3PAO Readiness Assessment Report Guide

Version 2.0

01/04/2022

info@fedramp.gov

fedramp.gov

DOCUMENT REVISION HISTORY

Date	Version	Page(s)	Description	Author
06/07/2017	1.0	All	Original document release	FedRAMP PMO
01/04/2022	2.0	All	Updated document to align with updates to the FedRAMP Readiness Assessment Report (RAR) Templates and provide additional guidance for 3PAOs	FedRAMP PMO

TABLE OF CONTENTS

Purpose

- To educate and guide Third Party Assessment Organizations (3PAOs) and Cloud Service Providers (CSPs) on how to best utilize the FedRAMP Readiness Assessment Report (RAR) templates to obtain optimal results from the FedRAMP Program Management Office's (PMO's) RAR Review Team
- To help 3PAOs and CSPs understand the rigor that FedRAMP requires for assessments
- To increase the likelihood of 3PAOs successfully completing RARs
- To ensure shared understanding of the RAR's intent, processes, and best practices

Intent of a Readiness Assessment

The RAR is similar to a security assessment in that the FedRAMP PMO expects the 3PAO to fully develop the RAR based on 3PAO observations and 3PAO gathered evidence. While the CSP should review the RAR for accuracy, the 3PAO has ownership of the RAR and is fully responsible for its content.

The intent of the Readiness Assessment is to have a 3PAO attest to a CSP's readiness for the FedRAMP authorization process. By completing a RAR, a CSP should be able to understand if their Cloud Service Offering (CSO) has the key technical capabilities to obtain a FedRAMP authorization.

In the RAR, a 3PAO documents and validates a CSP's full implementation of the technical capabilities required to meet FedRAMP security requirements, which is the biggest hurdle for CSPs to obtain a FedRAMP authorization. The RAR does require some evidence gathering by a 3PAO, but does not require having 100% of the documentation completed by a vendor. To complete a RAR, the 3PAO should focus on:

- Confirming full implementation of the CSO's technical capabilities
- Understanding how a CSO works and operates, not on how that functionality is translated to documentation
- Validating what is actually implemented within the CSO, not copying and pasting what a CSP has written in the system documentation
- Understanding the key functionalities of the CSO and documenting the RAR in a way that is understandable to customers
- Verifying that the stated authorization boundary of the CSO and the data flows within the system are practical, secure, and logical given 3PAO expertise in cloud implementations

A Readiness Assessment is not a CSP's opportunity to determine what the FedRAMP PMO may or may not accept. If a CSO does not fully implement the Federal Mandates, the CSO will not be accepted as FedRAMP Ready. 3PAOs must ensure all comments and feedback provided by the FedRAMP PMO have been addressed before resubmitting updated RARs.

RAR Audience

Remembering the RAR audience is key. A RAR is **NOT** intended solely for FedRAMP PMO review and understanding. A 3PAO should align their RAR toward agency customers that may or may not have a strong technical background.

The intent of the report is to aid agencies in determining if they wish to invest time and funding in a particular CSO based on the level of risk the agency will inherit by using the CSO within their organization.

The report also reflects the quality and technical acumen of a 3PAO. Whereas a well-written, clear, and succinct RAR enhances the reputation of a 3PAO, a poorly written RAR may damage the 3PAO's reputation, future business potential, and could potentially impact their FedRAMP recognition.

Required Discussions with CSP Clients

Not all CSPs will pass the Readiness Assessment Review

The FedRAMP PMO does not expect CSPs to pass their Readiness Assessment each time. 3PAOs should tell their CSPs that a Readiness Assessment is intended to determine their CSO's readiness to obtain a FedRAMP authorization, not guarantee it. Many times a Readiness Assessment will find significant gaps in a CSO's capabilities, resulting in remediation 'work' for a CSP.

3PAOs should NOT submit a RAR to FedRAMP unless they validate that all the Federal Mandates mentioned in RAR Section 4.1 are met, and believe a CSO has the necessary security capabilities and functionality to obtain a FedRAMP authorization.

3PAOs Must Maintain Independence and Impartiality When Working with CSPs

Throughout the Readiness Assessment process, 3PAOs are required to remain impartial and independent when working with CSPs. This should be clearly communicated to the CSP and 3PAOs can reference R311 - Specific Requirements: Federal Risk and Authorization Management Program (FedRAMP), Section 5.2.4 F.1, to support this position. According to the R311, "If a 3PAO is part of an organization that offers consulting services to CSPs, the 3PAO is not permitted to inspect a CSP system that it has provided consulting services on within the previous two years." Section 5.2.4. F.2 further states that "if a 3PAO is part of an organization that is also a CSP, the 3PAO is not permitted to inspect the work of their organization's CSP." These guidelines are in place to ensure 3PAOs acting on behalf of FedRAMP are impartial to the best extent possible.

Although a 3PAO could serve as an assessor and then as a consultant for a CSP pursuing a FedRAMP Ready designation, a 3PAO can never serve as an assessor after serving as a consultant for a CSP. If a CSP undergoes a Readiness Assessment and they are deemed 'not ready', they may hire the same 3PAO to serve as a consultant to help with the remediation of

issues; however, after the issues are resolved, a ***different*** 3PAO must be hired to handle the next Readiness Assessment. Similarly, if a 3PAO consults with a CSP to assist with the completion of their Readiness Assessment, a new 3PAO would need to be hired to conduct the security assessment when the CSP pursues a FedRAMP authorization.

Further, a 3PAO must not assess a product in which they have a vested interest. Section 5.2.4 F.3 of the R311 indicates that "tools owned or developed by a 3PAO that provide any type of direct service or support to a CSP including, but not limited to, creating FedRAMP documentation are considered a form of consulting. Therefore, to maintain the independence of an assessment, 3PAOs are not permitted to perform assessment services for the same CSP that has directly utilized tool(s) that are owned or developed by the 3PAO for any purpose. In scenarios where a tool being used is owned or developed by a company with an affiliation to a 3PAO or its management team, employees, or subcontractors, the 3PAO must document the rationale for how it maintains its impartiality from the CSP when the CSP is using the tool owned or developed by the entity affiliated with the 3PAO and how it does not infringe upon the boundaries between providing consulting and assessing services to the CSP. This rationale must be approved by both A2LA and the FedRAMP PMO".

Being FedRAMP Ready is Required for a JAB Authorization

The creation of the requirement for a Readiness Assessment is to ensure that a CSP is 'ready' to attain a FedRAMP authorization by ensuring there are no major gaps in technical capabilities. Before the Joint Authorization Board (JAB) can begin the authorization process with any CSP, a CSP must be deemed FedRAMP Ready on the FedRAMP Marketplace. Additionally, being FedRAMP Ready is a heavily weighted prioritization criteria to work with the JAB toward a Provisional Authority to Operate (P-ATO). If a CSPs is chosen for the JAB Authorization path, they must be FedRAMP Ready within 60 days of their prioritization unless otherwise discussed with the PMO.

Benefits of Becoming FedRAMP Ready

Many CSPs that begin a security authorization with the federal government are unaware of the gaps within their system - which often results in unforeseen costs and time for CSPs and 3PAOs during the authorization process. A Readiness Assessment helps CSPs identify whether they have a high likelihood of success when attempting to achieve a FedRAMP authorization.

Additionally, agencies use the FedRAMP Marketplace to research cloud services that meet their organizational requirements. If a CSP is interested in pursuing government clients, becoming FedRAMP Ready makes available valuable information about a service offering's security for potential agency customers via the FedRAMP Marketplace.

Finally, being deemed FedRAMP Ready can help a CSP move toward being listed as FedRAMP In Process on the FedRAMP Marketplace. To achieve this designation, the CSP will need to first obtain written confirmation of an agency's intent to authorize the system, and send their confirmation information to info@fedramp.gov.

Expiration of FedRAMP Ready Designation

A CSO's FedRAMP Ready designation does expire and is only valid for one year, beginning on the date the CSO was listed as FedRAMP Ready on the FedRAMP Marketplace. CSPs may choose to pursue the FedRAMP Ready designation prior to

identifying an agency partner for an initial Agency Authorization, or prior to being prioritized to work with the JAB. While a FedRAMP Ready designation does provide Marketplace visibility as well as additional benefits, it is important for CSPs to be aware of the associated time limitation.

After the CSO's one year anniversary date, the FedRAMP Ready designation is automatically removed from the Marketplace. The FedRAMP PMO sends an anniversary date reminder to the CSP four months prior to the anniversary date to remind the CSP of their upcoming Marketplace delisting. If a CSP needs an annual extension for being listed as FedRAMP Ready on the Marketplace, the CSP must work with a 3PAO to complete a new RAR to remain FedRAMP Ready for an additional year. The updated RAR must be submitted to the FedRAMP PMO via info@fedramp.gov prior to a CSO's anniversary date. Depending on the security state of the CSO, the CSO may or may not be granted FedRMAP Ready status for another year.

Preparing a FedRAMP RAR

FedRAMP RAR templates are available for systems categorized at the High or Moderate security impact level, in accordance with the Federal Information Processing Standards (FIPS) Publication 199 security categorization. The High and Moderate baselines follow the same steps for completion with additional substeps for the High baseline report. The RAR must provide:

- An overview of the system
- A subjective summary of a CSO's overall readiness, including rationale such as notable strengths and other areas for consideration
- An assessment of a CSO's ability to meet the Federal Mandates identified in Section 4.1, the FedRAMP Requirements identified in Section 4.2, and Additional Capabilities identified in Section 4.3
- A clear description and diagram of system components and services within the authorization boundary, as well as any connections to external systems and services that are outside of the authorization boundary
- A clear data flow diagram(s) and description(s) that accounts for all federal information, data, and metadata (including all flows through the authorization boundary and to/from external systems and services, and all flows between systems within the authorization boundary)
- A 3PAO's attestation regarding the CSO's readiness to meet FedRAMP Moderate baseline requirements within one year from the date of submission

For all RAR sections, it is important to be specific, clear, and succinct. The RAR template is primarily structured in a series of questions that cover key areas of concern to gauge readiness for moving towards FedRAMP authorization. The 3PAO should directly and clearly answer RAR requirements and questions, stating what they found (observations and evidence) during their review and HOW they came about determining if a CSP adequately addresses the question area. The HOW is very important and should briefly describe the specific method of testing the 3PAO performed to draw conclusions about a CSP's CSO security state/control implementations.

The FedRAMP PMO's guidance to 3PAOs and CSPs is that when the system is submitted for the status of FedRAMP Ready, all technical security controls should be implemented and working as they should be. The FedRAMP PMO does

not expect that the System Security Plan (SSP) documentation is totally completed. However, the system authorization boundary must be clearly defined and the data flows throughout the system must be documented.

NOTE

igh RARs are analyzed with the same rigor, regardless of the CSP's intention to pursue an Agency or JAB orization, and must meet the same requirements.

Steps to Adequately Develop a RAR and the FedRAMP PMO's Evaluation Methodology

1. Validate the Authorization Boundary

Before any CSO can be assessed for readiness, the offering must have a clearly defined and maintainable authorization boundary. 3PAOs must perform full authorization boundary validation to ensure nothing is missing from the CSP-identified boundary, as well as to ensure all included items are actually present and part of the system boundary. The 3PAO must ensure the diagram:

- Includes a clearly defined, high resolution authorization boundary (with a legend) that accounts for the flow of all federal information, data, and metadata through the system. It is acceptable to provide the diagram as a separate attachment or embedded in the RAR.
- Clearly defines services as wholly within the boundary
- Depicts services leveraged from the underlying IaaS/PaaS (as applicable) and identifies any services that are not FedRAMP Authorized
    - Note: some CSPs use color-coding with a corresponding legend, and others have included a call-out box that lists all services that are not FedRAMP Authorized
- Identifies all connections to external systems and services (including corporate shared services) and identify any systems/services that are not FedRAMP Authorized
- Depicts every tool, service, or component that is mentioned in the SSP narrative and controls
    - Includes services used to manage and operate the system (e.g., SIEM, vulnerability scanning, system health monitoring, and ticketing)
    - Identifies depicted tools, services, or components as either external or internal to the boundary
- Depicts how CSP administrators and agency customers access the cloud service (i.e., authentication used to access the service). While you will cover these in detail in the data flow diagrams, FedRAMP requires this information to also be included on the boundary diagram.
- If applicable, depicts components provided by the CSP and installed on customer devices as inside the authorization boundary. These components are required to be in the boundary if they materially affect the Confidentiality, Integrity, and Availability (CIA) of the CSO (e.g., data collectors in customer data centers and mobile applications).
- Shows connections between components within the boundary and to/from external services

  - For example, connections from load balancers to the servers they support; similar flows can also be combined or noted (e.g., bastion server access to all hosts, all devices forward logs to log server, etc.)
- Depicts the dev/test environment, alternate processing site, and location of backups
  - Includes the dev/test environment within the boundary if federal data is used and/or if federal government personnel have access to the environment for any reason, including training and user acceptance testing
  - Shows update services (e.g., malware signatures and OS updates) outside the boundary

If a CSO leverages external systems or services that are not authorized at the same impact level and authorization type, 3PAOs should identify potential risks to the CSO (using the guidance and instructions in Sections 3.2 and 3.3 of the RAR templates) and then consult the FedRAMP PMO before submitting a High RAR for a FedRAMP Ready decision. Under most circumstances, FedRAMP will not consider a CSP for either a JAB or Agency High Impact FedRAMP Ready designation if the CSO leverages external systems or services that are not FedRAMP Authorized at the same impact level.

Additionally, 3PAOs must analyze all border devices to ensure they provide appropriate segregation from other systems. This includes examination of all configurations.

TIP

- 3PAOs should validate BOTH what is inside the boundary AND outside the boundary.
- 3PAOs should ensure all boundary items included are somehow represented and part of a valid system inventory.
- 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 a discovery scan as part of the RAR. The discovery scan is intended to identify operating systems running on the network then map them to IP addresses, identify open ports and services, and gather rudimentary information on targeted hosts.
- 3PAOs should be able to look at vulnerability scans, as well, since discovery scans do not probe for vulnerabilities in the system.

2. Identify All Data Flows and Stores Within and Throughout the Authorization Boundary

A 3PAO must validate the data flow diagrams (DFDs) and provide a written description of the data flows. Each DFD must also be high resolution, reflect the same components as the authorization boundary diagram (ABD), and must explicitly identify everywhere internally and externally federal data and metadata at rest and in transit is in relationship to the

system authorization boundary. Please refer to the FedRAMP Authorization Boundary Guidance document for more detail on DFD requirements.

3. Determine Leveraged FedRAMP Authorizations

If there is a FedRAMP-leveraged CSO, be sure to provide the specific details regarding this relationship in Table 3-1 Leveraged FedRAMP Authorizations. The leveraged CSO must be listed on the FedRAMP Marketplace with a status of Authorized. There is a difference between FedRAMP Ready, In Process, and Authorized. A CSO going through the RAR process is working towards a FedRAMP Ready status. A CSO that has a full assessment package submitted and has been accepted by the JAB or approved by the PMO is Authorized and can be leveraged by a CSO. A CSO listed as In Process has not been Authorized and is considered as an external, non-authorized system to the CSO going through the RAR process. Please note:

- 3PAOs must validate that all sub-services listed in Table 3-1 are included in the leveraged CSO's authorization boundary, per the CSO's service description on the FedRAMP Marketplace. Services that are not included in a FedRAMP Authorized boundary must be listed in Table 3-2 External Systems and Services.
- If the system is leveraging external services from a FedRAMP Authorized system, the interfaces to the services must be included in the boundary and must also be assessed by the 3PAO.
- The Nature of Agreement can be any type of agreement between the CSP and the CSP vendors who support products (e.g., EULA, SLA, App License Agreement, and contract).
- FedRAMP expects that all vendor products are kept current and patched.

Additionally, a 3PAO should ensure that if they are assessing a SaaS, that subscriptions to underlying services (IaaS, PaaS) are documented accurately (i.e., government community cloud versus commercial cloud or hybrid, FedRAMP Authorized versus not FedRAMP Authorized).

4. Determine External and Corporate Systems and Services

FedRAMP defines a 'connection' as any communication path used to push, pull, or exchange data and/or information, including application programming interfaces (APIs). See Section 5, below.

FedRAMP encourages the use of FedRAMP Authorized services as connections, where possible. The RAR must indicate all external services leveraged/connected to. CSPs often establish connections to external systems and services to (i) exchange data and information or (ii) augment system functionality and operational support services. This includes corporate systems and services that are not part of the authorization boundary. FedRAMP does not consider cloud systems and services as corporate systems and services. These are external services since these are not under the complete control of the corporate entity. In most cases, corporate is also 'in the cloud'.

A 3PAO must report the use of third party providers and external services/systems lacking FedRAMP authorization, at the time of RAR completion. A 3PAO completes Table 3-2 to provide a mini-analysis of the RAR external leveraged services and associated risks. A 3PAO utilizes their expertise to determine residual risk posed to the potential agency customer for using these external systems and services. The information provided in the RAR is intended to help agencies in determining suitability of using the service based on each agency's risk tolerance. Any agency considering authorization of a CSO must recognize and accept risk for use of the external services lacking FedRAMP authorization. Agencies are encouraged to engage the CSP about questions concerning the use of the external services and may involve FedRAMP PMO in such discussions, as desired.

5. Application Programming Interfaces (APIs)

3PAOs must identify all connections to external systems and services in Table 3-2. In addition, most CSOs use APIs to access data and interact with other systems' software components, operating systems, and microservices. APIs are considered connections, but put in a category unto themselves.

NOTE

Microservices are not APIs. Microservices are in their own special category. FedRAMP does not yet require that the 3PAO differentiate the specific microservices available within the system.

6. Assess and Describe the Strength of the Physical and/or Logical Separation Measures within the System

Physical and/or logical separation measures within the system must form 'defense in depth'. **Adequate separation measures provide segmentation and isolation of tenants, administration, and operations, and address user-to-system, admin-to-system, and system-to-system relationships.**

A 3PAO must base the assessment of separation measures on very strong evidence, such as the review of any existing penetration testing results, or an expert review of the products, architecture, and configurations involved. No 'explicit' penetration test is required; however, if a CSP has one, either done by themselves or a third-party, it is recommended that it be reviewed. If no penetration test is available, a 3PAO must be able to provide a rationale for being able to prove that there is adequate segregation of tenants and data.

Additionally, 3PAOs must analyze all border devices to ensure they provide appropriate segregation from other systems; this includes examination of all configurations. A 3PAO must describe the methods used to verify the strength of separation measures and segmentation and isolation of tenant data flows and stores in the RAR.

TIP

- It is a best practice and an ultimate requirement of a FedRAMP initial authorization assessment to complete a penetration test for all Moderate and High baseline systems; however, a penetration test is not an explicit requirement for a Readiness Assessment.
- If possible, FedRAMP recommends that a penetration test for the system be reviewed - even if completed by a CSP or another assessor.

7. Ensure Federal Mandates Are Met

For both Moderate and High baseline systems, there are six Federal Mandates that must be met. If the answer to any of the following questions is "No", the RAR should not be submitted:

1. Are FIPS 140-2 Validated cryptographic modules (IAW SC-13) consistently used everywhere cryptography is required? This includes all SC-8, SC-8(1), and SC-28 required encryption.
2. Does the system fully support user authentication via Agency Common Access Card (CAC) or Personal Identity Verification (PIV) credentials?
3. Is the system operating at Digital Identity Level 3?
4. Does the CSP have the ability to consistently remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days, and Low vulnerabilities within 180 days?
5. Does the CSP and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements? [https://www.archives.gov/records-mgmt/grs; PL 104-231, 5 USC 552]
6. Does the system's external DNS solution support DNS Security Extensions (DNSSEC) to provide origin authentication and integrity verification assurances? This applies to the controls SC-20, SC-21, SC-22 in the SSP.

TIP

CSPs do not have to track deficiencies in the exact format FedRAMP requires, but a 3PAO should be able to easily determine that a CSP has demonstrated the capability to manage risks and remediate vulnerabilities in an efficient and effective manner as prescribed by FedRAMP remediation timeframes: 30 days for High vulnerabilities, 90 days for Moderate vulnerabilities, and 180 days for Low vulnerabilities.

8. Ensure DNSSEC is In Place

3PAOs must verify that the external authoritative DNS server replies with valid DNSSEC responses. Also, all external domain(s) used to access a CSO must be verified as being registered with a DNSSEC signature.

For SC-21, a 3PAO must verify that all internal recursive and caching servers are properly configured to make DNSSEC requests and are within a FISMA/FedRAMP authorized boundary; the recursive or caching DNS servers must make DNSSEC requests for domains outside the boundary, and DNS calls outside the boundary must maintain DNSSEC authentication and integrity.

Authoritative Server

- The authoritative server is signed by the Top Level Domain (TLD) server, which is in turn signed by the root server.
- The entire signature chain will be checked by the recursive server; therefore, any signature that is broken breaks the whole chain.

Recursive Server

- SC-21 calls for DNSSEC to be used on recursive or caching servers.
- Trust of network connections from DNS clients and forwarding servers to the SC-21 verified server needs to also be established.
- If it is in the boundary, that is usually sufficient.
- If it crosses a boundary, then additional measures are required.

9. Verify FIPS 140-2 validated encryption within and throughout the System Boundary

For FIPS 140-2 validated encryption, FedRAMP expects that all Moderate and above federal data and metadata is encrypted for all DAR and DIT internally, externally, and traversing the service boundary. CSPs/vendors who use FIPS 140-2 validated modules have a certified security policy that states how their products must be used in a particular way. NIST's Implementation Guidance (IG) for FIPS 140-2 and the Cryptographic Module Validation Program allows implementers to assert that the implementation is sufficient. If a CSP chooses to use a FIPS 140-2 validated module in a way other than what is indicated by the security policy, it is called a derivative product and a self-attestation is required. With respect to FIPS 140 IG G.5, a user may affirm that an existing cryptographic validation does indeed apply to a derivative product as long as:

1. The software is not modified (which as noted above can be cryptographically validated).
2. The software is used on a general purpose computer (GPC) with a compatible operating system.

The specifics of this claim, as well as additional context, can be found on pages 13, 14 and 15 of the FIPS 140 Implementation Guidance.

The FedRAMP PMO and federal agencies require an assertion statement from the CSP that states the module has been implemented per the security policy of the module, and that all cryptographic functions of the product are being performed in the module.

TIP

- Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program and Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program documentation can be found on the NIST website:
  - https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-2
- NIST Special Publication (SP) 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations can be found on the NIST website:
  - https://csrc.nist.gov/News/2019/nist-publishes-sp-800-52-revision-2

10. Assess Security Capabilities Sections

3PAOs must assess several of the system's technical, management, and operational capabilities using a combination of methods, including interview, observation, demonstration, examination, and onsite visits (e.g. in-person interviews and data center visits as needed). 3PAOs may use CSP-provided diagrams, but must validate the diagrams as though the

3PAO created them. A Readiness Assessment must be done based on an accurate ABD and DFD and should not be based exclusively by reviewing a CSP's written documentation and performing interviews. Active validation of all information provided within this report is required.

TIP

- The intent of a Readiness Assessment is to examine a CSP's real-time operations.
- All Readiness Assessments must include some portion of in-person interviews and observations that are written from a 3PAO perspective. CSP personnel should not author the document.
- 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.

The RAR capabilities sections are based on:

- Identification, Authentication, and Access Control
- Audit, Alerting, Malware, and Incident Response
- Contingency Planning and Disaster Recovery
- Configuration and Risk Management
- Data Center Security
- Change Management Capabilities
- Continuous Monitoring Capabilities

3PAOs must complete all sections and address all elements of each question in the RAR templates. 3PAOs must also describe observations of any missing elements (e.g., if a CSP fails to meet all of the elements in question for each capability). If a capability is fully inherited (e.g., data center security), answer "yes" and write "fully inherited" in the column provided for the capability description.

Control references are provided with the capabilities tables. These references are provided to help a 3PAO understand the basis for each question; however, a 3PAO must not copy and paste from these security control references and must use their experience and expertise to consider all relevant FedRAMP security controls and capabilities when assessing the CSO's capabilities.

Each capability response must have three sections that describe the (i) capability, (ii) supporting evidence, and (iii) any missing elements.

NOTE

- CSPs must have documented (at least in draft) policies, processes, procedures, and evidence of significant progress towards completed documentation. If a CSP does not have a majority of their policies, processes, and procedures written, a CSP would not have a mature organization.
- These capabilities sections are not meant to be a copy and paste from a CSP's SSP. A 3PAO should provide expertise and expert analysis to determine the adequacy of the security in place.

11. Complete Executive Summary and Ensure Alignment with Entire Document

In the Executive Summary, at a minimum, 3PAOs must describe the following:

- Overall alignment with the NIST definition of cloud computing according to NIST SP 800-145, including the requirement for a CSP to have a self-service portal
- Whether the CSP is pursuing a JAB P-ATO or an Agency ATO
- Notable strengths and weaknesses
- Ability to consistently maintain a clearly defined system boundary
- Ability to accurately describe intra and inter-system user and sensitive metadata data flow
- Risks associated with interconnections used to transmit federal data/metadata or sensitive system data/metadata
- Risks associated with the use of external systems and services that are not FedRAMP Authorized
- Clearly defined customer responsibilities
- Unique or alternative implementations
- Overall maturity level relative to the system type, size, and complexity
- Overall operational maturity relative to how long the system and required security controls have been in operation

In the RAR Executive Summary, 3PAOs are required to provide the date(s) and location(s) of the Readiness Assessment, as well as a brief description of what actions the 3PAO performed to gather and validate the information provided during the Readiness Assessment, including:

- Whether interviews were conducted and descriptions of the role(s) of the individuals interviewed (names are not necessary)
- Whether testing or examination was performed, a brief statement on what testing was conducted, and what was examined

The information provided in the Executive Summary should include a one paragraph description of the system that includes all the information provided in Table 2-1 - System Information of the RAR. Therefore, it is important that these two explanations match. Additionally, marketing content is not allowed, and the FedRAMP PMO requests that marketing jargon is removed from the Executive Summary and the RAR.

The RAR Executive Summary is the CSO 'resume' for prospective agency customers. The Executive Summary must be exact, concise, and easily understood. The FedRAMP PMO recommends beginning the Executive Summary just as you would prepare a white paper, using the RAR-prescribed subsection headers that correspond with the bullets that 3PAOs are specifically asked to address in the RAR's Executive Summary. Then, carefully proceed through each bulleted item and describe HOW the 3PAO developed the noted observation. For instance, one of the bulleted items to be addressed

in the Executive Summary is “notable strengths and weaknesses”. Under this item, the PMO expects to see something akin to the following:

Example Only:

Notable Strengths and Weaknesses

<ABCCloud> has met the expectations and requirements of the FedRAMP controls. The 3PAO was provided specific and targeted evidence/artifacts by the CSP that the 3PAO has used to validate the security expectations for this system. Specifically, their strengths include, but are not limited to, the following aspects:

- *During the initial assessment in <date conducted>, it was identified that <ABCCloud> had no processes in place to remediate vulnerabilities in FedRAMP required timeframes. The 3PAO instructed the CSP that they would begin the assessment again after the processes were integrated into the CSP workflow. <ABCCloud> has since instituted a strong vulnerability remediation program, which includes a monthly POA&M for tracking all vulnerabilities, particularly those dependent on vendors.*
- *<ABCCloud> exhibits logical separation of tenants within the environment through the use of Active Directory groups, permissions, and dedicated storage locations. Further detail is provided in section 3.7 Separation Measures.*
- *<ABCCloud> has fully implemented a detailed change control process, which includes a tracking mechanism, formal approvals, security impact analysis, and pre-production testing. Additional details can be found in section 4.2.6. Configuration and Risk Management.*

<ABCCloud> does have a specific weakness, as follows:

There is encryption used throughout the system, but the 3PAO could not validate that all cryptographic modules are FIPS 140-2 validated. This CSP does use the YubiKey4 and has followed the manufacturer’s directions for best practices. The CSP provided the 3PAO with evidence that the work order is in place.

NOTE

- In order to examine the organizational maturity and system functions and operations in action, a 3PAO should do this in real time.
- Any deviations from the set guidelines should be logically explained by the 3PAO in the report. Deviations from the set guidelines are not favorable for a FedRAMP Ready designation.
- A significant requirement is that the system is ‘fully operational’. Fully operational means that the architectural components of the system are all in place and operating as required, and the technical controls are implemented. However, for a RAR, the documentation may be partially developed.

12. Complete Each Security Control Capability Statement To Include the 3PAO Test Methodology

It is imperative that a 3PAO complete each security control capability statement in each section of the RAR. Each of the sections require a 3PAO to "describe the (i) capability, (ii) supporting evidence, and any (iii) missing elements".

In one of the specific capability areas relating to Identification and Authentication (I&A), called "Identification Authentication and Access Control", the question is as follows: *Does the system require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2(1), IA-2(3) (and IA-2(11) for a High Readiness Assessment)]*

An acceptable RAR Response might be something like:

Capability: *Access to the [ABC Cloud] requires use of <NAME of> MFA for all administrator accounts and functions. Access to the [ABC Cloud] is achieved via a VPN connection to the bastion host using <some authentication>. For the VPN connection to be granted a connection, a [technology used] token is used for authentication. Once a VPN connection is established, the administrator must SSH to the bastion. The administrator authenticates using a unique SSH private key stored on their corporate laptop. An additional token is required for SSH authentication. This [technology used] token is required for both the VPN and SSH connections and each challenge is unique for the separate connections.*

3PAO Test Methodology: *The 3PAO observed an administrator establish a VPN connection from their laptop to the [ABCCloud] network. Once the VPN connection was authorized using [MFA Technology], the administrator established an SSH session with the bastion host in the [ABCCloud] hosted in [IaaS] environment. The SSH session was authenticated using the employee's unique SSH private key located on the administrator's laptop (Moderate system). The 3PAO observed an administrator attempt to create a new user by reuse of an existing identifier.* The interface rejected the attempt and issued an error stating that the identifier was already in use.

Missing Elements: None.

NOTE

- Each security capability statement in the RAR requires that the 3PAO describe the capability as stated in the corresponding question, any supporting evidence identified to strengthen the compliance, and any missing elements, as required.
- The capability is NOT a copy and paste from the System Security Plan (SSP). A 3PAO must address the question and then indicate how they interviewed, examined, and or observed the capability in place.
- A 3PAO should only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Submission Instructions

All 3PAOs have a space created in the FedRAMP Secure Repository (MAX) for them to upload completed RARs. A 3PAO should confer with their CSP concerning the results of their Readiness Assessment before posting the RAR, but only 3PAOs, NOT CSPs, should upload RARs to MAX in order to maintain a chain of custody. Most importantly, **3PAOs should submit the RAR only if the 3PAO has fully validated:**

1. **The CSO authorization boundary and data flow diagrams**
2. **That the CSP has implemented all Federal Mandates**
3. **That there are no major technical gaps between the CSP's implemented technical controls and FedRAMP requirements**

In order to help the FedRAMP PMO gauge work and potential reviews, please notify the FedRAMP PMO via info@fedramp.gov of any engagements you have with CSPs for Readiness Assessments at least two weeks prior to submission (i.e., 10 business days).

When the FedRAMP PMO receives the submission, it is put in a review queue. If the queue is extensive, the FedRAMP PMO will send the CSP and 3PAO an email to set expectations regarding approximate review timeframes (e.g., 2 weeks, 4 weeks, etc.). This timeframe is based on the estimated time it will take the FedRAMP PMO to begin the review of the RAR, and does not reflect the time it will take the PMO to complete the review.

FAQs

To begin the approval process, is the vendor supposed to email FedRAMP with their intentions of submitting a Readiness Assessment Report (RAR)?

In order to ensure that all stakeholders are on the 'right path', FedRAMP suggests that CSPs email info@fedramp.gov regarding their intention to submit a RAR. The reason for this is to ensure that the CSP, the 3PAO, and the FedRAMP PMO are aligned as to the Readiness Assessment requirements. Many times the CSP does not understand the rigor applied to a Readiness Assessment and questions the 3PAO actions. By setting expectations in the beginning, the Readiness Assessment will proceed more smoothly. Readiness Assessments performed by a FedRAMP recognized 3PAO usually take 4 - 6 weeks on a Moderate system, plus another 2 weeks (minimum) to write the report. A High baseline system requires more rigor since the FedRAMP PMO must inspect the RAR with JAB requirements in mind. When a 3PAO determines that the vendor is FedRAMP Ready and is getting ready to send the report to FedRAMP for consideration, the 3PAO should notify FedRAMP (via info@fedramp.gov) about 2 weeks prior to upload.

Does a FedRAMP CSO environment need to be in production prior to beginning the FedRAMP ready assessment?

While the expectation for FedRAMP Ready is that the environment is fully operational and ready to undergo an initial FedRAMP assessment, it does not need to have active customers in the environment. A 3PAO will perform an assessment of the operational environment and recommend in the RAR whether the system meets FedRAMP requirements. The RAR templates are on FedRAMP.gov, under Resources > Documents and Templates. Referring to one of the RAR templates will give the CSP an idea of the assessment criteria and rigor. Additionally, a RAR submission does not guarantee a FedRAMP Ready designation, nor does it guarantee a FedRAMP authorization. During the RAR review and approval process, the FedRAMP PMO may require the CSP to perform additional actions to demonstrate readiness, which would require validation by the 3PAO. Concurrently, the FedRAMP PMO may require updates to provide clarity. 3PAOs conducting Readiness Assessments should advise CSPs that additional changes may be required after the RAR is submitted to the FedRAMP PMO for review and approval.

Is it true that once a SAR is done, a RAR cannot be done?

A RAR can be done after a SAR is completed for a CSO. CSOs are constantly changing and the dynamic nature indeed benefits from a Readiness Assessment. Additionally, for systems that are in the program vying for moving from a Moderate to a High baseline system, for instance, completing a RAR is recommended. This gives the CSP a reference for the rigor of a High baseline assessment.

Do FedRAMP RARs that have been authorized as Ready expire? Would the CSP need to complete their full ATO within a specific timeframe?

Yes, a RAR expires after one year. If the one year timeframe is soon coming to an end, a CSP is required to have a 3PAO complete another Readiness Assessment review and submit the report to the FedRAMP PMO just as they did in the beginning of the process. This allows a CSP to remain on the FedRAMP Marketplace as FedRAMP Ready as long as the system is still ready. Many times, the FedRAMP PMO sees systems that have languished over the one year period and have not been doing continuous monitoring. These systems no longer apply the rigor required for FedRAMP readiness and ultimately fail the assessment..

Is the process for submitting a High RAR any different than a Moderate RAR?

Yes, the process for submitting a High RAR has a few extra steps than when a 3PAO submits a Moderate RAR. First, the 3PAO must inform the FedRAMP PMO of the High RAR submission at least two weeks prior to the submission date via info@fedramp.gov. At this time, the 3PAO will work with their POC from info@fedramp.gov for specific submission instructions. These instructions are basic for maintaining the RAR's confidentiality and integrity. When submitting a High RAR to the FedRAMP secure repository, the 3PAO must encrypt the RAR before uploading. The PDF and WORD versions of the documentation should be enabled to open via a secure password. Instructions are given to the 3PAO through the email thread with info@fedramp.gov.