FEDRAMP READINESS ASSESSMENTS

A GUIDE FOR 3PAOS

Purpose

- To educate & guide 3PAOs on how to best utilize the readiness assessment report

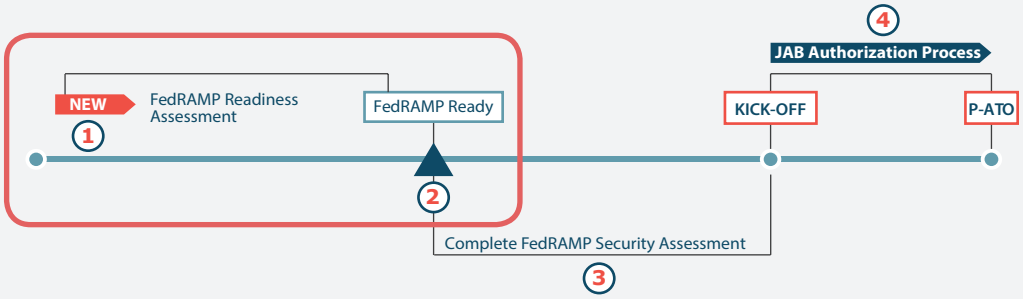
Outcomes:

- Higher likelihood of 3PAOs successfully completing the Readiness Assessment Report
- Shared understanding of RAR intent, processes, and best practices

BACKGROUND

FEDRAMP ACCELERATED

FedRAMP



CREATION

Original Draft Published on March 28th

- Coincided with FedRAMP Accelerated Launch Event

Went through Multiple Iterations Post March 28th

- Public comment period - received 100+ comments
- Additional reviews with 3PAO community
- Incorporated lessons learned from first vendors in FedRAMP Accelerated process

This is Intended to be a LIVING Document

- We expect to iterate and change this document on a regular basis
- This is a report template - relates to the overall FedRAMP documents
- We want your feedback - provide comments as you use it
- The RAR is available on FedRAMP.gov

INTENT OF READINESS ASSESSMENT

VALIDATE CAPABILITIES

Focus Should be on Capabilities

- The biggest hurdle for CSPs to obtaining a FedRAMP authorization is the full implementation of capabilities
- The RAR does NOT require massive evidence gathering by a 3PAO or 100% of documentation completed by a vendor
- 3PAOs should be focused on understanding how a CSP system works and operates, not on how that is translated to documentation

3PAOs Should Validate What's Implemented

- Technical writing is hard and many times inaccurate
- FedRAMP needs 3PAOs to validate what is actually implemented, not regurgitate what a CSP has written down
- A 3PAO should not simply validate what a CSP has documented, a 3PAO should validate in the RAR what a CSP system is and what it isn't

NOT ALL CSPS WILL PASS

Is a CSP Ready for FedRAMP?

- The intent of the RAR is for both CSPs and the Government to understand if a CSP is Ready for FedRAMP
  - CSPs should understand if they have key capabilities to obtain a FedRAMP authorization
  - The Government should be able to adequately understand if a CSP has a high likelihood of making it through a FedRAMP authorization

Not All CSPs Will Pass the RAR

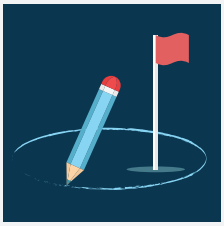
- 3PAOs should tell their CSPs that a readiness assessment is intended to determine readiness, not guarantee it
- Many times a readiness assessment will find significant gaps in CSP capabilities, resulting in the identification of work for a CSP
- 3PAOs should NOT submit a RAR to FedRAMP unless they believe a CSP has the necessary capabilities to obtain a FedRAMP authorization

FOCUS SHOULD BE ON CAP ABILITIES

TIPS AND LESSONS LEARNED

BOUNDARY

3PAOs must Validate That the Boundary is ACCURATE



- 3PAOs should validate that the boundary is accurate - identifying BOTH what is inside the boundary AND outside the boundary
- 3PAOs should also ensure that the boundary makes sense (e.g., just because a boundary is accurate doesn't mean it always provides adequate security)

3PAOs MUST do Discovery Scans and Analyze Border Devices

- 3PAOs MUST do a discovery scan as part of a Readiness Assessment
  - This is intended to provide a technical ability to ensure that things like all VLANS, subnets, undocumented hosts, etc. are discovered
- 3PAOs MUST analyze all border devices to ensure they provide appropriate segregation from any other systems
  - This includes examinations of all configurations to analyze network configurations

IN-PERSON

In-Person Discussions are Needed

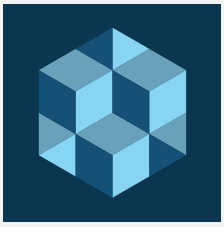
- In order to examine the organizational maturity and operations in action, a 3PAO needs to do this in person
- As detailed earlier, part of the intent of the RAR is to examine the operations of a CSP and this is not something that can be completed over video chats or over the phone

In-Person REQUIRED for all RARs

- All Readiness Assessments must include some portion of in-person interviews and observations
- Data center visits are not mandatory - but a 3PAO must be able to adequately state that data centers are not of a major concern if they are the responsibility of a CSP
  - For example, if an infrastructure provider is located in a CoLo data center provider the 3PAO has examined before or is a critical infrastructure data center, a data center visit might not be required

SEGREGATION

No Explicit Penetration Test Requirement



- It is a best practice and ultimate requirement of FedRAMP to complete a penetration test
- However, for a Readiness Assessment this is not an explicit requirement
- FedRAMP recommends that a Penetration Test be reviewed - even if completed by the CSP or another assessor

CSPs MUST be Able to Validate Adequate Segregation of Tenants and Data

- If a CSP has not had a penetration test, the 3PAO MUST be able to provide rationale for proving there is adequate segregation of tenants and data

REMEDIATION TIMES

30 Days for High, 90 for Moderate Risks

- The FedRAMP requirements for remediation of risks is incredibly clear
- CSPs have 30 days to remediate high vulnerabilities
- CSPs have 90 days to remediate moderate vulnerabilities

CSPs MUST be Able to Demonstrate the Capability to Remediate Vulnerabilities in a Timely Manner

- All Readiness Assessments must include some portion of 3PAOs should be able to see evidence that a CSP has a track record of being able to remediate vulnerabilities in a timely manner
- This doesn't mean a CSP has to be tracking in the exact format FedRAMP requires (POA&M template) BUT it does mean that a 3PAO should be able to see that a CSP has a demonstrated capability to manage risk and remediate vulnerabilities in a timely manner

DOCUMENTATION

Documentation Does Not Need to be 100% Complete

- The intent of a Readiness Capability is to determine the capabilities of a vendor, not review the documentation of a vendor
- The key focus of a 3PAO should be to review capabilities and functionality and to understand how a CSP system operates

CSPs MUST Have Documented Processes, Procedures, and Have Significant Progress Towards Completed Documentation

- In order to have organizational maturity, CSPs must have certain things documented
- If a CSP has not begun documenting an SSP - or even have a majority completed - then they would not be "ready" for a FedRAMP assessment
- Additionally, if they do not have a majority of their processes and procedures written, a CSP would not have a mature organization

DISCUSSION WITH CSP CLIENTS

LEVEL OF EFFORT

Estimated 2-4 Week Completion Time

- In the creation of this Readiness Assessment, FedRAMP worked with 3PAOs to estimate what would be sufficient to do a thorough assessment and write a quality report without making the cost too high for vendors
- The PMO estimates that a Readiness Assessment should take anywhere from 1-2 weeks to complete as well as 1-2 weeks to compile the report (for an average system)

Variability Based on Size, Complexity, Cooperation, and Preparedness of CSP

- This is not to say that all CSPs for a Readiness Assessment will take 2-4 weeks to complete
- CSPs must be prepared for the assessment (have the right staff available, be able to provide evidence, reports, etc. to the 3PAO)
- Additionally, the size and complexity of a CSP will factor heavily into the level of effort (e.g., a large IaaS provider with 15 data centers will take longer than a small SaaS solution residing within an authorized IaaS provider)

POWER OF FEDRAMP READY

CSP Knowledge of Likelihood of Success

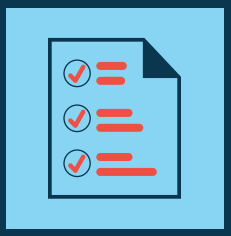
- Many CSPs begin a security authorization with the Federal Government and are unaware of the gaps within their system
- This results in unforeseen costs and time for CSPs in the authorization process
- The Readiness Assessment should benefit CSPs in helping them identify whether they have a high likelihood of success when attempting to achieve a FedRAMP authorization

Ability to Sell to Federal Agencies

- In addition to the CSP being able to ensure they have no major gaps in their system prior to beginning a FedRAMP authorization, a Readiness Assessment also provides the CSP with strong evidence of their capabilities in order to sell to Federal Agencies
- Approved RARs will be available to Federal Agencies through FedRAMP for up to one year after the delivery of a report in order to help validate a CSP's capabilities

REQUIRED FOR JAB

Required Prior to JAB Process



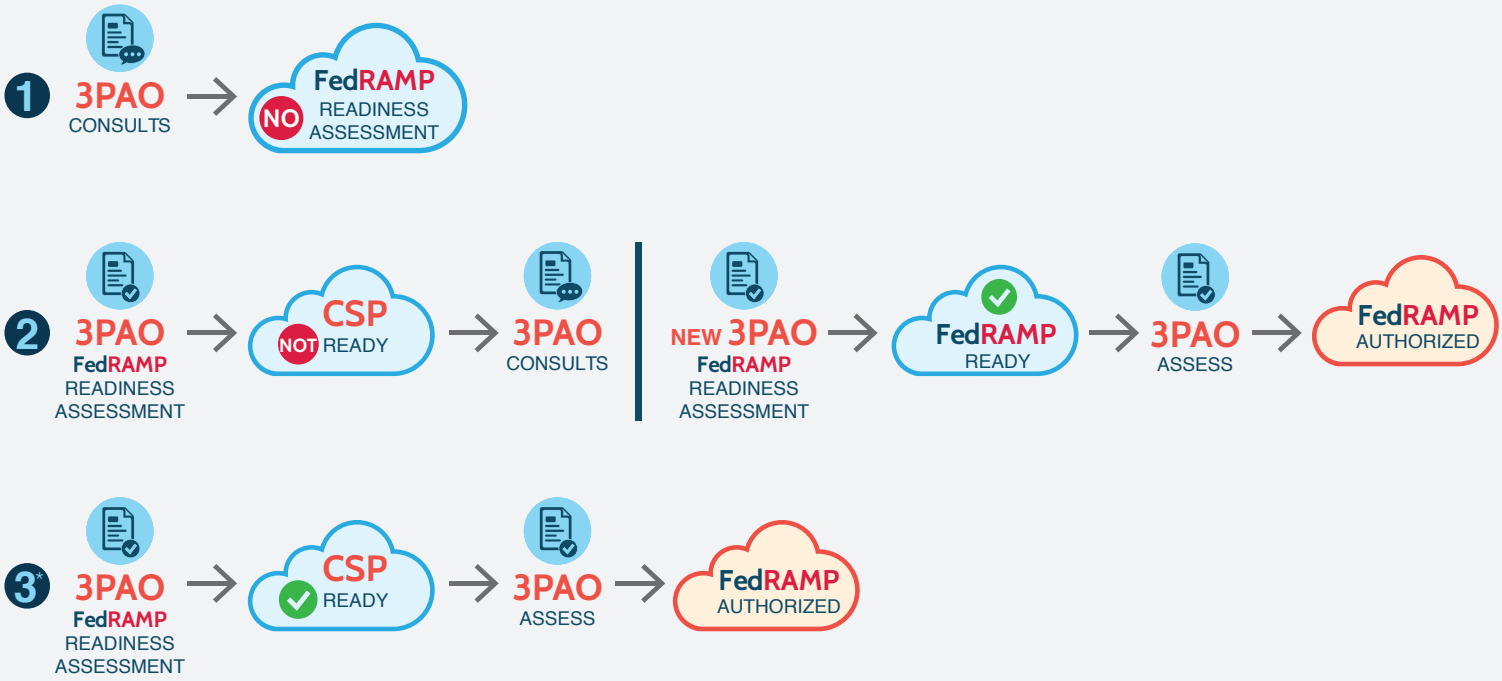
- The creation of the requirement for a Readiness Assessment is to ensure that a CSP is "ready" to begin a FedRAMP authorization by ensuring there are no major gaps in capabilities
- Before the JAB will begin the authorization process with any CSP, they must have an approved RAR by the FedRAMP PMO

Updated Prioritization Requirements Expected Within 90 Days

- The Joint Authorization Board is currently in the process of finalizing prioritization requirements
- There will likely be a short survey through FedRAMP in the next two weeks related to prioritization
- Prioritization of new vendors for the JAB will likely occur in the next 90-120 days to begin new authorizations with the JAB

SUBMISSION INSTRUCTIONS

INDEPENDENCE



* In option 3, there is the potential for iterations of the Readiness Assessment if a CSP is NOT deemed "Ready" in the first assessment. However, a 3PAO must NOT consult between Readiness Assessments as depicted in option 2 above.

3PAO MUST SUBMIT

3PAO Must Submit RARs to OMB MAX

- All 3PAOs will have a space created with the FedRAMP Secure Repository (OMB MAX) for them to upload Readiness Assessments
- 3PAOs, NOT CSPs, should upload RARs; this is to ensure chain of custody
- 3PAOs should not provide RARs without approval from a CSP
- 3PAOs must only submit RARs if they believe a CSP meets the required capabilities

Notify PMO Prior to Submission

- In order to help the PMO gauge work and potential reviews, please notify the PMO of any engagements you have with CSPs for Readiness Assessments
- Prior to uploading a completed RAR notify the FedRAMP PMO at **info@FedRAMP.gov** for submission methods

FAQs

1. DOES A RAR SUBMISSION REQUIRE A SIT-DOWN MEETING & PRESENTATION TO THE PMO?

No. However, the PMO staff will reach out to the 3PAO/CSP to require a 30 min - 1 hour briefing about the RAR within a week of delivery.

2. DO SYSTEMS HAVE TO BE FULLY OPERATIONAL TO HAVE A RAR?

Yes, systems must be fully operational. If the system is under development it is NOT ready for a Readiness Assessment Report.

3. CAN A 3PAO DO CONSULTING AND ASSESSMENTS? IF NOT, CAN YOU CITE THE POLICY THAT SAYS A 3PAO MUST BE INDEPENDENT?

A 3PAO can NOT do consulting and assessments. This is outlined by the 1720 requirements and accreditation by A2LA.

4. CAN PASSING FEDRAMP READY BE USED AS PART OF A FORMAL ASSESSMENT?

Yes, some FedRAMP Ready evidence can be used for a formal assessment. However, there are timeliness requirements around evidence that we will be clarified in the next release of the Timeliness and Quality of Testing Document.

5. ARE EVIDENCE & ARTIFACTS INCLUDED IN THE RAR AS ATTACHMENTS?

No. The RAR is intended to be quickly consumable. However, the 3PAO could use these for future assessments.