FedRAMP

Agency Authorization Kickoff/SAR Debrief Guidance

For Agency Authorizations

Last updated: 7/27/2022

GSA

info@fedramp.gov

fedramp.gov

About FedRAMP's Guidance

FedRAMP provides this guidance to inform a CSP's creation of briefing materials for an Agency Authorization Kickoff/SAR Debrief

How to Use

CSPs should use this guidance to inform their development of a slide briefing for a combined Kickoff/SAR Debrief

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

What to Prepare

CSPs should prepare a slide briefing using their own company branded template that addresses the content described in this guidance. 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 followed by some time for the PMO to share our review process, tips for success, and Q&A (PMO content).

CSP Content

CSPs are expected to us the templated slides that follow to fulfill the Kickoff portion of this slide deck

Audience and Introductions

A 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, 3PAO, and FedRAMP PMO

CSP	3PAO	Agency	FedRAMP PMO
• Program Manager / Authorization Lead • Security/Compliance Lead • Technical SMEs	• 3PAO Advisor / Consultant • 3PAO Assessors and Pen Tester*	• Agency Authorization Lead • Agency Liaison • Authorizing Official • ISSO / ISSMs • Technical Reviewers • Agency Business Owner**	• Customer Success Team

Identify the CSP, 3PAO and Agency team members supporting this authorization effort. Communicate the contact information to the PMO so the right team members are invited to this meeting.

**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/SAR Debrief Agenda

Combined Kickoff/SAR debrief meetings are considered a best practice for successful Agency Authorizations

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 (~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
- Tips for Success
- Agency Review Process
- Work Breakdown Structure Overview

Overview of the Cloud Service Offering

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

Authorization Boundary, Network and Data Flow Diagrams

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/metadata 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.

- CSPs are *required* to follow the FedRAMP Diagram Guidance when creating boundary, network and data flow diagrams.
- CSPs are *encouraged* to use a diagram Job Aid, which was developed by one of our agency partners. While this is not a FedRAMP product, the agency did an excellent job of visually representing the guidance that FedRAMP provides for these diagrams. We recognize there may be aspects that do not apply to your environment, which is why this is intended to be a Job Aid versus a template.
  - The Job Aid uses generic names for system components (e.g., SIEM, Ticketing, Anti-virus), but we ask that you use the actual name of the service/product on the diagram.
  - The Job Aid provides an example of the elements that should be included on a boundary diagram. It then starts with the boundary diagram "shell" and breaks out the level of detail that is expected on network diagrams and data flow diagrams. Some CSPs, especially those with complex systems, require multiple diagrams to depict the information in an easily digestible format. Others are able to present the information using only a couple diagrams - for example, some show the network elements on the boundary diagram and some show multiple data flows in one diagram. We leave this up to your creative license as long as all of the required elements are captured in the diagrams.

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

Network Diagram

Data Flow Diagram(s)

Services without FedRAMP Authorization

Provide a summary of ALL external services that are **not** FedRAMP Authorized at the same impact level. For each service, answer the following questions:

- What data types are being transmitted to, processed or stored by the service?
- What is the sensitivity of data?
- How would your cloud service offering and / or the federal data that resides in it be impacted if the CIA of the service was compromised?
- What mitigations or compensating controls are in place to minimize risk associated with unauthorized services?
- Is the service FedRAMP Ready or FedRAMP In Process? If not, are there future plans to bring the service in boundary or migrate to a FedRAMP-authorized service?

In addition to system interconnections, APIs, external cloud services, and Corporate Shared Services, this summary should include any services provided by the underlying IaaS / PaaS, but not included in the IaaS / PaaS FedRAMP-authorized boundary.

Resources

- Sample Template: **FedRAMP Readiness Assessment Report Table 3.3 - *External Systems and Services***
- FedRAMP Authorization Boundary Guidance

Security Controls: Gaps and Customer Responsibilities

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

Resources

- For additional information regarding the CIS/CRM see this blog

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

Authorization Recommendation

Insert the authorization recommendation statement from Section 7 of the SAR.

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 are expected to us the templated slides that follow to fulfill the SAR 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
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

Agency Review Process (CSP & Agency)

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. This slide will be used as a form of attestation to confirm we can move forward with scheduling the Combined Kickoff/SAR Debrief Meeting.

All personnel responsible for building the system, implementing security controls, and documenting the SSP are required to take the training before scheduling the 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]

REMINDER:
Upload This Deck to Your CSO's Secure Repository (e.g. Max.gov) 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 OMB MAX 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 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
- PMO performs gap review
  - Communicates remaining gaps or recommends authorization to FedRAMP leadership
  - Once approved, Marketplace designation is changed to FedRAMP Authorized

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:

- Dedicate a strong technical writer(s) to develop the security package
- Complete CSP training modules:
  - 200-A: FedRAMP System Security Plan (SSP) Required Documents
  - 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):

- Complete 3PAO Series 300 training modules
- 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

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

Contact us at info@fedramp.gov

@FEDRAMP