



FedRAMP

# Agency Authorization Kickoff/SAR Debrief Guidance

**For Agency Authorizations**

Last updated: 7/19/2024



[info@fedramp.gov](mailto:info@fedramp.gov)

[fedramp.gov](https://fedramp.gov)

FedRAMP provides this guidance to inform the development of briefing materials for a FedRAMP Authorization Kickoff/SAR Debrief

## **How to Use**

CSPs and 3PAOs use this guidance to inform the development of a slide briefing for a Kickoff, SAR Debrief, or combined Kickoff/SAR Debrief.

A prepared briefing should follow the general flow and topic progression of this guidance document.

CSPs/3PAOs prepare the briefing using their own company branded template, addressing the content described in this guidance.

FedRAMP provides this guidance to inform the development of briefing materials for an Agency Authorization Kickoff/SAR Debrief

## What to Prepare

**Kickoff only:** The briefing is delivered by the CSP and should be appropriate for a 60 minute discussion focused on the cloud service offering's architecture, boundary, data flows, and security capabilities.

**SAR Debrief only:** 3PAOs prepare slides that describe the security assessment plan and results. CSPs prepare slides that describe the remediation plan and timeline for residual risks, as well as any risk deviations that require AO approval. The briefing should be appropriate for a 70-minute discussion.

**Combined Kickoff/SAR:** The briefing should be appropriate for a 30 minute Kickoff discussion focused on the cloud service offering (CSP content), followed by a 60 minute discussion focused on the SAR Debrief which includes portions from the 3PAO and CSP.



# CSP Content

**CSPs must address the content in the slides that follow to fulfill the Kickoff portion of this slide deck**

A Kickoff or Combined Kickoff/SAR Debrief will begin with a review of the meeting's purpose and outcomes, followed by a round of introductions. These meetings include stakeholders from the Agency, CSP, and 3PAO.

CSP	3PAO	Agency
<ul style="list-style-type: none"><li>• Program Manager / Authorization Lead</li><li>• Security/Compliance Lead</li><li>• Technical SMEs</li></ul>	<ul style="list-style-type: none"><li>• 3PAO Advisor / Consultant</li><li>• 3PAO Assessors and Pen Tester*</li></ul>	<ul style="list-style-type: none"><li>• Agency Authorization Lead</li><li>• Agency Liaison</li><li>• Authorizing Official</li><li>• ISSO / ISSMs</li><li>• Technical Reviewers</li><li>• Agency Business Owner**</li></ul>

**Identify the CSP, 3PAO and Agency team members supporting this authorization effort and include those team members in the meeting invite.**

\*3PAO participation for a Kickoff meeting is encouraged if a 3PAO has been engaged to perform an assessment. 3PAO participation is required for a Combined KO/SAR Debrief.

\*\*While the Agency business owner(s) is welcome to attend, it is important to include the Agency team members that will be responsible for reviewing the authorization package and making authorization decisions

Kickoff and SAR debrief meetings are considered a best practice for successful Agency Authorizations.

This briefing guidance is used for Kickoff-only, SAR debrief-only, and for Combined Kickoff/SAR debriefs. This template should be maintained as an accumulation of all briefings.

This is not meant to be a sales meeting. CSPs should be prepared to deep dive into the system security and ensure that the appropriate CSP personnel are on hand to answer any technical questions that arise during the briefing.

## Kickoff Meeting-only (~60 minutes)

- Audience and Introductions
- Overview of the Cloud Service Offering
- Authorization Boundary
- Services without FedRAMP Authorization
- Data Flows
- Security Controls: Gaps and Customer Responsibilities

## SAR Debrief-only (~60 minutes)

- 3PAO Briefing
- CSP Briefing
- PMO Review Process
- ConMon Overview
- Tips for Success
- Work Breakdown Structure Overview

## Combined Kickoff/SAR Debrief

- **Kickoff (~30 minutes)**
  - Audience and Introductions
  - Overview of the Cloud Service Offering
  - Authorization Boundary
  - Services without FedRAMP Authorization
  - Data Flows
  - Security Controls: Gaps and Customer Responsibilities
- **SAR Debrief (~60 minutes)**
  - 3PAO Briefing
  - CSP Briefing
  - PMO Review Process
  - ConMon Overview
  - Tips for Success
  - Work Breakdown Structure Overview

## Provide the following information for the Cloud Service Offering:

- CSP Name
- Cloud Service Offering Name (as it will appear on the FedRAMP Marketplace)
- Service Offering Description
  - What are the core capabilities and functions provided by the service?
  - How does an Agency use and experience your offering?
  - Describe the federal data that will be stored / processed / transmitted by the service offering.
- FIPS 199 System Categorization - Low / Moderate / High
- Service Model - SaaS / PaaS / IaaS
- Deployment Model - Public / Community / Hybrid (**see note**)
- Cloud Stack / Leveraged Systems
  - If applicable, what underlying PaaS / IaaS are leveraged?

### Selecting the Right Deployment Model

CSPs should ensure they have identified the correct deployment model for a service offering.

- **Public** clouds include private sector and public sector tenants
- **Community** clouds are limited to tenants from a specific industry (e.g., Government-only Cloud)
- **Hybrid** clouds may include elements of private, public, and/or community deployments

To provide agencies with a clear picture of the system architecture and components that make up the authorization boundary for the cloud service offering, **the majority of the Kickoff portion is spent walking through the Authorization Boundary and Network Diagrams.** In addition, to inform the agency's understanding of how federal data and sensitive system data flows into, across, out of the cloud offering (and how that data is protected through encryption) the CSP will also walk through a series of **Data Flow Diagrams.**

When creating boundary, network and data flow diagrams, CSPs must follow the instructional text provided in the [SSP template](#), Section 8, Illustrated Architecture and Narratives.

**NOTE:** The Cloud Offering should be substantially complete with a well-defined authorization boundary at the time of the Kickoff. If the CSP is still in the early build phase with only a notional boundary, it is too soon to hold the Kickoff.



# Authorization Boundary Diagram





# Data Flow Diagram(s)



# Authorization Scope

## All Authentication Methods



If this is a Combined KO/SAR Debrief or SAR Debrief presentation, this slide will be presented in the 3PAO's portion, where the 3PAO will validate compliance or identify gaps.

For **ALL** Authentication Methods provide the following information:

### Authentication Methods

CSP Administrator:

- 1.
- 2.

Other CSP Personnel

- 1.
- 2.

Privileged Federal Customer

- 1.
- 2.

Non-Privileged Federal Customer

- 1.
- 2.

Commercial Customer

- 1.
- 2.

Others (including API's etc)

- 1.

Instructions: Include Role, authenticator, FIPS-status, Digital Identity level (1, 2, or 3). If cloud-based IDMS involved, include FedRAMP Authorization status.

# Authorization Scope

## All External Systems / Services Risk Summary



If this is a Combined KO/SAR Debrief or SAR Debrief presentation, this slide will be presented in the 3PAO's portion, where the 3PAO will communicate risks associated with the use of external services.

**External Systems:** For **ALL** external systems/services provide the following information:

System/Service Name	Description	Data Types	Data Categorization	Risk/Impact/Mitigation
<i>Provide the name of the external system/service</i>	<i>Describe the purpose of the system/service and the hosting environment (for example, corporate network, IaaS, 3rd party cloud service)</i>	<i>List the CSO data types transmitted to, stored, or processed by the system/service, including federal data and metadata (e.g., system log files, vulnerability scan data)</i>	<i>Identify the security impact level of the data (Low, Moderate, High) in accordance with FIPS 199</i>	<i>Describe potential risks introduced by the system/service and impact to the CSO or federal data if the confidentiality, integrity, or availability (CIA) of the system/service is compromised. Describe any mitigations or compensating controls in place to reduce risk.</i>

\*\* Organize and label the list of all external systems that appear in the SSP/SAR/POA&M's as follows:

### External Systems

1. Leveraged FedRAMP Authorized Systems (Federal Data involved)
2. Leveraged non-FedRAMP Systems (Federal Data involved) Provide RET and POA&M #.
3. Update Services (no Federal Data): ie OS's, AV signatures, Scanner Plug-in's
4. Development Environment (no Federal Data): ie code repo, software and container scanners
5. Reference Services (no Federal Data) ie Time, DNS etc.
6. Others (no Federal Data)::

# Authorization Scope

## Client-side and Mobile Components



If this is a Combined KO/SAR Debrief or SAR Debrief presentation, this slide will be presented in the 3PAO's portion, where the 3PAO will validate whether (or not) client-side and mobile components were included in the scope of testing.

*Provide a list of each client-side component. These are in-boundary components furnished by the CSP that operate within the Agency premises.*

### **Client-side and Mobile Components**

Indicate whether this is Browser-only

List all client-side components and mobile applications:

- Indicate whether the component is required for proper functioning of the cloud service.
- Indicate whether the component is properly documented in the SSP narratives, diagrams, control implementation statements and CIS/CRM.
- Indicate whether the component was 3PAO assessed in the SAR Pen Test Report.

During the assessment, 3PAOs are required to validate the encryption status of **all** data flows and data stores. If this is a Combined Kickoff/SAR Debrief or SAR Debrief presentation, this slide will be covered during the 3PAO's portion.

Using the authorization boundary diagram or data flow diagram(s), walk the audience through the encryption status of all data flows (internal and external) and data stores, including:

- Unencrypted
  - Describe the gaps, as well as the impacted data and sensitivity level (L/M/H), and discuss the remediation plan.
- Encrypted without FIPS validated cryptography
  - Point out where gaps exist and discuss the remediation plan
- Encrypted with FIPS validated cryptography

Confirm that the encryption status of all data flows/stores is accurately depicted on the data flow diagrams and described in the related SC control implementation statements.

**NOTE: The FIPS 140 mandate applies to NIST tested and validated cryptographic modules that use approved algorithms. \*\*TLS alone does not satisfy this requirement.**

# Contingency and Incident Response Plans Testing



During the assessment, 3PAOs validate successful performance of CP and IR Testing. If this is a Combined Kickoff/SAR Debrief or SAR Debrief presentation, this slide will be covered during the 3PAO's portion.

Contingency Plan and Incident Response Plan Testing MUST be successfully performed by the CSP and validated by the 3PAO prior to FedRAMP Authorization.

## Contingency and Incident Response Testing

1. Confirm completion of a Contingency Plan test, or provide schedule for completion
2. Confirm completion of an Incident Response test, or provide schedule for completion



Discuss the status of the authorization documentation. If this is a Combined KO/SAR Debrief, this slide will be covered in the 3PAO's portion.

Is the authorization documentation complete and ready for review? Confirm that **a thorough quality review** has been performed on the documentation to verify that the information is complete, clear, accurate and consistent.

**For example:**

- 1. Authentication Methods:** Are authentication methods completely discussed and depicted in narratives, diagrams and control statements?
- 2. External Systems:** Are all External Systems completely discussed and depicted in narratives, diagrams and control statements?
- 3. Client-Side Components:** Are all client-side and mobile components completely discussed and depicted in narratives, diagrams and control statements?
- 4. Encryption:** Is Encryption FIPS-status completely discussed and depicted in narratives, diagrams and control statements?

## Describe known security gaps

- Include remediation plan and timeline
- Discuss gaps that will/may require agency risk acceptance

## Describe Customer Responsibilities

- List controls that the Agency will be fully or partially responsible for implementing in the customer's boundary. Controls that cannot be fully inherited by the customer must be documented in the Customer Responsibility Matrix (CRM).
- If the Customer Responsibility Matrix (CRM) has been completed, walk through it during the kickoff
  - The CRM is included as a separate tab in the Control Implementation Summary (CIS) workbook

# Review Process (for Agency Authorizations)



Prior to the Kickoff, the CSP and Agency must be aligned on the on the Agency's review and authorization process, including:

- **Agency-specific requirements**
- **Key roles**
  - CSP Primary POC, Agency Primary POC, Agency AO, Agency Reviewers, Agency Liaison
- **Review approach**
  - Just-in-Time or All Deliverables at Once
  - WBS should reflect the review approach
- **Review methodology**
  - Process for performing a quality and risk review of the package. The PMO recommends following the guidance in the [FedRAMP ISSO training](#).
  - Method for capturing and tracking reviewer comments/questions
  - Communication cadence and channels (e.g., recurring weekly meetings)
- **Agency ATO decision**
  - Agency internal process for authorization recommendation and ATO issuance

Come to the Kickoff prepared to describe the agreed upon process for the Agency's review of the security package.

# CSP Training Attestation



FedRAMP requires CSPs to complete our [CSP Training](#). Please use this slide to provide a list of names of personnel who have completed the training.

**All personnel responsible for building the system, implementing security controls, and documenting the SSP are required to take the training before scheduling the Kickoff or Combined Kickoff/SAR Debrief meeting.**

The following members of the [INSERT CSP NAME] team has completed the CSP Training:

- [Insert Name]
- [Insert Name]
- [Insert Name]



# 3PAO CONTENT

**3PAOs are expected to give an independent and honest assessment of the system's overall risk posture and the CSP's overall operational maturity**

## Provide the Security Assessment schedule

- Include specific dates for controls testing, vulnerability scanning, and penetration testing
- Note any deviations from the original schedule

## Describe the Security Assessment methodology, including:

- Security controls assessment methods
  - Data gathering activities
  - Technical test methods (manual and automated tools)
  - List inherited and N/A controls that were excluded from the scope of testing
- Sampling methodology, if used

## Describe Penetration Test methodology\*, including:

- Attack vectors and key elements
  - Explain why a particular attack vector or key element was not applicable

\*As described in [FedRAMP Penetration Test Guidance](#)

3PAOs must validate the Authorization Boundary defined in the SSP to determine the scope of the assessment. Authorizing Officials need to understand services/components excluded from the assessment scope that require risk acceptance. Walk the audience through the boundary diagram and address the following questions.

- How did you validate the accuracy of the authorization boundary defined in the SSP?
- Did you identify any services/components essential to the operation, management and security of the CSO that needed to be brought into the tested boundary?
  - For example, CSP-provided components that run in the customer's environment
- Is the CSO leveraging services from an underlying FedRAMP Authorized IaaS/PaaS that are not accredited as part of the IaaS/PaaS boundary?
- Does the boundary diagram accurately reflect all external systems (including corporate networks) and external cloud services that process federal data or metadata and/or are essential to the function and operation of the CSO?
  - On the next slide, describe the risk associated with the use of external systems and cloud services that are not FedRAMP Authorized at the same impact level

# Authorization Scope

## All External Systems / Services Risk Summary



**External Systems:** For **ALL** external systems/services provide the following information:

System/Service Name	Description	Data Types	Data Categorization	Risk/Impact/Mitigation
Provide the name of the external system/service	Describe the purpose of the system/service and the hosting environment (for example, corporate network, IaaS, 3rd party cloud service)	List the CSO data types transmitted to, stored, or processed by the system/service, including federal data and metadata (e.g., system log files, vulnerability scan data)	Identify the security impact level of the data (Low, Moderate, High) in accordance with FIPS 199	Describe potential risks introduced by the system/service and impact to the CSO or federal data if the confidentiality, integrity, or availability (CIA) of the system/service is compromised. Describe any mitigations or compensating controls in place to reduce risk.

\*\* Organize and label the list of all external systems that appear in the SSP/SAR/POA&M's as follows:

### External Systems

1. Leveraged FedRAMP Authorized Systems (Federal Data involved)
2. Leveraged non-FedRAMP Systems (Federal Data involved) Provide RET and POA&M #.
3. Update Services (no Federal Data): ie OS's, AV signatures, Scanner Plug-in's
4. Development Environment (no Federal Data): ie code repo, software and container scanners
5. Reference Services (no Federal Data) ie Time, DNS etc.
6. Others (no Federal Data)::

\*\*The level of detail provided on this slide should also be captured in the RET so that Agency AOs have the information needed to make a risk acceptance decision



# Authorization Scope

## All Authentication Methods



For **ALL** Authentication Methods provide the following information:

### Authentication Methods

CSP Administrator:

- 1.
- 2.

Other CSP Personnel

- 1.
- 2.

Privileged Federal Customer

- 1.
- 2.

Non-Privileged Federal Customer

- 1.
- 2.

Commercial Customer

- 1.
- 2.

Others (including API's etc)

- 1.

Instructions: Include Role, authenticator, FIPS-status, Digital Identity level (1, 2, or 3). If cloud-based IDMS involved, include FedRAMP Authorization status.

# Authorization Scope

## Client-side and Mobile Components



*Provide a list of each client-side component. These are in-boundary components furnished by the CSP that operate within the Agency premises.*

### **Client-side and Mobile Components**

Indicate whether this is Browser-only

List all client-side components and mobile applications:

- Indicate whether the component is required for proper functioning of the cloud service.
- Indicate whether the component is properly documented in the SSP narratives, diagrams, control implementation statements and CIS/CRM.
- Indicate whether the component was 3PAO assessed in the SAR Pen Test Report.

3PAOs are required to validate the encryption status of **all** data flows and data stores

Using the authorization boundary diagram or data flow diagram(s), walk the audience through the encryption status of all data flows (internal and external) and data stores, including:

- Unencrypted
  - 3PAO to describe the gaps, as well as the impacted data and sensitivity level (L/M/H). The CSP will describe the remediation plan and mitigations in place during the POA&M portion of the SAR Debrief.
- Encrypted without FIPS validated cryptography
  - 3PAO to point out where gaps exist. The CSP will describe the remediation plan during the POA&M portion of the SAR Debrief.
- Encrypted with FIPS validated cryptography

Confirm that the encryption status of all data flows/stores is accurately depicted on the data flow diagrams and described in the related SC control implementation statements.

**NOTE: The FIPS 140 mandate applies to NIST tested and validated cryptographic modules that use approved algorithms. \*\*TLS alone does not satisfy this requirement.**

3PAOs are required to validate successful performance of CP and IR Testing

Contingency Plan and Incident Response Plan Testing MUST be successfully performed by the CSP and validated by the 3PAO prior to FedRAMP Authorization.

Contingency and Incident Response Testing

1. Indicate assessment result of Contingency Plan testing (provide RET and POA&M # if applicable).
2. Indicate assessment result of Incident Response testing (provide RET and POA&M # if applicable).

3PAOs are required to validate quality of the authorization documentation.

Discuss the quality of the authorization documentation. Is the information is complete, clear, accurate and consistent? How were gaps documented in the SAR?

**For example:**

- 1. Quality Statement:** In the assessors view, will the lack of quality result in undue time consuming remediation in the PMO Review phase prior to FedRAMP Authorization? Provide RET and POA&M #s if applicable.
- 2. Authentication Methods:** Are authentication methods completely discussed and depicted in narratives, diagrams and control statements?
- 3. External Systems:** Are all External Systems completely discussed and depicted in narratives, diagrams and control statements?
- 4. Client-Side Components:** Are all client-side and mobile components completely discussed and depicted in narratives, diagrams and control statements?
- 5. Encryption:** Is Encryption and FIPS-status completely discussed and depicted in narratives, diagrams and control statements?

# Assessment Results



If this was a Rev 4 assessment, include Table F-1. If this was a Rev 5 assessment, include Table 2-2.

# Risks with Mitigating Factors



List all risk adjustments validated during the assessment and provide the supporting rationale (mitigating factors, compensating controls).

# Operational Requirements



List all operationally required risks validated during the assessment and provide supporting rationale.



**Insert the authorization recommendation statement from Section 7 of the SAR (Rev 4) or Section 2 of the SAR (Rev 5).**

**NOTE:** If the 3PAO did not issue a favorable recommendation, the SAR Debrief will be postponed until the CSP has addressed all outstanding issues required for the 3PAO to issue a favorable authorization recommendation.



# CSP Content

**CSPs must address the content in the slides that follow to fulfill the SAR  
Debrief portion of this slide deck**

# Remediated Risks



List any risks that have been remediated since the final SAR was delivered.

POA&M ID	Risk Description	Risk Rating
<i>Include the RET Identifier in the POA&amp;M ID for traceability</i>	<i>Include the risk description from Column D of the RET.</i>	<i>List High risks first, then Moderate, then Low</i>

\*\* Add remediated risks to the Closed POA&M Items tab in the POA&M. Be sure to include a description of the actions taken to remediate the risk and reference evidence of remediation (or evidence supporting a False Positive determination).

# Risks with Mitigating Factors



List any additional Risks Adjustments that were not validated during the 3PAO assessment.

POA&M ID	Description	Initial Risk Rating	Current Risk Rating	Description of Mitigating Factors and Compensating Controls
Include the RET Identifier in the POA&M ID for traceability				

\*\* Risk Adjustments require AO approval.



List any Operational Requirements (ORs) that were not validated during the 3PAO assessment.

POA&M ID	Description	Risk Rating	Operational Requirements Rationale and Mitigating Factors/Compensating Controls
Include the RET Identifier in the POA&M ID for traceability			

\*\*An OR indicates a weakness in the system that that cannot be corrected without impacting the operation of the system.

\*\*ORs require AO approval and are still considered open risks. They must be captured on the Open POA&M Items tab and periodically reassessed by the CSP.

# False Positives



List any False Positives that were not validated during the 3PAO assessment.

POA&M ID	Description	Risk Rating	False Positive rationale and evidence
Include the RET Identifier in the POA&M ID for traceability			

\*\* False Positives require AO approval.

# Remaining Open Risks



Describe the remediation plan and timeline for High and Moderate risks that remain open. Use multiple slides, if needed.

POA&M ID	Risk Description	Risk Rating	Remediation Plan	Scheduled Completion Date
Include the RET Identifier in the POA&M ID for traceability	Include the risk description from Column D of the RET.	List High risks first, then Moderate	Describe the plan to remediate the risk.  If remediation is dependent on a downstream vendor to provide a patch/fix, describe the dependency. NOTE: High risk Vendor Dependencies must be mitigated to a Moderate level through compensating controls within 30 days.	Provide the anticipated completion date.

\*\* The AO needs to understand the current risk posture in order to make an authorization decision. Be sure the information provided is clear and concise. Do NOT simply provide a link to the POA&M.

Include the WBS to guide a discussion about the next steps to a  
FedRAMP Authorization





REMINDER:  
Upload This Deck to Your CSO's  
Secure Repository (e.g. USDA  
Connect) Once Complete

**The PMO will not accept any deliverables shared over email.**

**Please contact the PMO if you need assistance in setting up a repository on USDA Connect for your CSO. If you are a High system, please use your selected secure repository. Finally, please inform the PMO via email once your deck has been uploaded.**



# PMO review process, ConMon overview, and Tips for Success

**\*\*These slides are informational for all stakeholders and should be  
included in your presentation\*\***

- Agency sends ATO letter to CSP and [ato-letter@fedramp.gov](mailto:ato-letter@fedramp.gov)
- CSP and 3PAO upload current versions of package deliverables to secure repository
  - USDA Connect.gov (formerly OMB MAX.gov) for Low and Moderate packages
  - CSP's repository for High packages
- CSP completes and submits [FedRAMP Initial Authorization Package Checklist](#) to [info@fedramp.gov](mailto:info@fedramp.gov)
- PMO verifies that all package deliverables are uploaded
- Package is placed in PMO Review Team's queue. Packages are reviewed in the order they are received.
- The scope of the PMO's review includes:
  - A quality review to ensure the authorization package clearly and accurately represents the security and risk posture of the Cloud Service Offering
  - A risk review to identify weaknesses or deficiencies that must be addressed before the Marketplace status is changed to 'FedRAMP Authorized'

- Review team sends draft Review Report to all stakeholders (CSP, 3PAO, Agency)
  - Draft report documents findings identified during PMO's review, and any areas that require clarification
  - PMO coordinates review meeting to walk through findings and clarification requests, as well as plans for remediation by CSP/3PAO
  - Draft report is sent at least one week prior to the meeting
- CSP/3PAO address findings and resubmits package; notifies [pmo\\_review@fedramp.gov](mailto:pmo_review@fedramp.gov)
- PMO performs gap review
  - Communicates remaining gaps or recommends authorization to FedRAMP leadership
  - Once approved, Marketplace designation is changed to [FedRAMP Authorized](#)

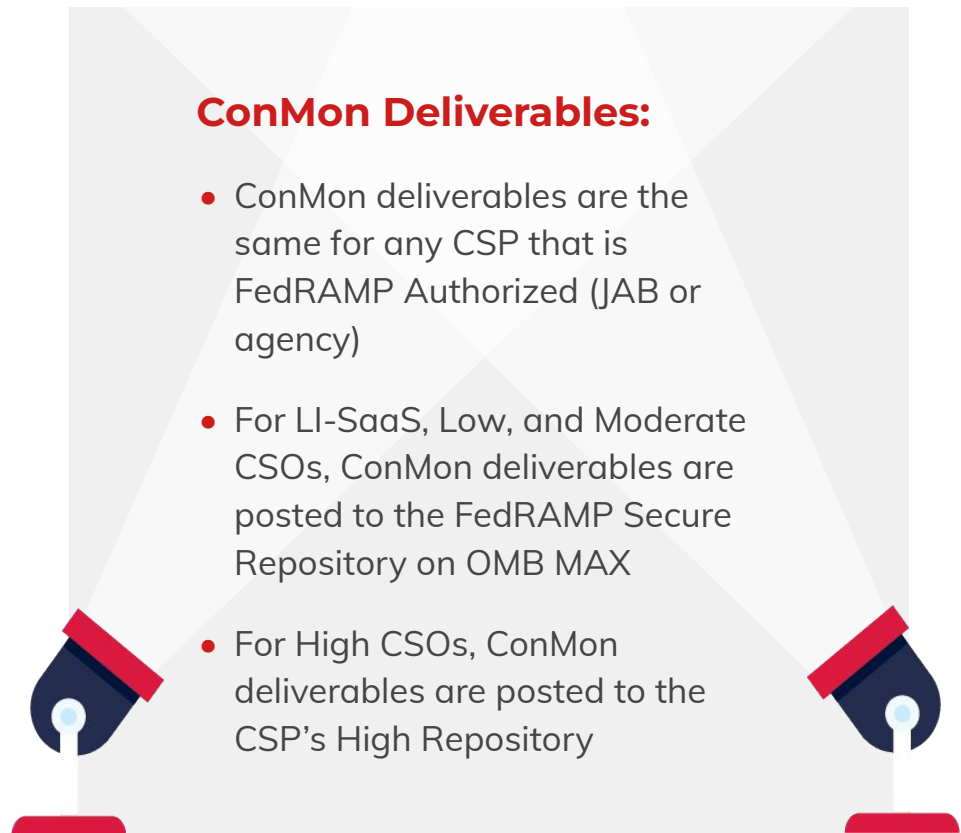
Continuous Monitoring (ConMon) ensures a cloud service offering maintains an appropriate security posture for the life of the system.

CSPs maintain and validate the security posture of their service offering through:

- Vulnerability Management
  - Monthly OS / Web / Database raw scans
  - POA&M & Updated Inventory
- Configuration Management / System Changes
- Annual Assessments
- Incident Reporting

## ConMon Deliverables:

- ConMon deliverables are the same for any CSP that is FedRAMP Authorized (JAB or agency)
- For LI-SaaS, Low, and Moderate CSOs, ConMon deliverables are posted to the FedRAMP Secure Repository on OMB MAX
- For High CSOs, ConMon deliverables are posted to the CSP's High Repository





## AGENCY RESPONSIBILITIES

- Review monthly/annual ConMon deliverables
- Approve deviation requests and significant change requests
- Ensure that the security and risk posture remains acceptable
- Raise questions or concerns with the CSP regarding any of the ConMon deliverables and security posture
- Reach out to the FedRAMP PMO at [info@fedramp.gov](mailto:info@fedramp.gov) if you are unable to obtain the information you need



## KEY FEDRAMP RESOURCES

- [ConMon 101 for Agencies](#)
- [Continuous Monitoring Strategy Guide](#)
- [Vulnerability Scanning Requirements](#)
- [POA&M Template](#)
- [POA&M Template Completion Guide](#)
- [Continuous Monitoring Monthly Executive Summary Template](#)
- [Deviation Request Form](#)
- [Continuous Monitoring Performance Management Guide](#)
- [Collaborative ConMon Quick Guide](#)

## SSP Tips for Success:

- Dedicate a strong technical writer(s) to develop the security package
- Complete [CSP training module](#): 201-B: How to Write a Control
- Make sure SSP control narratives address the actual control requirement and describe how the requirement is met
- Make sure the SSP implementation status & control origination align with the CIS/CRM
  - Be sure to use the current CIS/CRM workbook template
  - Clearly describe customer responsibilities
- Perform a final quality review of the package and correct:
  - Inconsistencies across SSP control narratives
  - Inconsistencies between the boundary diagram, data flow diagrams and SSP narrative
  - Inconsistencies between control narratives and what is validated by the 3PAO and described in the Test Case Workbook
  - Inconsistencies between the SAR and POA&M

To expedite the Agency and PMO reviews, deliver a high quality package that clearly and accurately describes the security and risk posture of the CSO.

## SAR Tips for Success (3PAO):

- Verify that all findings in the Security Test Case Procedures Workbook (“Test Case Workbook”) are documented in the SAR. All instances of controls with an assessment result of “Other than Satisfied” should be documented as an open risk in the RET, unless the finding was corrected during testing. If the finding was corrected during testing, it should be documented on the RET Risks Corrected During Testing tab.
- Be sure to clearly describe steps taken to independently evaluate and validate the control implementation. Echoing back the SSP implementation statement is not sufficient.
- Verify that the detailed breakdown of risks in Table F-1 (Rev 4) Table 2-2 (Rev 5) of the SAR is consistent with the RET.
- Use the CSP-established schema to assign a unique identifier (ID) to each RET item. In other words, the RET ID = POA&M ID.

## POA&M Tips for Success:

Review your POA&M against the [FedRAMP POA&M Template Completion Guide](#) to make sure you are documenting POA&M entries correctly. Here are some specific tips that will help prevent delays during the review process:

- For Risk Adjustments (RAs), False Positives (FPs) and Operational Risks (ORs) validated by the 3PAO during the assessment, be sure to include the deviation rationale provided by the 3PAO in Column X



## POA&M Tips for Success, cont:

- For RAs, FPs and ORs approved by the Agency, provide the deviation rationale in Column X and add a statement in the Comments column indicating Agency approval
  - Validated/approved FPs are not considered open risks and can be moved to the Closed Items tab
  - Approved ORs are still considered open risks and must be captured on the Open Items tab and periodically reassessed
- A Vendor Dependency (VD) exists when the CSP must rely on a downstream vendor to resolve a vulnerability, such as a patch for a commercial off-the-shelf (COTS) product, but the vendor has not yet made the fix available. VDs are not considered deviation requests and do not require approval. VDs are tracked as open risks and CSPs are required to check in with the vendor at least once a month to determine the status of the patch/fix. When capturing risks as VDs in the POA&M, select “Yes” in Column P (Vendor Dependency), enter the last check-in date in Column Q (Last Vendor Check-in Date), and enter the product name in Column R (Vendor Dependent Product Name).
- For all remaining open POA&Ms, be sure to complete all required fields and clearly describe the remediation plan

**3PAOs/CSPs must upload a draft Kickoff/SAR Debrief deck to the secure repository prior to the PMO scheduling a meeting.**

Learn more at [fedramp.gov](https://fedramp.gov)

Contact us at [info@fedramp.gov](mailto:info@fedramp.gov)



**@FEDRAMP**