FedRAMP New Cloud Service Offering (CSO) or Feature Onboarding Request Template



<CSP Name or Logo>

<Cloud Service Offering Name>

< Service/Feature Name>

Version 2.0

<Date>

As Prepared by <3PAO>

**Company Sensitive and Proprietary**

**For Authorized Use Only**



Template Revision History

| **Date** | **Version** | **Page(s)** | **Description** | **Author** |
| --- | --- | --- | --- | --- |
| 9/15/2016 | 0.4 | All | FedRAMP-New-Service Onboarding-Request-DRAFT V0.4\_09152016.docx sent to JAB TRs for comments | FedRAMP PMO |
| 10/24/2016 | 0.5 | All | Added DoD, DHS, and GSA comments | FedRAMP PMO |
| 11/8/2016 | 1.0 | All | Incorporated all DoD, DHS, and GSA comments from 11/3/2016 concurrences reached via teleconference | FedRAMP PMO |
| 3/9/2017 | 2.0 | All | PMO Quality Review | FedRAMP PMO |
| 6/6/2017 | 2.0 | Cover | Updated logo | FedRAMP PMO |

# Third Party Assessment Organization (3PAO) Attestation

An Accredited 3PAO must attest that they have performed the Cloud Service Offering service or feature assessment and that the Cloud Service Offering feature or service is FedRAMP compliant and can be onboarded to the Cloud Service Provider’s system. For the new feature or service to be onboarded securely, the 3PAO is using its expert judgment to subjectively evaluate the overall compliance of the new service or feature with the FedRAMP requirements and attest to its readiness for inclusion into the existing system P-ATO boundary and factor this evaluation into its attestation.

|  |
| --- |
| [3PAO name] attests that the [CSP name system and Cloud Service Offering feature or service name] meets the FedRAMP requirements as described in this FedRAMP New Cloud Service Offering / Feature Onboarding Request. [3PAO name] recommends the FedRAMP JAB grant [CSP system name] [new Cloud Service Offering feature to be onboarded] “New Cloud Service Offering Onboarding” approval.  This FedRAMP New Cloud Service Offering / Feature Onboarding Request was created in alignment with the FedRAMP requirements and guidance. This request is based on [3PAO name]’s evaluation of [CSP name and system name] and the [new Cloud Service Offering feature to be onboarded] which includes observations, evidence reviews, personnel interviews, and demonstrated capabilities of security implementations.  This attestation is based on [3PAO name]’s 3PAO Accreditation by the American Association of Laboratory Accreditation (A2LA) and FedRAMP, experience and knowledge of the FedRAMP requirements, and knowledge of industry cybersecurity best practices. Further, [3PAO name] attests this report is an independent validation and verification that the [new Cloud Service Offering feature] is compliant with FedRAMP requirements and cybersecurity best practices.  Lead Assessor’s Signature: X\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  <Lead Assessor’s Name>  <3PAO Name> |

# Executive Summary

In the space below, 3PAO must provide a one-paragraph description of the new service as it relates to the system. The description should contain all the information provided in Table 3-1, System Information.

The, 3PAO must also provide up to four paragraphs summarizing the data and information flows for the service based on the 3PAO’s cybersecurity expertise and knowledge of FedRAMP, including notable strengths and other areas for consideration when considering onboarding the new service. Diagrams can be included to explain concepts but, must also be accompanied by the explanatory text.

The 3PAOs should consider how the addition of the Cloud Service Offering service or feature affects the system to which it is being added/adopted, FedRAMP requirements, and if security controls artifacts are affected by the addition as reflected in the existing System Security Plan, system architecture and network diagrams, security controls implementation details, changes to processes and procedures, and inventory. The 3PAO should ensure the security impact analysis looks at the new service as if it were in the original system definition and what would have changed if it existed at that time. The following situations are “show-stoppers” for onboarding new Cloud Service Offerings via this process. If the new Cloud Service Offering feature introduces one or more of the following situations, the new feature is considered a significant change and must be added to the system via the FedRAMP Significant Change process or during the next annual assessment. If onboarding the feature or service severely impacts the security posture of the system, the CSP should not consider adding this via the new Cloud Service Offering /Feature Onboarding process.

If the new Cloud Service Offering feature or service:

* Replaces an existing Cloud Service Offering feature or service previously assessed as included in the original system assessment, or if the new feature or service is a Significant Change, the new feature or service should be added to the system via the FedRAMP Significant Change process or during the next annual assessment.
* Is an outsourced feature or service not belonging to the Cloud Service provider and belongs to a different Cloud Service Provider, this new feature or service is a Significant Change and must be added to the system via the FedRAMP Significant Change process or during the next annual assessment.
* Changes the categorization of the existing Cloud Service Offering from, i.e., Infrastructure as a Service to Platform as a Service or to Software as a Service, this is a Significant Change and must be added to the system via the FedRAMP Significant Change process or during the next annual assessment.
* Introduces vulnerabilities that affect the current security posture of the system as it exists in Continuous Monitoring, this is a Significant Change and must be added to the system via the FedRAMP Significant Change process or during the next annual assessment.
* Affects the existing security controls implementation details of any of the security controls as these are captured in the System Security Plan, this is a Significant Change and must be added to the system via the FedRAMP Significant Change process or during the next annual assessment.
* Adds a unique or alternative implementation of any of the security controls as these are captured in the System Security Plan, this is a Significant Change and must be added to the system via the FedRAMP Significant Change process or during the next annual assessment.

The 3PAO should consider the following for dialogue, when evaluating the overall readiness of a Cloud Service Offering feature or service to be onboarded:

* Overall alignment of the new feature or service with the FedRAMP and National Institute of Science and Technology (NIST) definition of cloud computing, according to NIST SP 800-145
* Whether the feature or service remediates and/or introduces mitigations to current vulnerabilities
* Observed strengths and weaknesses of the service or feature implementation
* Clearly defined CSP and customer responsibilities related to the new service/feature within the system to which it is being added
* Overall maturity level relative to the system type, size, and complexity and how that relates to the new service onboarding.

|  |
| --- |
| **IMPORTANT:** For this new Cloud Service Offering Onboarding effort, it is imperative that the new feature or service to be onboarded lies within the <Cloud Service Offering Name> authorization boundary. Inaccuracies regarding the new feature or service onboarding within the New Cloud Service Offering Onboarding Feature Request may give authorizing officials and FedRAMP grounds for disallowing any further services onboarding, removing a vendor from FedRAMP, and disciplinary actions initiated against the 3PAO as per the guidelines set by FedRAMP. |

Document Revision History

| **Date** | **Page(s)** | **Description** | **Author** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Third Party Assessment Organization (3PAO) Attestation ii](#_Toc466293916)

[Executive Summary iii](#_Toc466293917)

[1. Introduction 1](#_Toc466293918)

[1.1. Purpose 1](#_Toc466293919)

[1.2. Outcomes 1](#_Toc466293920)

[1.3. FedRAMP Approach and Use of this Request Document 2](#_Toc466293921)

[2. General Guidance and Instructions 4](#_Toc466293922)

[2.1. Embedded Document Guidance 4](#_Toc466293923)

[2.2. Additional Instructions to 3PAOs 4](#_Toc466293924)

[3. CSP System Information 6](#_Toc466293925)

[3.1. Identify Relationship to Existing FedRAMP P-ATO 6](#_Toc466293926)

[3.2. Authorization Boundary, Network, and Data Flow Diagrams 6](#_Toc466293927)

[3.3. Service or Feature Interconnections 7](#_Toc466293928)

[4. FedRAMP Capabilities 8](#_Toc466293929)

[4.1. FedRAMP CIS Workbook 8](#_Toc466293930)

[4.1.1. Change Management Maturity 8](#_Toc466293931)

[4.1.1. Vendor Dependencies and Teaming Agreements 9](#_Toc466293932)

[4.1.2. Continuous Monitoring (ConMon) Capabilities 10](#_Toc466293933)

List of Tables

[Table 3-1. System and Service Information 6](#_Toc466293904)

[Table 3-2. Parent Relationship to Other CSP 6](#_Toc466293905)

[Table 3-3. System Interconnections 7](#_Toc466293906)

[Table 3-4. Connections with Other Services 7](#_Toc466293907)

[Table 4-1. Change Management 9](#_Toc466293908)

[Table 4-2. Vendor Dependencies and Teaming Agreements 9](#_Toc466293909)

[Table 4-3. Vendor Dependency Details 9](#_Toc466293910)

[Table 4-4. Teaming Agreements Details 10](#_Toc466293911)

[Table 4-5. Continuous Monitoring Capabilities 10](#_Toc466293912)

# Introduction

## Purpose

This request and its underlying assessment are intended to enable FedRAMP to reach an approval decision for onboarding a new service or feature to a Cloud Service Provider’s (CSP) offering based on the operational security posture of the service selected for onboarding, the maturity of the organizational processes, and security capabilities of the system inheriting the new service. If the CSP is onboarding new features and services, it is implied that the CSP is already offering these features and services and has adequate data available upon which security posture and risk exposure can be evaluated.

**IMPORTANT:** It is imperative that the new service or feature to be onboarded lies within the <System Name> authorization boundary. Inaccuracies regarding the new service within the New Service Onboarding Request may give authorizing officials and FedRAMP grounds for disallowing any further services onboarding and/or removing a vendor from FedRAMP.

FedRAMP grants approval when the information in this report indicates that the CSP is likely to achieve a Joint Authorization Board (JAB) approval to add the new service to the system.

## Outcomes

If the new service or feature introduces one or more of the following situations, the new feature is considered a significant change and must be added to the system via the FedRAMP Significant Change process or during the next annual assessment. If onboarding the feature or service severely impacts the security posture of the system, the CSP should not consider adding the new service or feature via the new Cloud Service Offering Feature Onboarding process.

If the new Cloud Service Offering feature or service:

* Replaces an existing Cloud Service Offering feature or service previously assessed as included in the original system assessment, the new feature or service is a Significant Change. This new feature or service should be added to the system via the FedRAMP Significant Change process or during the next annual assessment.
* Is an outsourced feature or service not belonging to the Cloud Service Provider and belongs to a different Cloud Service Provider, this new feature or service is a Significant Change and must be added to the system via the FedRAMP Significant Change process or during the next annual assessment.
* Changes the categorization of the existing Cloud Service Offering from, i.e., Infrastructure as a Service to Platform as a Service or to Software as a Service, this is a Significant Change and must be added to the system via the FedRAMP Significant Change process or during the next annual assessment.
* Introduces vulnerabilities that affect the current security posture of the system as it exists in Continuous Monitoring, this is a Significant Change and must be added to the system via the FedRAMP Significant Change process or during the next annual assessment.
* Affects the existing security controls implementation details of any of the security controls as these are captured in the System Security Plan, this is a Significant Change and must be added to the system via the FedRAMP Significant Change process or during the next annual assessment.
* Adds a unique or alternative implementation of any of the security controls as these are captured in the System Security Plan, this is a Significant Change and must be added to the system via the FedRAMP Significant Change process or during the next annual assessment.

A 3PAO should only submit this request to FedRAMP if it determines the new service or feature onboarding to the CSP system is likely to achieve JAB approval. Submission of this request by the 3PAO does not guarantee JAB approval.

## FedRAMP Approach and Use of this Request Document

FedRAMP considers any new service to be a significant change because the new service changes the definition of the CSP offering as defined in the original Provisional ATO and as reflected in the System Security Plan (SSP). As such, it is required that FedRAMP grants approval for these types of services before they are implemented in the operational CSP offering. These changes, as listed in Section 1.2, are considered significant changes and must be addressed through the FedRAMP significant change process.

This Cloud Service Offering Onboarding Request can be used, if the new service or feature to be onboarded:

* Does not replace an existing service/feature that was previously assessed as included in the original system assessment
* Is not an outsourced service not belonging to the Cloud Service Provider and belongs to a different Cloud Service Provider
* Does not change the categorization of the Cloud Service Offering
* Does not introduce vulnerabilities that affect the current security posture of the system as it exists in Continuous Monitoring
* Does not affect the existing security controls implementation details of any of the security controls as these are captured in the System Security Plan
* Does not add a unique or alternative implementation of any of the security controls as these are captured in the System Security Plan

This document should not be submitted by the 3PAO with the 3PAO attestation if the information concerning the new service/feature negatively affects any of the above mentioned circumstances.

This document identifies clear and objective security impacts related to the addition of the new service or feature. It describes the objective capabilities and requirements where possible, while also allowing for the presentation of more subjective information. The clear and objective requirements enable the 3PAO to identify whether a service or feature to be onboarded aligns with the FedRAMP requirements as these exist within the CSP’s authorized boundary. The combination of objective requirements and subjective information enables FedRAMP to render an evaluation of the overall risk of the new service or feature within the existing Cloud Service Offering and how this new service or feature to be onboarded aligns with the FedRAMP security objectives and the CSP’s existing security capabilities.

# General Guidance and Instructions

## Embedded Document Guidance

This document contains embedded guidance to instruct the 3PAO on the completion of each section. This guidance ensures FedRAMP receives all the information necessary to render a new service or feature onboarding decision.

The guidance text is in grey and should be removed after the report is fully developed, but before it is submitted to FedRAMP.

## Additional Instructions to 3PAOs

*The 3PAO must adhere to the following instructions when preparing the new service or feature onboarding request:*

1. *The new service or feature onboarding request must provide:*
   1. *An overview of the service or feature and the evaluated and analyzed Continuous Monitoring (ConMon) performance by the 3PAO in order to determine CSP process maturity*
   2. *A description of how the new service or feature interacts with the other CSP CSO capabilities, security measures, and services*
   3. *A subjective summary of the new service or feature’s compliance with FedRAMP requirements and the CSP’s readiness to support a full assessment based on those requirements. The subjective summary must include rationale such as notable strengths/ weaknesses and security weaknesses mitigated with the inclusion of the service or feature*
   4. *A summary of the updates to Section 9 of the CSP SSP and system inventory that is captured in the next monthly Continuous Monitoring*
   5. *An updated CIS workbook and Security Requirements Traceability Matrix (SRTM) clearly identifying which controls are inherited/leveraged by the new service or feature from the parent service offering and the control implementation status for all controls specific to the new service being onboarded.*
   6. *The 3PAO Attestation to the contents of the new service or feature onboarding request based upon FedRAMP guidance within this Onboarding document, and to the completion of independent verification and validation of the evidence and artifacts aggregated, to demonstrate FedRAMP compliance. The 3PAO is attesting they have completed all these steps and that the CSP’s assertions have been verified/validated as being true.*
      1. *Provide a 3PAO attestation letter assuring that the new service onboarding request is complete and the new service onboarding request meets all FedRAMP requirements.*
      2. *Provide any supporting artifact evidence regarding the suitability and security posture of the service to be onboarded.*
      3. *Provide the artifacts to demonstrate the compliance for service specific controls.*
2. *FedRAMP will not consider a new service for onboarding unless this document and the updated CIS/SRTM are completely filled out. Please note, meeting these requirements does not guarantee approval.*
3. *The 3PAO must assess the service or feature’s technical, management, and operational capabilities using a combination of methods, including interview, observation, demonstration, inspection, including onsite visits (e.g., in-person interviews and data center visits as needed to verify the contents of the request). The 3PAO may use CSP-provided diagrams, but must validate all evidence materials’ accuracy. The 3PAO must* ***not*** *conduct this new service onboarding request process exclusively by reviewing a CSP’s written documentation and performing interviews. Active validation, as defined by NIST SP 800-53A, of all information provided within this report is required[[1]](#footnote-2).*
4. *The 3PAO is expected to assess applicable FedRAMP security controls for the new service before preparing their recommendation/attestation.*
5. *The 3PAO must ensure and attest to the requirements in this onboarding document have been met.*
6. *Once the JAB has reviewed the new service or offering request, a JAB representative will notify the CSP of the approval. The timeframe for JAB review and approval is approximately 10 business days.*

# CSP System Information

Table 3-1. System and Service Information

|  |
| --- |
| CSP Name:  System Name:  Service Model: (IaaS, PaaS, SaaS) Choose an item.  FIPS PUB 199 System Security Level: (Low, Moderate or High) Choose an item.  Deployment Model: Choose an item.Is the service a Public Cloud, Government-Only Cloud, Federal Government-Only Cloud, or DOD Cloud?  System Functionality: Briefly describe the CSO as currently approved in order to put the new service(s) into context.  New Service or Feature name  This section addresses the functionality and the impact of new service or feature on existing customers or to other CSPs leveraging this CSP's capabilities. Since the new service or feature only leverages existing security controls, the new service or feature will not have a functional impact on a leveraging CSP unless the leveraging CSP wants to adopt the new service or feature.  Please note: It may be desirable for CSP and/or 3PAO to articulate how the subject functionality supplements the system to which it is being onboarded as new services, not as major changes. Recommend considering clarifying "affects" in the "New Service Functionality" subsection to also include an explanation and an attestation of the claim that the added functionality ought to be considered as a "new service". |

## Identify Relationship to Existing FedRAMP P-ATO

If the parent system to which this service is being onboarded leverages another CSP’s environment or is inheriting security capabilities, please provide the relevant details below.

Table 3-2. Parent Relationship to Other CSP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **Yes** | **No** | **N/A** | **If Yes, please describe.** |
| Is this system leveraging an underlying provider? |  |  |  | (If “yes”, identify the underlying CSP. If “no”, the following questions in this table are “N/A”) |
| If “yes”, does the leveraged system have a JAB P-ATO? |  |  |  |  |
| If the leveraged system does not have a JAB P-ATO, does it have an Agency ATO? |  |  |  | (Identify any Agency ATOs and indicate which are FedRAMP Agency ATOs) |

## Authorization Boundary, Network, and Data Flow Diagrams

The 3PAO must perform full new service assessment and validation, as defined in Sections 1.2, 1.3, and 2.2 of this document for the New Service or feature; must ensure nothing is missing from the new service or feature description and potential threat/attack vectors, and ensure all included items for the new service or feature are actually present and are part of the system inventory. Once the new service or feature is onboarded, the list of service assets provided in the artifacts package can be reconciled against the next month’s Continuous Monitoring submission. To achieve this, the 3PAO must perform the same types and scopes of activities as if the new service or feature were included in the original FedRAMP assessment, including, but not limited to, examination of artifacts, testing of security controls as they relate to the new services, discovery scans and in person interviews and physical inspections, where appropriate.

Insert 3PAO-validated updated network and dataflow diagram(s) of the system reflecting the new service or feature to be onboarded. The 3PAO must ensure each network diagram:

* includes a clearly defined system authorization boundary;
* clearly defines where the new service resides within the boundary;
* depicts the location of all major components (software/virtual components) of the new service or feature within the boundary;
* identifies all interconnected internal and external services inside the boundary;
* depicts all major hardware, software/virtual components (or groups of) for the new service within the boundary; and
* is validated against the system/service inventory.

*The 3PAO must ensure each dataflow diagram is updated to include the new service or feature as it relates to:*

* Identifying where Federal data is to be processed, stored, or transmitted through the new service or feature;
* Identifying how data comes into and out of the new service; and
* Identifying how all ports, protocols, and services of all inbound and outbound traffic for the service or feature are represented and managed. Please note, if the new service or feature uses different ports, protocols, and/or services than are identified within the front matter of the existing SSP, the new feature or service is considered a Significant Change and must proceed through the FedRAMP Significant Change process.

## Service or Feature Interconnections

The 3PAO must complete the table below. If the answer to any question is “yes”, please briefly describe the connection. Also, if the answer to the last question is “yes”, please complete Table 3-4 below.

Table 3-3. System Interconnections

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Yes** | **No** | **If Yes, please describe.** |
| Does the new service workflow connect with other services? |  |  | *If “yes”, Table 3-4 (below) must be filled out.* |
| Does the new service workflow connect to a corporate network? |  |  |  |

If there are connections to other services offered by the CSP, please list each in the table below, using one row per connection. If there are no other services affected, please type “None” in the first row.

Table 3-4. Connections with Other Services

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Does Connection Exist?** | |  |
| **Service Connection** | **Yes** | **No** | **Interconnection Description** |
|  |  |  |  |
|  |  |  |  |

# FedRAMP Capabilities

## FedRAMP CIS Workbook

This section contains an updated Controls Implementation Summary (CIS) which identifies the CSP system security controls affected by the additional FedRAMP new services onboarding requirements. The CIS must be filled out entirely and must clearly indicate the current control status for the new service (i.e., which controls the new service or feature leverages) and the control status for the parent Cloud Service Offering.



* + 1. Change Management Maturity

As part of operational Continuous Monitoring, FedRAMP mandates all system changes undergo the CSP-approved configuration and change control processes and measures from the original P-ATO. As part of this new service offering service or feature onboarding, the 3PAO verifies that the CSP internal change management processes have been fully implemented, a security impact analysis has been completed, and the change has been approved by the Change Control Board. Assurance of, and 3PAO attestation to, a strong CSP change management capability indicates a more mature change management capability, and influences a FedRAMP approval decision, especially for larger systems where the service is integrated into the system development life cycle (SDL).

The Change Request and test results for the new service to be onboarded are included as an attachment to this request. Also, all security development artifacts, such as threat models or other evidence that demonstrate the organizational security development practices that were exercised during the onboarding of the new service are included within the artifacts submitted

The 3PAO must answer the questions below.

Table 4-1. Change Management

| **Question** | **Yes** | **No** | **If “no”, please describe how this is accomplished.** |
| --- | --- | --- | --- |
| Does the CSP’s change management process incorporate the necessary system and security information necessary to assess the security impact of the new service within the existing system boundary? |  |  |  |
| Has the change request been approved by the required persons with security responsibility for the CSP’s CCB? If yes, please provide the date of the approval. |  |  |  |
| Do the results in the CSP’s test plan demonstrate a successful deployment and integration test of the new service in a development or test environment prior to production deployment? |  |  |  |
| Do the security development artifacts provided demonstrate that the vendor has assessed the new service using their existing security development standards and processes? |  |  |  |

* + 1. Vendor Dependencies and Teaming Agreements

The 3PAO must answer the questions below.

Table 4-2. Vendor Dependencies and Teaming Agreements

| **Question** | **Yes** | **No** | Instructions |
| --- | --- | --- | --- |
| Does the service have any dependencies on other vendors, such as for hypervisor and operating system patches? |  |  | If “yes,” please complete Table 4-3. Vendor Dependencies below. |
| Within the service, are all products still actively supported by their respective vendors? |  |  | If any are not supported, answer, “No.” |
| Does the CSP have teaming arrangements for system maintenance for the service? |  |  | If “yes,” please complete Table 4-4. Teaming Agreements below. |

If there are vendor dependencies, please list each in the table below, using one row per dependency. For example, if using another vendor’s operating system, list the operating system, version and vendor name in the first column, briefly indicate the CSP’s reliance on that vendor for patches, and indicate whether the vendor still develops and issues patches for that product. If there are no vendor dependencies, please type “None” in the first row.

Table 4-3. Vendor Dependency Details

|  |  | **Still Supported?** | | **Existing POA&M?** | |
| --- | --- | --- | --- | --- | --- |
| **Product and Vendor Name** | **Nature of Dependency** | **Yes** | **No** | **Yes** | **No** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

If there are teaming agreements, please list each in the table below, using one row per agreement and provide as attachments to this document. If there are no teaming agreements, please type “None” in the first row.

Table 4-4. Teaming Agreements Details

| **Organization Name** | **Nature of Teaming Agreement** |
| --- | --- |
|  |  |
|  |  |

* + 1. Continuous Monitoring (ConMon) Capabilities

In the tables below, please describe the 3PAO determination of the current state and effectiveness of the approved operational Continuous Monitoring status as applied to the new service to be onboarded As CSP internal onboarding processes and procedures many times mandates that the new service and/or feature to be onboarded must have been included internally as part of the internal Continuous Monitoring program, it is important to note how long the CSP Service Team has been participating successfully in the internal Continuous Monitoring program.

Please provide scan results which demonstrate the security configuration and patch status for the assets associated with the new service to be onboarded. Also please include any POA&M information associated to the service to be onboarded. This information should include any existing POA&Ms that have been adjusted to include the new service assets or any new POA&M items created as a result of the new service onboarding control validation.

Table 4-5. Continuous Monitoring Capabilities

| **Question** | **Yes** | **No** | **Describe capability, supporting evidence, and any missing elements** |
| --- | --- | --- | --- |
| Does the CSP have the ability to scan all hosts in the service inventory? Are the assets associated with the new service included in the latest ConMon submission? |  |  |  |
| Will these services be integrated into the normal monthly ConMon submission? |  |  |  |
| Is the CSP and the CSP Service Team properly maintaining their Plan of Actions and Milestones (POA&M), including timely, accurate, and complete information entries for new scan findings, vendor check-ins, and closure of POA&M items? |  |  |  |

|  |
| --- |
| **Continuous Monitoring Capabilities – Additional Details** |
|  |

1. CSPs may wish to consider the involvement of their 3PAO in observing the system development lifecycle and change management processes in order for the 3PAO to gain a better understanding of the CSP’s maturity in those areas and ultimately aid them in assessing whether or not CSPs are following their internal processes for onboarding new services. [↑](#footnote-ref-2)