FedRAMP

SAR Debrief Preparation Guidance

Last Update: 2/28/2022

For Agency Authorizations

GSA

info@fedramp.gov

fedramp.gov

About FedRAMP's Guidance

FedRAMP provides this guidance to inform the creation of briefing materials for a SAR debrief to an Agency customer(s)

How to Use

3PAOs and CSPs will use this guidance to create the content for a SAR debrief meeting.

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

What to Prepare

3PAOs will prepare slides that describe the security assessment plan and results.

CSPs will prepare slides that describe the remediation plan and timeline for residual risks, as well as any risk deviations that require AO approval.

3PAOs and CSPs should prepare their portions of the briefing using their own company branded template. **Be sure to cover all of the content in this guidance document.** The briefing should be appropriate for a 70-minute discussion with the FedRAMP PMO and Agency customer.

Purpose of a FedRAMP SAR Debrief

SAR Debriefs are a best practice for Agency authorization of cloud services

Successful SAR debriefs will create shared understanding of:

- Assessment scope, timeline, and methodology
- Assessment findings
- CSP plan for remediation of identified risk
- Deviation Requests requiring Agency approval
- Required actions to achieve Agency ATO

Audience

Cloud Service Provider (CSP)

- System Architect
- System Administrator
- Security Lead / SMEs
- System Owner
- Project Manager

3PAO

- Assessment Lead
- Penetration Tester

Agency

- Authorizing Official / AO Representatives
- Project Manager
- Security Representatives (ISSO, ISSM)

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

Assessment Schedule and Methodology

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

Assessment Scope
Authorization Boundary

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
External Systems / Services Risk Summary

For **each** external system/service that is **not** FedRAMP authorized at the same level as the CSO and was **not** included in the scope of testing, 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.*

**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

Encryption Status

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.

Assessment Results

Insert SAR Table F-1, Assessment Results

Risks with Mitigating Factors

Insert SAR Table 5-2, Risks with Mitigating Factors

Operational Requirements

Insert SAR Table 5-3, Risks Remaining due to Operational Requirements

CSP Content

Remediated Risks

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

POA&M ID	Risk Description	Risk Rating
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, then Low*

** 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 Agency approval.

Operational Requirements

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 Agency 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 Agency 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 Agency needs to understand the current risk posture in order to make an authorization decision. Be sure the information provided is clear and concise.

Work Breakdown Structure - Next Steps

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

PMO Content

****CSP please copy and paste this section of the deck into your presentation****

PMO Review Process

- Agency sends ATO letter to CSP and info@fedramp.gov
- CSP and 3PAO upload current versions of package deliverables to secure repository
  - OMB MAX for Low and Moderate packages
  - CSP's repository for High packages
- CSP completes and submits FedRAMP Initial Authorization Package Checklist to 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.
- Package reviews typically take 10 business days (from start of review). This assumes there are no significant quality issues.
- 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'

PMO Review Process, cont.

- 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 info@fedramp.gov
- PMO performs gap review
  - Communicates remaining gaps or recommends authorization to FedRAMP leadership
  - Once approved, Marketplace designation is changed to FedRAMP Authorized

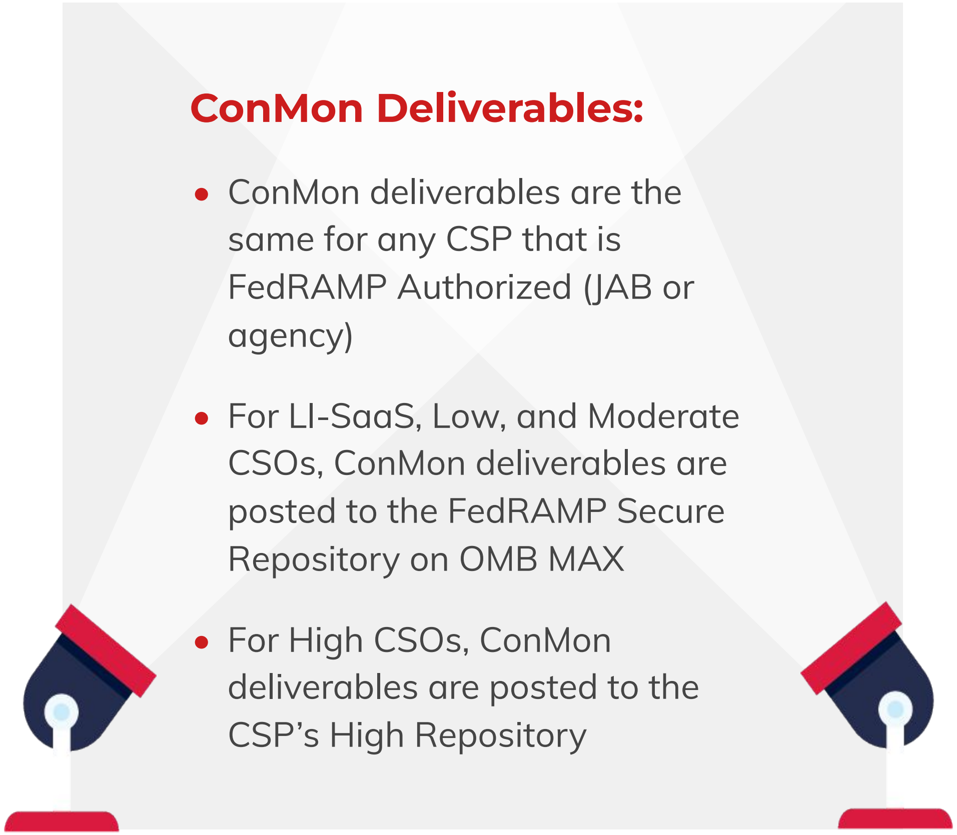
The PMO will not hold back an authorization recommendation due to minor documentation issues. However, if systemic quality issues prevent us from understanding the system boundary, data flows and control implementations, we will ask you to address the issues before recommending a FedRAMP Authorized designation

Continuous Monitoring Overview

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 ConMon Responsibilities and Resources

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 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
- Guide for Multi-Agency Continuous Monitoring

Tips for Success

SSP Tips for Success:

The Agency Review Report Template is used to guide the PMO's review. It is intended to be a starting point. If we need to dig deeper, we do. To get ahead of any issues with our review of the SSP, take the time to conduct your own "self-review" using Sections C & D of the template.

- Make sure the control implementation statements accurately describe *how* the control requirement is met, rather than simply repeating the control requirement
- Peform a quality review of the CIS/CRM to ensure consistency with the SSP
- If needed, update the boundary diagram to depict all services and components essential to the operation, management and security of the CSO. Make sure it is clear which services and components are included in the authorization boundary, and which ones are excluded.
- If needed, update the data flow diagrams to be consistent with the boundary diagram. Make sure the encryption status is accurately reflected on the data flow diagrams.

Tips for Success, cont.

**Authorizing Officials rely heavily on the boundary and data flow diagrams to understand what, exactly, they are being asked to authorize and to understand:

- the scope of the assessment;
- how federal data/metadata flows into, across, and out of the boundary;
- how that data/metadata is protected; and
- areas that will require risk acceptance.

Issues related to unclear, inaccurate, incomplete or inconsistent diagrams must be addressed prior to achieving a FedRAMP Authorized designation. Please reference the guidance and Job Aid provided during the Kickoff phase, as well as feedback provided by the 3PAO, and take the time to update the diagrams before the package is delivered to the PMO.

Tips for Success, cont.

SAP and SAR Tips for Success (3PAO):

Conduct your own "self-review" using Sections E and F of the Agency Review Report Template. In addition:

- 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 in Table 5-1 of the SAR, Risks Corrected During Testing.
- 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 Appendix F, Assessment Results, is consistent with the RET.

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 each POA&M item, be sure to include the Identifier listed in Column A of the RET for traceability. This can be done by using the RET Identifier as the POA&M Unique Identifier. Alternatively, you can add the corresponding RET Identifier to Column Z (Comments) of the POA&M.
- 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

Tips for Success, cont.

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 provide a draft SAR briefing prior to the PMO scheduling a debrief.

Learn more at **fedramp.gov**

Contact us at **info@fedramp.gov**

@FEDRAMP