FedRAMP™

FedRAMP® Continuous Monitoring Playbook

Version 1.0

11/17/2025

GSA®

info@fedramp.gov
FedRAMP.gov

DOCUMENT REVISION HISTORY

Date	Version	Page(s)	Description	Author
11/17/2025	1.0	All	Initial publication	FedRAMP

TABLE OF CONTENTS

1. Introduction

This FedRAMP Continuous Monitoring (ConMon) Playbook provides an overview of FedRAMP Rev 5 continuous monitoring (ConMon) requirements and activities, along with guidance and best practices. The information in this playbook applies to cloud service offerings (CSOs) authorized via the legacy JAB path and current Rev5 Agency Authorization path. This playbook is a consolidation of the following ConMon-related guidance previously provided as standalone documents:

- FedRAMP Continuous Monitoring Strategy Guide, version 3.2 (2018)
- FedRAMP Vulnerability Scanning Requirements, version 3.0 (2024)
- FedRAMP Vulnerability Scanning Requirements for Containers, version 1.0 (2021)
- FedRAMP Guide for Determining Eligibility and Requirements for the Use of Sampling for Vulnerability Scans, version 1.0 (2018)
- Vulnerability Scanning FAQ (2025)
- FedRAMP Annual Assessment Guidance, version 3.0 (2024)
- FedRAMP Significant Change Policies and Procedures, version 1.0 (2018)
- FedRAMP Incident Communications Procedures, version 5.0 (2024)
- FedRAMP Collaborative ConMon Quick Guide (2023)
- FedRAMP Continuous Monitoring Performance Management Guide, version 3.0 (2023)

2.Continuous Monitoring Overview

FedRAMP ConMon 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; and (iii) attendance to incident response duties.**

The effectiveness of a CSP's ConMon capability supports ongoing agency authorization decisions. CSPs report on the status of the CSO's security posture by providing ConMon deliverables to federal agency customers. Required ConMon deliverables are described in greater detail throughout this playbook.

CSPs with more than one federal agency customer are required to implement a collaborative ConMon approach, intended to streamline the ConMon process and potentially minimize duplicative efforts in a way that helps each federal agency still perform their due diligence related to ConMon. This approach is described in Section 7 of this playbook.

Continuous Monitoring Process Areas

Operational Visibility

CSPs demonstrate a mature and effective security program through the implementation of security controls (for example, system monitoring and event logging) and provide operational visibility by producing required deliverables and supporting evidence. Deliverables and supporting evidence are provided monthly, annually, every three years, and on an as-needed basis. Controls with minimally required frequencies for each continuous monitoring activity are identified in Column J of the FedRAMP Security Controls Baseline workbook.

Change Control

Cloud systems are dynamic and are in a constant state of change. Configuration management and change control processes help maintain a secure baseline configuration of the cloud system. Before implementing a change, CSPs conduct a security impact analysis, and - depending on the type of change - implement the Significant Change process steps described in Section 5 of this playbook.

Incident Response

CSPs must demonstrate the ability to adequately respond to security incidents and emergency directives. As part of the FedRAMP authorization process, the CSP is required to submit and

maintain an incident response plan. Requirements and guidance for incident communications are described in Section 6 of this playbook.

Continuous Monitoring Roles & Responsibilities

Cloud Service Provider (CSP)

Cloud Service Providers (CSPs) bear the primary responsibility for implementing and maintaining the security controls documented in their System Security Plan (SSP) and continuously monitoring the effectiveness of those controls. This includes proactively identifying and addressing vulnerabilities, responding to security incidents, and providing timely and accurate information to agency AOs, the FedRAMP PMO, and assessors. CSPs are expected to fully cooperate with assessments, providing access to systems, documentation, and personnel as needed to demonstrate compliance with FedRAMP requirements. Furthermore, CSPs are responsible for maintaining a secure repository of ConMon deliverables, either on USDA Connect.gov or their own secure repository. They must also promptly address any findings or recommendations identified during assessments or by other stakeholders, ensuring the ongoing security and compliance of their cloud offerings.

Agency Authorization Official (AO)

Agency AOs and their teams review the CSP's ConMon activities to ensure the security posture remains sufficient for the agency's use and supports an ongoing authorization. This includes reviewing the monthly Plan of Action and Milestones (POA&M), approving deviation requests and significant change requests, and reviewing the results of the annual assessment. AOs use this information to make risk-based decisions about ongoing authorization of the system for that agency.

FedRAMP Program Management Office (PMO)

The FedRAMP PMO oversees daily operations, provides guidance to agencies and CSPs, and ensures ConMon materials are made available to all leveraging agencies for review. CSPs with cloud offerings categorized at LI-SaaS, Low, or Moderate use the FedRAMP secure repository on USDA Connect.gov for posting ConMon deliverables. CSPs with cloud offerings categorized at High use their own secure repository.

Cybersecurity and Infrastructure Security Agency (CISA)

The Cybersecurity and Infrastructure Security Agency (CISA) coordinates with the FedRAMP PMO when issuing Binding Operational Directives (BODs) and Emergency Directives (EDs).

Independent Assessment Organizations

Independent assessors perform initial and annual assessments of cloud systems, as well as out-of-cycle assessments associated with significant changes. Most CSPs use a FedRAMP recognized Third Party Assessment Organization (3PAO) that meets the necessary quality, independence, and knowledge requirements to perform independent security assessments. A list of FedRAMP recognized 3PAOs can be found on the FedRAMP Marketplace.

With approval by the agency AO, CSPs may choose to use an independent assessment organization that is not recognized by FedRAMP, such as an agency's Independent Verification and Validation (IV&V) team. When using an agency's IV&V team or other third-party assessor that is not a FedRAMP recognized 3PAO, the agency AO must attest to the independence of the assessment organization. In addition, the assessor must comply with FedRAMP requirements and guidance, and use FedRAMP provided templates.

3PAOs (or other independent assessors) are responsible for ensuring that the chain of custody is maintained for any 3PAO-authored documentation. 3PAOs also ensure the veracity and integrity of data provided by the CSP. For 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 and verify the results of the scans through other means.
- Documentation provided to the CSP must be provided in a format that either the CSP cannot alter or that allows the 3PAO to verify the integrity of the document.

Throughout the remainder of this playbook, FedRAMP recognized 3PAOs, other third-party independent assessment organizations, and agency IV&V teams will be collectively referred to as "assessors".

Monthly ConMon Reporting

Security control CA-5 requires CSPs to develop and maintain a POA&M to document remediation plans for correcting risks (e.g., weaknesses, deficiencies, and vulnerabilities) identified during security assessments and ConMon activities. Security control CM-8 requires CSPs to provide an updated inventory at least monthly or when there is a change. Each month, the CSP uploads an up-to-date POA&M and inventory, along with raw vulnerability scan files (when required by agreements with agency customers) and reports to the secure repository. Agency AOs review these deliverables to ensure the risk posture of the CSO remains sufficient for the agency's use of the system.

3. Vulnerability Scanning

Continuous monitoring ensures CSPs continuously maintain the security of their FedRAMP Authorized systems by providing AOs monthly insight into the security posture of the system. CSP scanning policies, procedures, and tools (including vulnerability scanners) are key components to ConMon activities. In an effort to increase the efficiency and effectiveness of ConMon activities, this section provides guidance for scanning requirements.

Background

Vulnerability scanning is a key part of continuous monitoring. Agencies who wish to review CSP vulnerability scans on a routine basis should require CSPs to do so by initiating a customer agreement. These scans augment the FedRAMP Integrated Inventory Workbook Template and FedRAMP Plan of Action and Milestones (POA&M) to provide the designated agency ConMon lead and consuming agencies monthly insights into the risk posture of the CSO. This section does not define additional requirements; rather, it clarifies existing requirements and provides best practices for implementing FedRAMP vulnerability scanning for all FedRAMP security control baselines, specifically in control RA-5.

General Scanning Requirements

Scanner Resiliency: Scanners should be hardened to resist unauthorized use or modification (i.e., unnecessary ports and/or unnecessary services should be closed).

Authenticated Scanning: For Moderate and High systems, the CSP must ensure authenticated scans are performed wherever possible. [RA-5(5)]

Scanning with Full Authorization: For all Moderate and High systems, the CSP must ensure that scans are being performed with full system authorization. [RA-5(5)]

- Scanning must avoid typical lack of authorization issues (including lack of access to remote registry, limited registry access, limited file access, etc.).

Machine-Readable Findings: The scan output must display all scan findings with a low risk or higher in a structured, machine-readable format (such as XML, CSV, or JSON).

- If the scanner is able to output/export findings in more than one machine-readable format, the CSP must select the format that provides the greatest amount of information.

- Where possible, the machine-readable data must include the authentication and authorization status of the scans to demonstrate the degree to which an authenticated scan was performed on each host.

National Vulnerability Database (NVD): For any vulnerability listed in the latest version of the National Institute of Standards and Technology (NIST) NVD, the Common Vulnerabilities and Exposures (CVE) reference number must be included with the machine-readable findings data for that vulnerability.

Common Vulnerability Scoring System (CVSS) Risk Scoring: For any vulnerability with a CVSSv3 base score assigned in the latest version of the NVD, the CVSSv3 base score must be used as the original risk rating. If no CVSSv3 score is available, a CVSSv2 base score is acceptable where available. If no CVSS score is available, the native scanner base risk score can be used.

Configuration Settings: The CSP must provide machine-readable evidence that the scanner's configuration settings have not been altered from the assessor-validated configuration settings approved during the initial authorization assessment.

Configuration Changes: If a scanner configuration change is required (above and beyond normal patching and updates) the AO must be notified and approve of the change.

Signature Updates: For each deliverable, the CSP must update the list of vulnerabilities scanned to the latest available list. [RA-5(2)]

- The CSP must use a vulnerability scanner that checks for automatic signature updates of the scanner's vulnerability database at least monthly.
- The CSP must provide automated machine-readable evidence of the most recent update performed prior to scanning.

Adequate Asset Identification: The scanner findings must contain unique asset identifiers that map to an inventory.

- The CSP must have an automated mechanism to identify and catalog all assets, within the authorization boundary, every month in order to ensure that everything is being scanned appropriately.
- For Web scans, a dynamically updated catalog of Web services should be maintained to include the ports where Web services reside.
- Ephemeral assets: All ephemeral/dynamic assets must be uniquely tagged as such. Oftentimes, ephemeral environments can cause discrepancies when ensuring all assets identified within the inventory have been scanned.

- Container Images: A unique asset identifier must be assigned to every class of image which corresponds to one or more production-deployed containers. These image-based asset identifiers must be documented in the inventory. Instances of production-deployed containers must be tracked internally by the CSP via an automated mechanism, which must be validated by an assessor to meet the baseline control CM-8. Every production-deployed container must correspond to the image from which the deployed container originated, in order to identify the total number of relevant vulnerabilities on production associated with that container.

Types of Scans: CSPs must scan operating systems, Web applications, and databases monthly. [RA-5]

- The entire inventory (or approved sampling percentage) within the boundary must be scanned at the operating system (OS) level at least once a month.
- All Web interfaces and services (or approved sampling percentage) must be scanned.
- All databases (or approved sampling percentage) must be scanned, including those required to support the infrastructure.

Plan of Action and Milestones (POA&M) Entries: The CSP must track each unique vulnerability as an individual POA&M item.

- Individual vulnerabilities must be based on the scanning tool's unique vulnerability reference identifier (ID).
- The CSP may break a unique vulnerability into multiple POA&M items, such as for a vulnerability that applies to different asset types that will be remediated in different ways.
- The CSP must not group multiple unique vulnerabilities into a single POA&M item.

All Non-Destructive Detections: The CSP must enable all non-destructive detections within the scanner.

Image Scanning: Where the CSP offers services, such as virtual images, and where the customer is responsible for scanning but is reliant on the CSP for patching, the CSP must scan the source image for all available customer leveraged images.

- This applies to all images in use or available for use by federal government customers.

Container Unique Requirements

The following requirements are applicable for all CSPs implementing container technologies:

Hardened Images: The CSP must only utilize containers where the image is "hardened." Where applicable, the hardening must be in accordance with relevant benchmarks listed in the National Checklist Program and defined by the National Institute of Standards and Technology (NIST) SP 800-70. Benchmarks are used as a baseline and may be altered. However, the final configurations must be validated by an assessor to ensure they meet FedRAMP requirements for the baseline controls CM-6, SC-2, SC-3, SC-4, SC-6, SC-28, and SC-39. In the case of containers leveraging an image that does not have a listed benchmark available, the CSP must create and maintain an assessor validated benchmark for the purpose of hardening. Non-hardened or general-purpose images may not be used within the authorization boundary. The assessor must validate the CSP build, test, and orchestration pipeline and process of hardening images intended for deployment. Assessor validation of every individual container instance deployed to production is not required. This requirement should not restrict a CSP from leveraging third-party software within hardened containers. This requirement also does not restrict a CSP from using hardened images or software obtained from a secure repository in groups which share IP addresses and may share volumes.

Container Build, Test, and Orchestration Pipeline: The CSP must leverage automated container orchestration tools to build, test, and deploy containers to production. These automated tools must be validated by an assessor to meet FedRAMP requirements for the baseline controls CA-2, CM-2, CM-3, SC-28, SI-3, and SI-7. However, components of the pipeline that fall to the left of the production container registry, including environments intended for development or testing, may reside outside of the system boundary. Non-automated processes should not be considered part of the container testing and orchestration process, except in the case of intentional manual procedures for quality review purposes. These processes and tools must include a mechanism to restrict containers that do not adhere to FedRAMP requirements from successfully deploying.

Vulnerability Scanning for Container Images: Prior to deploying containers to production, a CSP must ensure that all components of the container image are scanned. When possible, the container orchestration process should incorporate scanning as one of the steps in the deployment pipeline. The 30-day scanning window begins as soon as the container is deployed to the production registry. Only containers from images that have been scanned within a 30-day vulnerability scanning window can be actively deployed on the production environment. Additionally, modification of configuration settings defined within the image or software patching should never occur directly on the production environment, but rather on the replacement image to be deployed to production. Performing vulnerability scanning directly on containers deployed to production is not recommended, unless it is performed via the use of independent security sensors deployed alongside production-deployed containers.

Security Sensors: Independent security sensors may be deployed alongside production-deployed containers to continuously inventory and assess a CSP's security posture. This independent deployment allows the security sensors to maintain broad visibility across containers. Security sensors should be run with sufficient privileges to avoid lack of visibility and false negatives. If utilized, security sensors should be deployed everywhere containers execute to include within registries, as general-purpose sensors, and within CI/CD pipelines. If this approach is taken, the sampling guidance below MAY be applicable.

Registry Monitoring: The container registry MUST be monitored per unique image to ensure that containers corresponding to an image that has not been scanned within the 30-day vulnerability scanning window are not actively deployed on production. As the registry itself is often not a policy control point, this process may be managed by alarms that inform operators or other control mechanisms to prevent unauthorized deployment.

Sampling for Vulnerability Scanning

In order to respond to rapidly changing demands for increases and decreases in cloud resources in this environment, CSPs must maintain rigid change management processes and highly automated mechanisms for deploying system images in large geographically dispersed production environments. This leads to establishing a very short list of standard system images that make up the unique inventory. Usually, vulnerability scans are performed on 100% of these assets, but because of the high fidelity of system configurations across the environments, the scan results of a subset of components can be used to ascertain the state of the entire population. Therefore, a sampling of the assets within each of the standard system images is considered sufficient. An assessor must attest that the sample selected is sufficient to represent the state of the unique inventory and the AO must approve the sample methodology prior to implementation.

A *unique inventory item* is a grouping of one or more discrete inventory assets that are managed as a single asset class. For example, 1,000 servers deployed using the same system build or system image release are considered to be a single, unique inventory item, even if that system build has been updated and only a subset of the 1,000 servers is running the newest version, because the servers are being managed as a single asset class. In these cases, the configuration management plan must identify how the CSP is managing the inventory items and asset classes, ensuring all assets are updated within an appropriate/approved amount of time (limiting the number of different builds/versions in a given asset type). Unique inventory items must be defined as part of the Vulnerability Sampling Plan reviewed by the assessor.

This guidance applies to system builds that are deployed from standard images (that must remain unchanged when pushed to and running on subsequent devices or machines in production) to general purpose servers in highly dynamic virtual, and some physical, environments. The guidance also applies to operating systems deployed to network devices, web applications, databases, and other software products where appropriate.

FedRAMP vulnerability scanning guidelines require at least monthly scans of 100% of inventory components. Vulnerability scanning using sampling targets the same component asset categories but instead requires scanning of a sample attested to represent the unique inventory by an assessor and approved by the AO. Given the risk, FedRAMP recommends that externally accessible (outside of the boundary, without the use of a VPN) system components do not use this sampling methodology; 100% of externally accessible system components should be scanned, using a scanning technology appropriate for the access type (web scanners for web endpoints and portals, network scanners for operating systems, etc.).

The following steps are required for the CSP and assessor to ensure that an appropriate Vulnerability Sampling Plan is implemented, a unique inventory is maintained, components are appropriately selected, scans are performed, and results are reviewed and remediated:

1. **Comply with FedRAMP Requirements for Vulnerability Scans**
2. **Activate Capabilities to Ensure Unique Inventory Items are Identical**
    - The CSP will activate a method to demonstrate that all individual assets in a class are identical; within operational and management parameters.
    - The CSP will provide, to the assessor, a description of the product/method for ensuring unique inventory items are configured appropriately. The CSP will perform a test of the solution to demonstrate effectiveness annually, at time of FedRAMP Annual Assessment of the system, and provide the results to the assessor.
3. **Develop Vulnerability Sampling Plan**
    - Establish a Plan (methodology) by which sampling will be used; the Plan shall be reviewed at least annually, and maintained current.
    - Describe how components will be selected. Justify how the unique inventory item (such as a network device OS version) is built from a standard image and meets the intent of this guideline.
    - Ensure at each selection interval (each month when scans are run), that the assets are selected randomly from the total inventory. Describe the randomization method.

- Describe how this sample effectively represents the entire inventory and satisfies the intent of vulnerability scan requirements.

4. **Establish *Unique Inventory* and Samples:**
   - Establish a list of the *unique inventory*.
   - Ensure each unique inventory item is based on system builds that are deployed from standard images (that must remain unchanged when pushed to and running on subsequent devices or machines in production) to general purpose servers in highly dynamic virtual, and some physical, environments. This also applies to operating systems deployed to network devices, web applications, databases, and other software products where appropriate.
   - Select a sample sufficient to represent the unique inventory item. The sample must be attested to by an assessor at the time of the FedRAMP Annual Assessment.
     - Should the unique inventory change during the year, the CSP will update the Vulnerability Sampling Plan, including documenting how these devices continue to implement previously approved change, deviation, and security controls. Assessors will perform an assessment over the changed inventory at the time of the next FedRAMP Annual Assessment.
     - FedRAMP recommends that 100% of externally accessible (outside of the boundary, without the use of a VPN) system components be scanned. However, if a sampling methodology is approved, there should be a strong justification, given the potential risk.
5. **Analyze Scan Results:**
   - Analyze the scan results to determine whether there was any variance in findings among components within the same unique inventory group outside of documented operational or management parameters. All unexpected variances within a *unique inventory* group must be discussed with the AO with the next Plan of Action and Milestones (POA&M). If applicable, a high-risk POA&M item should be created to investigate and explain why the variance occurred, and correct the unexpected variance. At the discretion of the AO, if the sampling methodology is found to be inefficient (whether through one variance, or multiple variances), the AO may rescind sampling approval, requiring 100% scanning.
6. **Justify Appropriateness of CSP's Participation in "Sampling:"**

- Prior to acceptance to participate in sampling, the CSP should provide a convincing justification that participation is appropriate. This justification should reference all implemented controls that demonstrate adherence with the principles and requirements contained within this vulnerability scan sampling guide, enabling successful adherence to FedRAMP vulnerability scanning requirements testing using sampling.

7. **Assessment and Attestation by Assessor and Approval of Authorization Official:**
   - The assessor will review the CSP's Vulnerability Sampling Plan, implementation and test results and attest to the sampling's effectiveness.
   - The AO for any agency issuing an ATO must approve the plan and justification, prior to participating in sampling.
   - Approval for using sampling can be rescinded by the AO due to identification of weaknesses in the plan, implementation or effectiveness, for example, if an anomaly was identified and a major issue was discovered during the investigation (as part of the high POA&M item).

4. Annual Assessments

Security control CA-2 requires the CSP to undergo an independent assessment of the cloud service offering at least annually. This section describes the FedRAMP Rev 5 annual assessment process and includes guidance for determining the scope and selection of controls to be included in the assessment. This guidance assumes the CSP has already transitioned to, and has undergone an assessment against, the FedRAMP Rev 5 baselines for the cloud offering. CSOs that were last assessed against the FedRAMP Rev 4 baselines must undergo a new full security assessment against the FedRAMP Rev 5 baseline.

Annual Assessment Process Steps

Develop the Assessment Schedule

Most FedRAMP recognized 3PAOs have developed an assessment schedule template to help facilitate this process. Major milestone activities that are typically included in the schedule are described in the sections that follow. The schedule should include timeframes and resources to support technical and quality assurance reviews of all deliverables.

Review and Update Documentation

CSPs must review the SSP and appendices, and update (as necessary) at least annually to incorporate system changes and/or changes in processes and procedures.

***NOTE to CSP and Assessor:** FedRAMP periodically publishes updates to the SAP, SAR (including SRTM and RET) and POA&M templates, so make sure you are using the most recent template when preparing for the annual assessment.*

Incident Response and Contingency Testing

CSPs are required to test the Incident Response Plan (IRP) and Contingency Plan (CP) at least annually. Failure to perform this testing can delay the assessment, so be sure to build this into your schedule.

Define the Assessment Scope

The CSP and assessor work together to define the scope of the FedRAMP Rev 5 annual assessment using the FedRAMP Annual Assessment Control Selection Worksheet. Guidance for completing the worksheet is provided in the template. The completed worksheet must be included in the SAP prepared and submitted by the assessor. The scope of a FedRAMP Rev 5 annual assessment includes:

- FedRAMP-selected list of core controls (as defined in the control selection worksheet)
- CSP-selected controls required to address system changes that have been implemented and/or changed by a CSP since their last assessment (this excludes those controls or portions of controls previously assessed under a significant change within the same annual period)
- Validation of POA&Ms closed since the last assessment
- Validation of POA&Ms identified as vendor dependencies (VDs) or deviation requests (DRs)
- Controls identified as “Not Applicable” (N/A) to validate they are, in fact, not applicable
- Controls that have not been assessed, at least once in a three year period, to ensure controls are meeting periodicity requirements

Develop Security Assessment Plan (SAP)

The assessor prepares and submits the SAP using the FedRAMP Security Assessment (SAP) template. The SAP defines the planned process, procedures, and methodologies for testing. The scope of controls to be tested is based on the control selection process defined in the previous section.

Brief Agency Customers on Assessment Plan

The CSP and assessor brief the agency customers (AOs and/or their representatives) on the assessment plan, scope and schedule. If multiple agencies are leveraging the CSO, schedule the briefing during the monthly collaborative ConMon meeting.

NOTE: Some agencies may want to review the SAP and supporting documentation (e.g., controls section worksheet), so be sure to make these documents available via the secure repository.

Conduct the Security Assessment and Develop SAR

When developing the assessment schedule, be sure to build in time for developing the draft SAR, CSP remediation activities, assessor remediation testing, and final SAR development.

The assessor prepares and submits the SAR and supporting documents using the following templates:

- FedRAMP Security Assessment Report (SAR) Template*
- Depending on the impact categorization:
  - FedRAMP SAR Appendix B - Low Security Requirements Traceability Matrix Template
  - FedRAMP SAR Appendix B - Moderate Security Requirements Traceability Matrix Template
  - FedRAMP SAR Appendix B - High Security Requirements Traceability Matrix Template
- SAR Appendix A - FedRAMP Risk Exposure Table (RET) Template

In accordance with the SAP, the SAR documents the actual process, procedures, and methodologies followed during the assessment, the assessment results, risks corrected during testing, and risks that remained at the conclusion of the assessment.

* For LI-SaaS cloud offerings, the control implementations, assessment test procedures, and assessment results are combined into one document using the SSP Appendix A - LI-SaaS FedRAMP Security Controls template. To facilitate agency customer reviews, FedRAMP recommends aggregating the remaining risks using the RET template.

Complete Plan of Action and Milestones (POA&M)

The CSP prepares and submits the POA&M using the FedRAMP Plan of Action and Milestone (POA&M) Template. The CSP documents residual risks identified in the SAR and defines a plan for remediation of those risks in the POA&M.

5. Significant Changes

During continuous monitoring, CSPs may need to make changes to the system. A "significant" change is one that is likely to affect the security state of the system. CSPs document significant changes, conduct a security impact analysis, and - depending on the type of change - implement the significant change process steps described in this section.

Types of Changes

A significant change is defined in NIST SP 800-37 Rev. 2 as "a change that is likely to substantively affect the security or privacy posture of a system." FedRAMP has defined three types of significant changes: Routine Recurring, Transformative, and Adaptive. Routine Recurring changes do not require review and approval by agency authorizing officials (AOs). Transformative and Adaptive changes require review and approval.

Routine Recurring Changes

This type of change is performed regularly and routinely by CSPs to address flaws or vulnerabilities, address incidents, and generally perform the typical maintenance and service delivery changes expected during day-to-day operations.

These changes leverage mature processes and capabilities to identify, mitigate, and remediate risks as part of the change. They are often entirely automated and may occur without human intervention, even though they have an impact on security of the service.

If the activity does not occur regularly and routinely then it cannot be a significant change of this type. For example, replacing all physical firewalls to remediate a vulnerability is obviously not regular or routine.

Routine recurring changes generally occur as part of ongoing operations or vulnerability management.

Ongoing operations

Key Tests:

- Routine care and feeding by staff during normal duties
- No major impact to service availability
- Does not require executive approval

Examples:

- Provisioning or deprovisioning capacity to support service elasticity
- Changing or tuning performance configurations for instances or services
- Updating and maintaining operational handling of information flows and protection across physical and logical networks (e.g., updating firewall rules)
- Generating or refreshing API or access tokens

Vulnerability Management

Key Tests:

- Minor, incremental patching or updates
- Significant refactoring or migration process NOT required
- No breaking changes

Examples:

- Updating security service or endpoint signatures
- Routine patching of devices, operating systems, software or libraries
- Updating and deploying code that applies normal fixes and improvements as part of a regular development cycle
- Vulnerability remediation activity that simply replaces a known-bad component(s) with a better version of the exact same thing, running in the exact same way with no changes to processes

Transformative Changes

Activities that match the *transformative* significant change type are rare for a cloud service offering, adjusted for the size, scale, and complexity of the service. Small cloud service offerings may go years without transformative changes, while hyperscale providers may release multiple transformative changes per year.

Key Tests:

- Alters the service risk profile or requires new or significantly different actions to address customer responsibilities
- Requires significant new design, development and testing with discrete associated project planning, budget, marketing, etc.
- Requires extensive updates to security assessments, documentation, and how a large number of security requirements are met and validated

Examples:

- The addition, removal, or replacement of a critical third party service that handles a significant portion of information (e.g., IaaS change)
- Increasing the security categorization of the entire offering or a service within the offering that actively handles federal customer data
- Replacement of underlying management planes or paradigm shift in workload orchestration (e.g., bare-metal servers or virtual machines to containers, migration to kubernetes)
- Datacenter migration where large amounts of federal customer data is moved across boundaries different from normal day-to-day operations
- Adding a new AI-based capability that impacts federal customer data in a different way than existing services or capabilities (e.g., integrating a new third-party service or training on federal customer data)

Adaptive Changes

Activities that match the *adaptive* significant change type are a frequent and normal part of iteratively improving a service by deploying new functionality or modifying existing functionality in a way that is typically transparent to customers and does not introduce significant new security risks.

In general, most changes that do not happen regularly will be adaptive changes. This change type deliberately covers a wide range of activities in a way that requires assessment and consideration.

Key Tests:

- Requires minimal changes to security plans or procedures
- Requires some careful planning and project management to implement, but does not rise to the level of planning required for transformative changes
- Requires verification of existing functionality and secure configuration after implementation

Examples:

- Updates to operating systems, containers, virtual machines, software or libraries with known breaking changes, complex steps, or service disruption
- Deploying larger than normal incremental feature improvements in code or libraries that are the work of multiple weeks of development efforts but are not considered a major new service
- Changing cryptographic modules where the new module meets the same standards and characteristics of the former
- Replacing a like-for-like component where some security plan or procedure adjustments are required (e.g., scanning tool or managed database swap)
- Adding models to existing approved AI services without exposing federal customer data to new services

Significant Change Process Steps

This section describes the steps taken by CSPs, assessors and agency AOs (or their designees) for transformative and adaptive changes. The steps may be altered under certain circumstances. For example, CSPs with multiple agency customers may define a slightly different process in the Collaborative ConMon Charter, whereby the review/approval of SCRs is performed by voting members. In some cases, the AO may be willing to accept an assessor attestation letter in place of the SAP and SAR. These are typically for adaptive significant changes that are small in scope (i.e., impacts a small number of controls). CSPs and assessors must first consult with their AO POCs to confirm that an assessor attestation is appropriate and acceptable for the SCR.

1. CSP and AO meet to discuss the significant change, potential security impacts and any increases in risk posture to the current authorization from the CSP's perspective. To facilitate the discussion, the CSP provides a Security Impact Analysis which includes an estimate of known and potential security changes, and the security impact associated with these changes (reference CM-4).
2. If the AO and CSP agree that the change is routine recurring in nature, the CSP proceeds with normal monthly ConMon activities. If they determine the change is transformative or adaptive, the CSP documents the Significant Change Request (SCR) and begins the process to engage an assessor. FedRAMP does not provide a SCR template. However, the SCR must include at least the following information:
    a. Service Offering FedRAMP ID
    b. Assessor Name
    c. Related POA&M (if the change is being implemented to address a known risk)
    d. Significant Change type and explanation of categorization
    e. Short description of change
    f. Reason for change
    g. Summary of customer impact, including changes to services and customer configuration responsibilities
    h. Plan and timeline for the change, including for the verification, assessment, and/or validation of impacted security controls
    i. Copy of the security impact analysis
    j. Name and title of CSP approver (typically the system owner)
3. Assessor begins to assess the impact of the proposed change on system functionality and security by reviewing the SCR and other relevant system security documentation.
4. Assessor develops a Security Assessment Plan (SAP) which documents the scope of the assessment.
5. The SCR and SAP are submitted to the AO for review and approval.
6. Once approved, the CSP implements the change while ensuring minimal security impact to the existing environment.

7. Once implemented, the assessor conducts testing, develops a SAR package, and briefs the CSP and AO on the outcome of the assessment.
8. The AO reviews the SAR package and determines if the change is acceptable (i.e., no impact to the security posture of the system). If not, the CSP would be required to remediate risks or roll back to the previous version. If the change is accepted, then the CSP must update the POA&M with any conditions. All other documentation must be updated no later than the next Annual Assessment.
9. CSP continues with normal ConMon operations.

Scheduling Significant Changes with Annual Assessments

With buy-in from the AO(s), significant changes may be scheduled with the annual assessment (AA). The process and requirements follow those described above, except that the SAP will include the assessment plan for both the AA and the significant change. Similarly, the AA SAR will incorporate the results of the AA as well as the results for the significant change.

Assessment Reuse

Under certain conditions, assessment results from an out-of-cycle significant change assessment may be reused for the current annual assessment. The conditions for reuse of assessment results are the following:

- The change occurred between the last and current annual assessments
- The change was approved by the AO
- The assessment results for reuse are only NIST 800-53 controls assessment results (not scans or pen test results etc)
- The change documentation is not an attestation

If assessment results from an approved significant change were reused for the annual assessment, the approved SAR and supporting documentation for that significant change must be included and referenced as artifacts in the annual assessment package.

6. Incident Communications

This section describes the steps FedRAMP stakeholders must use when reporting information related to security incidents, including responses to published emergency directives. The steps included in this document provide a sequence of required communications that are in place to ensure accurate and timely information is reported to all relevant stakeholders.

Incident communications stakeholders include a variety of teams and individuals with a vested interest in the successful implementation and operations of FedRAMP. They include:

- CSPs
- FedRAMP
- Cybersecurity and Infrastructure Security Agency (CISA)
- CSP customers (including federal and other FedRAMP-Authorized CSPs)
- Interconnected systems

The Federal Information Security Modernization Act of 2014 (FISMA) is the authoritative source for incident definitions. FISMA defines an "incident" as "an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." The terms “security incident” and “information security incident” are also used interchangeably with “incident” within the body of the law.

Clear and timely incident communication to stakeholders is a key aspect of ConMon to ensure that incident handling is transparent and stakeholders are aware of the current status and remediation efforts.

FedRAMP requires CSPs to report any incident (suspected or confirmed) that results in the actual or potential loss of confidentiality, integrity, or availability of the cloud service, including the impact to federal customer data that it stores, processes, or transmits. Reporting real and suspected incidents allows agencies and other affected customers to take steps to protect important data, to maintain a normal level of efficiency, and to ensure a full resolution is achieved in a timely manner.

Reporting suspected or confirmed incidents, as well as responses to emergency directives to stakeholders, does not result in punitive actions against the CSP; however, failure to report incidents will result in escalation actions as defined in Section X of this playbook. A collaborative

approach to reporting incidents between CSPs and other stakeholders allows all parties to be aware of, and successfully manage, the risk associated with an incident and to classify and resolve suspected incidents.

Assumptions

- Key CSP personnel have been identified and are trained in their relevant incident roles and responsibilities
- Agency incident response plans are in place
- CSP incident response plans are in place and have been tested in accordance with FedRAMP incident response (IR) controls
- Both internal and external incident response contact lists (in all incident response plans) are accurate and up-to-date
- CSP contact information is up-to-date and on file with FedRAMP and all federal customers of a CSP's FedRAMP-Authorized services

Roles and Responsibilities

The following table describes the stakeholder roles and responsibilities in the incident communication process.

Stakeholder	Role	Responsibility
CISA	Risk Advisor and Incident Handling	• Coordinates security and resilience efforts across private and public sectors • Delivers technical assistance and assessments to federal stakeholders and infrastructure owners nationwide • Conducts nationwide outreach to support and promote the ability of emergency response providers and relevant government officials in the event of an emergency • Provides incident handling assistance, as needed, to CSPs and agencies • Provides reporting for any identified incidents affecting government or government contracted systems to appropriate stakeholders
FedRAMP	Incident	• Monitors incident reporting submissions to FedRAMP

	Communication Monitoring	• Updates FedRAMP Marketplace with status of CSP CAPs, suspensions, and revocations, including those related to information security incidents • Supports and advises AOs as needed
Agency AO	Risk Monitoring	• Provides CSP status updates to FedRAMP, including CAPs, suspensions, and revocations • Acts as the final approval authority for the use of an offering by their agency • Notifies CSP, CISA, and FedRAMP stakeholders if the agency becomes aware of an incident or suspects an incident that a CSP has not yet reported • Ensures requirements for agency-specific incident response plans are met • Confirms with a CSP that they reported an incident to CISA and has obtained a CISA tracking number
CSP	Service Provider	• Protects incident information commensurate with the impact level of the cloud service • Maintains a satisfactory risk management program for the cloud service in accordance with FedRAMP • Complies with incident response guidance and requirements • Maintains a list of all current customers and the proper communication channels with all AOs and assessors • Notifies affected customers of information security incidents • Notifies CISA of information security incidents as needed (see the CSP General Reporting Process section) and provides the CISA tracking number to FedRAMP at fedramp_security@gsa.gov (as well as to all applicable stakeholders) of information security incidents and provides status updates thereafter • Requests assistance from CISA, as needed • Provides a final report to FedRAMP at fedramp_security@gsa.gov (as well as to all applicable stakeholders), including the agency AO or AO representatives, after completion of the Post-Incident Activity phase of the Incident Response Life Cycle • Responds to emergency inquiries from FedRAMP, including those that are the result of the issuance of CISA Emergency Directives
Assessor	Independent Assessor	• Performs any required independent security assessments related to information security incidents

CSP General Reporting Process

CSPs must report all incidents, which include any suspected or confirmed events, that result in the potential or confirmed loss of confidentiality, integrity, or availability to assets or services provided by the service offering. Reporting requirements to CISA, agency customers and FedRAMP are identified in this section.

As CSPs manage and report incidents, they must not deviate from FedRAMP requirements to protect the confidentiality, integrity, or availability of data stored, processed, or transmitted by the system as well as data about the system and related to the incident. Sensitive information must be provided using approved mechanisms. CSPs must report suspected and confirmed information security incidents to the following parties **within one (1) hour** of being identified by the CSP's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or information technology department to the following stakeholders:

- Customers who are impacted or who are suspected of being impacted (via the CSP Incident Information and Forms folder in their respective FedRAMP Secure Repository)
- CISA, under the following conditions:
    - The CSP has confirmed, has yet to confirm, or suspects the incident is the result of any of the attack vectors listed at Federal Incident Notification Guidelines | CISA
    - Reporting location: https://www.cisa.gov/forms/report
- FedRAMP at fedramp_security@gsa.gov
- Agency POCs to include AOs, AO representatives, and Agency Incident Response Teams (as identified by the authorizing agency)

FedRAMP encourages the use of automated mechanisms for incident reporting. If a CSP wants to leverage automated incident reporting mechanisms, the CSP must work with the AO and FedRAMP to ensure the content and context of the automated reporting provides the required information.

CSPs must maintain current and accurate contact information on file for all POCs including FedRAMP, agency customers, and other applicable stakeholders. The CSP must provide the tracking number to all POCs as soon as it is made available by CISA. Incident notifications, provided by the CSP to any POCs verbally (e.g., by phone) must be followed up by an email; however, sensitive information must be protected.

When reporting to CISA, CSPs must include the required data elements as well as any other available information. CSPs must submit incident notifications in accordance with the Submitting Incident Notifications section of https://www.cisa.gov/federal-incident-notification-guidelines. In some cases, it may not be feasible to have complete and validated information prior to reporting. CSPs should provide their best estimate at the time of notification and report updated information as it becomes available.

After initial incident notification, the CSP must provide updates to CISA as well as daily updates to all POCs. The final daily update must be provided to all POCs after the CSP has completed the Recovery phase of Incident Response Life Cycle (Containment, Eradication, Recovery, and Post-Incident Activity). The CSP must also provide a report to all POCs after it has completed the Post-Incident Activity in the Incident Response Life Cycle. The final report must describe what occurred, the root cause, the CSP's response, lessons learned, and changes needed.

Additionally, CSPs are responsible for responding to emergency inquiries from FedRAMP, including those that are the result of the issuance of CISA Emergency Directives. If any emergency inquiry is issued, the CSP must comply within the timeline described in the request. Any additional reporting requirements identified in the inquiry must also be met. If there are any explicit actions the CSP must take that are identified in the emergency inquiry, they must be addressed in the timeline prescribed. Failure to report or respond to emergency inquiries, or failure to perform the prescribed remediation actions, can result in the escalation actions outlined in Section 8 of this playbook.

AO Responsibilities

Upon receipt of a CSP's notification, AOs must take the following actions:

1. Verify that, if required, CISA has been notified
2. Request that the CSP provides daily updates and the CISA tracking number when it has become available
3. Verify the CSP's notification and supporting documentation is posted to the Incident Information and Forms folder in the FedRAMP secure repository
    a. Notifications of incidents should be sent to the following FedRAMP POCs after each update, should not contain any sensitive data, and should direct POCs to the CSP's designated FedRAMP secure repository:
        i. FedRAMP at fedramp_security@gsa.gov

ii. AO and applicable team members (contact information on file with the CSP)

The AO will evaluate the final report submitted by the CSP and determine an appropriate path forward. This may include developing a plan of action and milestones (POA&Ms) and/or CAPs to address areas needing improvement.

7. Collaborative ConMon

The FedRAMP High, Moderate and Low baselines require CSPs to develop a ConMon strategy that complies with the requirements defined in CA-7, Security Assessment and Authorization | Continuous Monitoring.

FedRAMP does not currently have the capacity to actively monitor continuous monitoring for all Rev 5 FedRAMP Authored services. Each agency that issues an ATO or Authorization to Use (ATU) for the CSO is responsible for performing oversight for their use of the system to ensure the security posture remains sufficient for its own use and supports an ongoing authorization.

For CSOs that have more than one active ATO/ATU on file with FedRAMP, CA-7 requires the CSP to implement a Collaborative ConMon approach. Collaborative ConMon benefits both agencies and CSPs:

- **Agency Benefits:** Allows agencies to share responsibility for ConMon oversight and make better risk-based decisions through collaboration
- **CSP Benefits:** Creates a central forum for addressing questions related to the CSP's ConMon activities, and achieving consensus on Deviation Requests (DRs), Significant Change Requests (SCRs) and the Annual Assessment (AA) - versus having to coordinate with each agency separately.

FedRAMP has worked with a number of CSPs to successfully implement Collaborative ConMon. In doing so, we have found there is no "one size fits all" approach. Therefore, this guide provides a framework that CSPs can leverage to develop their own Collaborative ConMon process. At a minimum, CSPs must include the following key elements in their Collaborative ConMon process.

Step 1: Develop Collaborative ConMon Draft Charter

The charter defines the process for conducting Collaborative ConMon. The draft charter should be shared with the member agencies ahead of the inaugural Collaborative ConMon meeting (see Step 2) for review and feedback. At a minimum, the charter should include the following sections, but

CSPs and agencies are free to include additional sections or subsections to further define the Collaborative ConMon process:

Section 1: Collaboration Group Member Contact Information

In addition to the CSP, membership includes one or more security representative(s) from each agency. This may include the Authorizing Official (AO) at each agency; however, AOs typically delegate this responsibility to Information System Security Officers (ISSOs) on the Chief Information Officer's (CIO's)/Chief Information Security Officer's (CISO's) team. The Collaboration Group membership will change over time as new agency customers are onboarded or discontinue using the cloud service.

NOTE: You should already have direct points of contacts (POCs) at each agency as part of your Incident Response Plan, but the PMO recognizes that POC information may become outdated with employee turnover. Feel free to contact the PMO if you need help identifying security POCs at your member agencies.

Independent assessors are not typically included as members of the Collaboration Group unless you are using an assessor in a consulting role to perform ConMon activities. Assessors may be asked to attend Collaborative ConMon meetings on an ad hoc basis - for example, to brief the results of the Annual Assessment.

Section 2: Meeting Schedule

The PMO recommends holding a monthly, one-hour recurring Collaborative ConMon meeting. To ensure high participation, we recommend scheduling the recurring meeting on Tuesday, Wednesday, or Thursday and in the early afternoon (EST) to accommodate different time zones.

NOTE: It may not be necessary for a CSP to meet each month with their agency customers if there are no substantial changes to the system or vulnerabilities identified. In such cases, the CSP can simply post their Continuous Monitoring reports to their respective repository and inform customers that the meeting is not being held that month.

Section 3: Meeting Agenda

A typical agenda for the monthly collaborative ConMon meeting includes:

- Summary of monthly vulnerability scan results
- Discussion of past due POA&Ms and any new POA&Ms that are dependent on a downstream vendor (i.e., Vendor Dependencies)

- Open Deviations Requests (DRs) pending approval (Operational Requirements, Risk Adjustments, False Positives)
- DRs newly approved
- Significant Change Requests (SCRs) (planned changes, changes pending approval, status of implementation and testing)
- Annual Assessment (scope of upcoming assessment, brief out assessment results)
- Status of Incident Handling/Response, Cybersecurity and Infrastructure Security Agency (CISA) Emergency Directive, etc. (if applicable)
- Agency-specific reporting requirements (if applicable)
- Question & Answer (Q&A)

A good way to disseminate this information is in a summary report that agency representatives can use to brief their respective AOs on the security posture of the cloud offering.

Note: It is not practical to cover every POA&M item, particularly those you intend to remediate within the FedRAMP-prescribed timeframes. The focus of the POA&M discussion should be the status of any past due POA&Ms, Vendor Dependencies, and Deviation Requests - most importantly, any areas that require risk acceptance.

Be sure to differentiate between changes that impact all agency customers versus a specific agency. For example:

- A Low->Moderate or Moderate->High “uplift” is considered a significant change. Oftentimes, uplifts are requested by a single agency with a use case at the higher impact level. In this scenario, all agency customers should be made aware of the change, but the requesting agency should take the lead on reviewing and approving the SCR, reviewing the assessment results, and issuing an ATO at the higher impact level.
- From time to time, CSPs choose to add services or features to the authorization boundary through the significant change process. This may be done at the request of one or more existing agency customers OR as an effort to expand the CSP’s offering to attract new customers. If the latter, CSPs should not assume that existing agency customers will approve the addition of services/features. This is something that needs to receive buy-in from existing agency customers along with a commitment to review and approve the SCR,

review the assessment results and issue an updated ATO that covers the expanded offering. Otherwise, the CSP will be required to find an agency willing to review the SCR and issue an ATO that covers the expanded offering.

Section 4: ConMon Deliverables

The PMO recommends uploading the monthly ConMon deliverables (summary report, vulnerability scan files, updated POA&M and Inventory, DRs, SCRs) on the same day each month and then hold the recurring meeting a week later. This will give each agency representative time to review the deliverables and come to the meeting ready with questions and recommendations for DR/SCR approvals.

Section 5: Decision-Making Authorities

Determining how decisions are made, and by whom, is a critical part of the Collaborative ConMon process. While it's important to give each agency a voice, it is not always practical or in the best interest of security to seek unanimous agreement - particularly if the issue at hand only affects a single agency. Most CSPs that have successfully implemented Collaborative ConMon have used one of two approaches (or some combination) to decision making.

Voting Members: During the inaugural Collaborative ConMon meeting, the collaboration group grants certain members decision-making authority for DRs, SCRs, or any other area that requires agency approval. Oftentimes, agency representatives will volunteer to take on this responsibility. Depending on the number of agency customers, the PMO recommends at least two (2) or more voting members share this responsibility.

Comment Period: Some collaboration groups have agreed to a "comment period" approach, whereby all group members are allowed an agreed upon period of time to raise questions, concerns or objections. If there are no objections when the time period ends, the matter is considered approved. The PMO recommends giving group members two weeks. For any group members that were unable to attend the monthly meeting, two weeks will allow those members to review the relevant documentation. This approach typically works as follows:

- The CSP makes information (e.g., DR, SCR, etc.) available via the FedRAMP secure repository at least one week prior to the monthly Collaborative ConMon meeting and then notifies all group members.
- During the monthly Collaborative ConMon meeting, the CSP briefs all group members on DR, SCR, etc. and holds room for Q&A.

- After the monthly meeting, the CSP sends a follow up email that summarizes the discussion topics and reminds group members of the window of time to ask any follow up questions. After the defined Q&A period has ended, the CSP sends a follow-up email, informing group members that no objections were raised; therefore, the DR, SCR, etc. is considered approved.

Section 6: Agency-specific ConMon requirements

The charter should identify additional ConMon requirements that the member agencies need to meet their own agency-specific reporting requirements. Agency-specific requirements above and beyond the FedRAMP baselines should be documented in the contract and/or ATO letter.

Section 7: ConMon Performance Management

While it is ultimately up to each agency Authorizing Official to maintain or revoke an ATO, this section can be used by the collaboration group to define performance triggers and associated escalation levels (for example, Corrective Action Plan "In Remediation" status) when the CSP fails to comply with FedRAMP's continuous monitoring requirements or the agreed upon charter. The PMO recommends using the process defined in Section 8 of this playbook as the basis for this section.

Step 2: Hold Inaugural Collaborative ConMon Meeting

The goal of the inaugural Collaborative ConMon meeting is to introduce collaboration group members and achieve consensus on the draft charter. Keep in mind that agency representatives may have different opinions on the scope and structure of Collaborative ConMon. The PMO has found that most agencies are agreeable to holding monthly recurring meetings that cover the typical agenda described above. In addition, most agencies are agreeable to some form of the decision-making approaches described above. However, keep in mind that you may have to go through a couple iterations before the charter is finalized.

Step 3: Finalize Collaborative ConMon Charter

Once feedback from agency representatives has been received and incorporated into the draft charter, upload the final Collaborative ConMon Charter to the top-level ConMon folder in your secure repository and notify the collaboration group. Remember, as agency representatives join or leave the collaboration group, the charter should be updated to reflect the current member contact information. Maintaining an updated list of agency POCs is critical for effective communication in the event of a security incident, emergency directive, etc.

Step 4: Hold Monthly Recurring Collaborative ConMon Meetings

Now that you have identified collaboration group members and achieved consensus on the Collaborative ConMon Charter, you are ready to hold monthly recurring Collaborative ConMon meetings. Here are some tips for ensuring a smooth Collaborative ConMon process:

- Upload deliverables to the secure repository at least one week prior to the meeting and remind the collaboration group to review the information prior to the meeting, especially if there are new areas that require discussion and approval, such as DRs and SCRs. Be sure to provide a link to the secure repository in the email notification.
- Follow the typical agenda described above, but feel free to adjust it as needed. For example, you may use the meeting time to brief the results of the annual assessment (AA) or testing associated with a significant change. Be sure to invite the assessor to these types of meetings.
- When you receive a new Agency ATO, forward it to the PMO at ato-letter@fedramp.gov and then invite the Agency AO to the monthly Collaborative ConMon meetings. Be sure to email the AO, explaining the meeting purpose and goals. The AO may choose to delegate this responsibility to members of the CIO/CISO team.
- As collaboration group members join/leave the group, update the charter and monthly meeting invite. Keep in mind, as new agency representatives join the group, they may have different opinions about the scope and structure of the Collaborative ConMon process you have defined. Be open, flexible, and willing to make adjustments.
- With enough notice, the PMO can attend monthly Collaborative ConMon meetings on an as-needed basis to provide guidance.

8. ConMon Performance Management

This section describes escalation triggers and actions when a CSP is not meeting ConMon requirements for its FedRAMP authorized CSO. It also includes recommended actions to take when a CSP fails to maintain an adequate ConMon capability for an authorized CSO.

In addition to meeting FedRAMP ConMon requirements, CSPs are required to address additional conditions specified in the Agency ATO letter.[1]

Failure to adhere to FedRAMP ConMon requirements and conditions in the ATO letter may result in escalation actions by either your federal agency customer or FedRAMP or both.

NOTE: The term "Agency AO" is used throughout this section; however, specific actions may be taken by the Agency AO, the AO's representative, or collaborative ConMon group.

Performance Management for Ongoing Authorization

This section provides a recommended process to help agencies perform oversight of CSOs authorized via the FedRAMP agency authorization path.

NOTE: The initial authorizing agency (aka "partner" or "sponsor") is not responsible for performing ConMon oversight on behalf of subsequent authorizing agencies. Each agency that issues an ATO, or authority to use (ATU), for a cloud offering must review the CSP's ConMon activities to ensure the security posture remains sufficient for its own use and supports an ongoing authorization. This includes:

- Reviewing the monthly POA&Ms
- Approving deviation requests
- Approving significant change requests; and
- Reviewing the results of the annual assessment.

For CSPs with more than one agency ATO/ATU, security control CA-7 | Continuous Monitoring requires the CSP to implement the collaborative ConMon approach described in Section 7 of this playbook.

Agencies should implement an escalation process to monitor their authorized CSOs, which may result in one of the following escalation levels[2]:

[1] Agency AOs are encouraged to use the FedRAMP ATO Letter Template which includes these requirements. Additional requirements may be included in an agency ATO letter to address system-specific security concerns identified during an assessment.

[2] Agency AOs (or collaborative ConMon groups) should determine which escalation levels are appropriate.

- **Detailed Finding Review (DFR):** A request from an agency AO for a CSP to assess a deficiency and report the cause and remedy. If the CSP does not resolve a DFR within the agreed upon timeframe, the agency AO may escalate to a corrective action plan (CAP).
- **CAP:** A request from an agency AO for a CSP to perform a root-cause analysis and provide a formal plan for remediation. If the CSP does not resolve a CAP within the agreed upon timeframe, the agency AO may suspend or revoke the CSO's ATO(s).
- **Suspension:** A decision by an agency AO to temporarily suspend a CSO's ATO(s) until the identified deficiencies are resolved. In this phase, an agency may choose to suspend use of the CSO. If the CSP does not resolve a suspension within the agreed upon timeframe or if the agency AO determines the CSP can no longer meet FedRAMP compliance requirements, the agency AO may revoke the CSO's ATO(s).
- **Revocation:** A decision by an agency AO to revoke a CSO's ATO and migrate the data to another CSO.

When an agency AO identifies a deficiency in the CSP's ConMon capabilities, the following escalation process should be initiated:

1. The agency AO identifies a deficiency with a CSP's ConMon capability.
2. The Agency AO reviews the deficiency and compares it to the CSP's past ConMon performance. As a result of the review, the agency AO decides on one of the following actions:
    a. The agency AO may elect to simply monitor the CSP more closely and take no further action. If so, no notice is sent and the process stops here;
    b. The agency AO may increase a CSP's existing escalation level; for example, a CSP on a CAP may face Suspension; or
    c. The agency AO may determine the deficiency is severe enough to make the escalation effective immediately in which case, steps 3 and 4 are skipped.
3. The agency AO notifies the CSP of the deficiency and the agency AO's intended escalation.
4. The CSP responds to the notification. The CSP's response should include any information that may rebut the escalation decision. Depending on the intended escalation level, the CSP's response must come from:
    a. The CSP's security POC for a DFR; or

b. The CSP's system owner for a CAP, Suspension, or Revocation.

5. The agency AO reviews and adjudicates the CSP's response, and renders a formal escalation decision.
6. The Agency AO notifies the CSP of its decision. If the agency AO decides to follow through with an escalation, this notice:
    a. Identifies the criteria for returning the CSO to a Satisfactory status. It may also include a deadline by which the CSP must fully satisfy the criteria or face more severe escalation; and
    b. Requires certain actions from the CSP. Typically, an agency AO would require the CSP to perform a root-cause analysis and develop a formal plan for addressing the deficiencies.
7. The CSP responds to the Agency AO notification. This response must include:
    a. The results of the root cause analysis;
    b. The CSP's plan for fully resolving the issues, with clearly established milestones and dates, including a date of full resolution;
    c. For a CAP or Suspension, the system owner's signature on the plan and agency AO approval of the plan; and
    d. Any other items as specified by the agency AO in the notification.
8. When a CSP is subject to escalation as described above, the following occurs:
    a. Notification to FedRAMP: Agency AOs must notify FedRAMP at info@fedramp.gov if a decision is made to initiate Suspension or Revocation. CAP letters should be uploaded to the FedRAMP secure repository.
9. When the agency AO determines the CSP has fully resolved the cited deficiencies and satisfied the identified criteria communicated in the notification, the agency AO must take the following actions:
    a. Notification to FedRAMP: Agency AOs must notify FedRAMP at info@fedramp.gov if an escalation has been resolved. CAP release letters must be posted to the FedRAMP secure repository.

Agency Performance Management Deficiency Triggers

To ensure consistent expectations and enforcement, an agency AO should define performance management deficiency "triggers." An agency can pick and choose the appropriate triggers. Examples are described in the table below.

Table 1. Agency Performance Management Deficiency Triggers

Process Area	Deficiency Trigger	Minimum Escalation Level
Operational Visibility	**Unique Vulnerability Count Increase** 20% from ATO baseline or 10 unique vulnerabilities, whichever is greater. Note: A request to re-baseline a unique vulnerability count, accompanied with proper justification, can be submitted to the agency, and may be approved on a case-by-case basis.	DFR
	Non-compliance with scanning requirements outlined in FedRAMP Vulnerability Scanning Requirements. **First incident in the previous six months.** Unauthenticated scan results delivered as part of the initial SAR submission, as part of the annual SAR submission, or as part of the monthly scanning submission, where the unauthenticated scans are 10% or greater of the total scan submission. This applies only to a CSP's first submission that is non-compliant with authenticated scan requirements.	DFR
	Non-compliance with scanning requirements outlined in FedRAMP Vulnerability Scanning Requirements. **Each subsequent incident beyond the first within the previous six months.** Unauthenticated scan results delivered as part of the initial SAR submission, as part of the annual SAR submission, or as part of the monthly scanning submission, where the unauthenticated scans are 10% or greater of the total scan submission, result in a CSP being placed on a CAP, when a second or subsequent CSP submission is non-compliant with authenticated scan requirements.	CAP

	Late Remediation High Impact Vulnerabilities Five or more unique vulnerabilities or POA&M items aged greater than 30 days.	DFR
	Late Remediation High Impact Vulnerabilities Five or more unique vulnerabilities or POA&M items aged greater than 60 days.	CAP
	Late Remediation Moderate Impact Vulnerabilities Ten or more unique vulnerabilities or POA&M items aged greater than 90 days.	DFR
	Late Remediation Moderate Impact Vulnerabilities Ten or more unique vulnerabilities or POA&M items aged greater than 120 days.	CAP
	Late Delivery of Annual Assessment SAP Delivery of annual assessment SAP less than 60 days before annual ATO anniversary date.	CAP
	Late Delivery of Annual Assessment Package Delivery of full annual assessment package after annual ATO anniversary date.	CAP
	Poor Quality of Deliverables Untimely or inaccurate submission of any deliverable, including (but not limited to) monthly ConMon documents, deviation requests, or significant change requests.	DFR
	Lack of Transparency Failure to report known issues to FedRAMP or purposely manipulating scans to avoid risk management deficiency triggers.	CAP
	Multiple Recurrences Any trigger that is realized multiple times within a six-month timeframe.	CAP
	Insufficient Notice of Planned Change Notification received less than 30 days before the planned change or insufficient documentation of a security impact analysis.	CAP
Change Control	**Late Notice of Emergency Change** Notification received more than five days after the change.	CAP

	Undocumented/Unreported Change No notification.	CAP
	Degradation of the Change Management and Change Control Processes Insufficient adherence to the provided configuration management plan as determined by FedRAMP.	DFR
Incident Response	**Late Incident Notification** Late notification of incident not in accordance with Section 6 of this playbook.	CAP
	Late response to Cybersecurity and Infrastructure Security Agency (CISA) Emergency Directives Failure to respond to CISA Emergency Directives within prescribed timeframes.	CAP
	Incident Frequency of Recurring Type Any incident with recurring type and/or cause	CAP
	Incident Frequency Four or more incidents within six months	DFR
	Timely and Ongoing Notification of Zero-day Attack Failure to provide to FedRAMP daily updated progress in addressing zero-day attacks	CAP

FedRAMP Responsibilities for Agency ATOs

The FedRAMP PMO monitors agency packages to ensure that the service remains in good standing. Specifically, FedRAMP ensures:

- The annual assessment package is uploaded and complete;
- The latest SAR recommends continued authorization; and
- The FedRAMP Marketplace and repository appropriately reflects authorization, suspension, and revocation status.