Plan*. |  |  |  |
| 46 | Physical Access Control | PE-3g | CSPs must change combinations and keys annually. The date that the keys and combinations are changed must be recorded in the *System Security Plan* along with the name of the person responsible for making the changes. |  |  | This activity must also be performed when keys are lost, combinations are compromised, or individuals are transferred or terminated. |
| 47 | System Security Plan | PL-2c | CSPs must review and update the *System Security Plan* annually. Submit the new plan to the ISSO one year from the Provisional Authorization date (and each year thereafter). | ✓ |  |  |
| 48 | Access Agreements | PS-6b,  PS-6c | CSPs must review and update access agreements annually. The date of the access agreement review must be recorded in the *System Security Plan*.  Individuals requiring access to organizational information and information systems must re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or at least annually. |  |  | A good time to do this is during the annual user re-certification (AC-2j). |
| 49 | Vulnerability Scan | RA-5a | CSPs must have an accredited 3PAO scan operating systems/infrastructure, web applications, and databases annually. All scan reports must be sent to the ISSO. |  | ✓ | Deliverables produced by 3PAOs are always separate from deliverables produced by CSPs. |
| 50 | Boundary Protection | SC-7(4)e | CSPs must remove traffic flow that is no longer supported by a business/mission need. Changes and updates to traffic flow must be made in accordance with the change control process described in the CSP’s *Configuration Management Plan*. |  |  |  |
| 51 | Security Training | AT-3b,  AT-3c | CSPs must provide role-based security training annually and when required. The date that the training took place, along with whom provided the training, must be recorded In the *System Security Plan*. |  |  | Role-based security training is typically for privileged users. |
| 52 | Security Training Records | AT-4b | CSPs must archive security training records at least annually. In the *System Security Plan*, record who participated in training and when the training took place. Archive the actual training materials. |  |  |  |
|  | **Every Two Years** | | | | | |
| 53 | Identifier Management | IA-4d | Prevent reuse of user and device identifiers every two years. |  |  |  |
|  | **Every Three Years** | | | | | |
| 54 | Security Authorization | CA-6c | The security authorization will be re-evaluated by the Authorizing Official at least every three years. CSPs must record the date of the Provisional Authorization, and any reauthorization, in the *System Security Plan*. |  |  | This activity must also be performed whenever there is a major significant change to the system.  CA-6c. Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the Authorizing Official. |
| 55 | IT Contingency Plan Testing & Exercises (Low Systems) | CP-4a | CSPs must test and exercise the *IT Contingency Plan* (for Low systems) every three years using table top written tests. Record the testing date in the *System Security Plan*. | ✓ |  | Guidance: Plans for this test must be submitted at least 30 days prior to test to ISSO.  CP-4a. Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended); plans are approved by Risk-executive/ Authorizing Official prior to initiating testing. |
| 56 | Position Categorization | PS-2c | CSPs must review position categorizations every three years. Record the date that position categorization was completed in the *System Security Plan*. |  |  |  |
| 57 | Risk Assessment | RA-3c, RA-3e | CSPs must review and update security assessments every three years and record the date of the last security assessment in the *System Security Plan*. |  |  | This activity must also be performed whenever there is a major significant change to the system.  Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.  RA-3d. Requirement: to include the Risk Executive; for JAB authorizations to include FedRAMP |
|  | **Every Five Years** | | | | | |
| 58 | Personnel Screening | PS-3b | Law enforcement must undergo personnel screening every 5 years. Any law enforcement staff screened must have the screening date recorded in the *System Security Plan* along with their name.  For national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance.  For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions. |  |  | High impact personnel screening is not required at this time because FedRAMP is not supporting high impact sensitive systems at this time. |

Table A-1 – Summary of Continuous Monitoring Activities & Deliverables

# Appendix B – Template Monthly Reporting Summary

As described in the FedRAMP requirements, CSPs must provide monthly reports of all vulnerability scanning to authorizing officials for review and tracking these vulnerabilities within the POA&Ms. These deliverables are really a subset of the evidence required at time of authorization. In this vein, the analysis of these scan results should be performed in the same manner they were for time of authorization. In particular, this means:

* All scan findings must be documented (including low findings)
* Each unique vulnerability is tracked as an individual POA&M item
* Deviation requests must be submitted for any requested changes to scan findings (e.g. risk adjustments, false positives, and operational requirements)

On a monthly basis, Authorizing Officials will be monitoring these deliverables to ensure that the CSP maintains an appropriate risk posture – which typically means the risk posture stays at the level of authorization or improves. As a part of any authorization letter, CSPs are required to maintain a continuous monitoring program. CSPs should understand that this means their continuous monitoring deliverables and associated view of risk posture means that this analysis on a monthly basis leads to a continuous authorization decision every month by Authorizing Officials.

## JAB P-ATO Continuous Monitoring Analysis

In an effort to aid agencies in their analysis and help CSPs understand how agency authorizing officials will analyze the continuous monitoring deliverables, the following are some details on how the FedRAMP PMO and JAB analyze continuous monitoring deliverables for those CSPs who achieve a P-ATO.

Some notes on the analysis of reporting within continuous monitoring for JAB P-ATOs:

* Summary information is requested from CSPs in order to provide easier analysis of the continuous monitoring reporting (the reporting format is provided below).
* Verifying what CSPs provide and their analysis is imperative to ensure that the risk posture is accurately depicted in this summary information.
* Trending data is imperative to understand the overall effectiveness of a CSPs continuous monitoring program.
* Late POA&Ms and risk are of high importance to the JAB. This details an inability of vendors to meet the FedRAMP requirements and identifies key risks that agencies should be aware of. Also, a repeated history of late POA&Ms is a key indicator of an ineffective continuous monitoring program and usually also indicates misaligned business processes and operations within a CSP.
* It is normal to have deviation requests and unique items for each vendor that must be analyzed on a system to system basis. Some specifics on how the JAB handles these unique items:
  + Date adjustments are not treated as deviation requests, as this does not change the fact that a POA&M is late for remediation within the required timeframes.
  + CSPs many times buy products or services and incorporates these in to their cloud environment to deliver their services. Many times risks can be related to these products and services and these risks are considered “vendor dependant.” Risks are only considered vendor dependencies when remediating vulnerabilities within a product or service is not allowed by the vendor (e.g. it would void the warranty).
    - All vendor dependencies at a high risk level must be mitigated to a moderate through compensating controls within 30 days.
    - Vendor dependencies at the low and moderate level require CSPs to be in contact with their vendors at a minimum of a monthly basis to ensure there are no updates that would remediate the known vulnerabilities.
    - If a CSP contacts their vendors and provides evidence with their monthly deliverables of this contact regarding any fixes to the open vulnerabilities, then a vendor dependency is not considered a late POA&M.
  + Operational requirements exist only for vulnerabilities where the ability to remediate a vulnerability does not exist or remediating a vulnerability is not supported if the vulnerability is vendor dependent.

Attached you will find the Monthly Reporting Summary the FedRAMP PMO uses to highlight key considerations for review to the JAB on a monthly basis for each CSP that achieves a P-ATO. In this template you will see:

* System Status
* Overview
* Unique Scanning Summary
* Raw Scanning Summary
* Open POA&M Summary
* Items of Note
* Considerations for Review
* Additional Information
* Requested Deviation Details

