FedRAMP

FedRAMP Agency Authorization Kickoff Briefing Guidance

For Agency Authorizations

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

How to Use

CSPs should use this guidance to inform their development of a slide briefing for a kickoff meeting

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 60 minute discussion focused on the cloud service offering (CSP content), followed by a 30 minute discussion focused on the PMO's review process, tips for success, and Q&A (PMO content).

Kickoff Agenda

Kickoff meetings are considered a best practice for successful Agency Authorizations

Kickoffs are not 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.

CSP Content (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
- Agency Review Process
- Work Breakdown Structure Overview

PMO Content (30 minutes)

- PMO Review Process
- Tips for Success

CSP CONTENT

Audience and Introductions

Kickoffs will begin with a review of the meeting's purpose and outcomes, followed by a round of introductions. Kickoffs 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 the kickoff.

*FedRAMP encourages assessor participation if a 3PAO has been engaged

**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

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 (SSP - Section 9)

Provide an easy-to-read diagram that depicts the authorization boundary for the cloud service offering. The diagram should:

- Align with the key concepts and principles described in the FedRAMP Authorization Boundary Guidance
- Include a legend
- Include a prominent RED border drawn around all system components and services included in the authorization boundary (*the authorization boundary defines the scope of 3PAO testing*)
- Depict all services and components within the boundary, including security services used to manage and operate the system (e.g., SIEM, Vulnerability Scanning, System Health Monitoring, Ticketing)
- Depict services leveraged from the underlying IaaS/PaaS and identify any services that are not accredited as part of the IaaS/PaaS FedRAMP boundary
- Depict all ingress/egress points and external entities that access the system (e.g., Agency users, CSP admins)
- Depict cloud components deployed in the customer's environment such as an endpoint application/agent
- Depict dev/test environment, alternate processing site, and location of backups
- Depict connections to external systems and services that provide functionality to the system, are used to manage and operate the system, or provide updates such as OS and antivirus updates
  - This includes system interconnections, APIs, external cloud services, and Corporate Shared Services
  - Use the legend to differentiate between external services that **are** FedRAMP-authorized and those that **are not**. Agencies need to understand and accept risk associated with external services that process / store / transmit federal data or metadata (for example: system log files, vulnerability scan data)

Every tool, service, or component that is mentioned in the SSP should appear on the boundary diagram that is provided in Section 9 of the SSP. All components provided by the CSP should be tested by the 3PAO and shown as in-boundary.

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

Data Flows (SSP - Section 10)

Provide an easy-to-read data flow diagram(s) that address all components reflected in the ABD. At a minimum, include diagrams for the following logical data flows:

- Customer User and Customer Admin Authentication, including type of Multifactor Authentication (MFA)
- CSP Administrative and Support Personnel Authentication, including type of MFA
- System Application Data Flow within the Authorization Boundary
- System Application Data Flow to/from:
  - External services, including corporate shared services
  - Interconnected systems
  - Alternate processing sites and backup storage
  - Dev/Test environment

Each DFD should depict:

- All ports and protocols for inbound and outbound traffic
- Everywhere (internal & external) federal data and metadata **at rest** and **in transit** is not protected through encryption, everywhere data is protected through encryption, and whether or not the encryption using FIPS-validated cryptographic modules. How you do this is up to you. Most CSPs use color-coding and a legend.

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

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

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.

Work Breakdown Structure

During this section CSP will present their WBS to the group to ensure all parties are aligned on timelines and milestones.

Kickoff Briefings should be provided to the PMO for review prior to scheduling a kickoff briefing.

Please work with your FedRAMP agency liaison to address questions.

Learn more at fedramp.gov

Contact us at info@fedramp.gov

@FEDRAMP

PMO Content

PMO Review Process

- Agency sends ATO letter to CSP and info@fedramp
- 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
- 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). Assumes 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

Tips for Success (1 of 3)

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.

Tips for Success (2 of 3)

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

Tips for Success (3 of 3)

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

Q&A