FedRAMP High Readiness Assessment Report (RAR) Template



<CSP Name or Logo>

<System Name>

<Version #>

<Date>



|  |
| --- |
| This FedRAMP Readiness Assessment Report (RAR) template is intended for systems categorized at the **High** security impact level, in accordance with the Federal Information Processing Standards (FIPS) Publication 199 Security Categorization. A RAR template for Moderate systems is available on the FedRAMP web site. |

# Third Party Assessment Organization (3PAO) Attestation

An Accredited 3PAO must attest to the readiness of the Cloud Service Provider’s (CSP) system. To be considered FedRAMP-Ready, the CSP must meet all the requirements in Section 4.1, Federal Mandates. In addition, the 3PAO must assess the CSP’s ability to meet the requirements in Section 4.2, FedRAMP Requirements. The 3PAO must use its expert judgment to subjectively evaluate the CSP’s overall readiness and factor this evaluation into its attestation.   
**THE 3PAO SHOULD SUBMIT THE RAR ONLY IF THE CSP IS FULLY READY TO PURSUE A FedRAMP PROVISIONAL AUTHORIZATION-TO-OPERATE (P-ATO) or AGENCY AUTHORIZATION-TO-OPERATE (ATO) AT THE TIME OF ASSESSMENT.**

|  |
| --- |
| [3PAO name] attests to [CSP name and system name]’s readiness to meet the FedRAMP requirements as described in this FedRAMP Readiness Assessment Report (RAR). [3PAO name] recommends that the FedRAMP PMO grant [CSP system name] “FedRAMP-Ready” status based on the CSP’s security capabilities as of [Assessment Completion Date].  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.  This FedRAMP RAR was created in alignment with the FedRAMP requirements and guidance. While this report only contains summary information regarding a CSP’s ability to meet the FedRAMP requirements, it is based on [3PAO name]’s evaluation of [CSP name and system name] which included observations, evidence reviews, personnel interviews, and demonstrated capabilities of security implementations.  Lead Assessor’s Signature: X\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  <Lead Assessor’s Name>  <3PAO Name> |

# Readiness Assessment Activities

In one or two paragraphs, 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 in this report. If interviews were conducted, state the role(s) of the individuals interviewed. Names are not necessary. If testing or examination was performed, please briefly state what testing was conducted and what was examined.

# Executive Summary

In the space below, provide a one-paragraph description of the system that includes all the information provided in Table 3-1, System Information.

In the space below, make a statement as to the CSP’s overall readiness, then provide up to four paragraphs that summarize the information provided in Sections 4.1, 4.2, and 4.3, based on the 3PAO’s cybersecurity expertise and knowledge of FedRAMP, including notable strengths and other areas for consideration.

At a minimum, the 3PAOs must describe the following:

* Overall alignment with the National Institute of Science and Technology (NIST) definition of cloud computing according to NIST SP 800-145;
* Notable strengths and weaknesses;
* Ability to consistently maintain a clearly defined system boundary;
* Clearly defined customer responsibilities;
* Unique or alternative implementations;
* Overall maturity level relative to the system type, size, and complexity; and
* Overall operational maturity relative to how long the system and required security controls have been in operation

Table of Contents

[Third Party Assessment Organization (3PAO) Attestation i](#_Toc478479877)

[Readiness Assessment Activities i](#_Toc478479878)

[Executive Summary ii](#_Toc478479879)

[1. Introduction 1](#_Toc478479880)

[1.1. Purpose 1](#_Toc478479881)

[1.2. Outcomes 1](#_Toc478479882)

[1.3. FedRAMP Approach and Use of This Document 1](#_Toc478479883)

[2. General Guidance and Instructions 2](#_Toc478479884)

[2.1. Embedded Document Guidance 2](#_Toc478479885)

[2.2. Additional Instructions to 3PAOs 2](#_Toc478479886)

[3. CSP System Information 4](#_Toc478479887)

[3.1. Relationship to Other CSPs 4](#_Toc478479888)

[3.2. Authorization Boundary and Data Flow Diagrams 5](#_Toc478479889)

[3.2.1. Authorization Boundary 5](#_Toc478479890)

[3.2.2. Data Flow Diagrams 5](#_Toc478479891)

[3.3. Separation Measures [AC-4, SC-2, SC-3, SC-7] 6](#_Toc478479892)

[3.4. System Interconnections 6](#_Toc478479893)

[4. Capability Readiness 7](#_Toc478479894)

[4.1. Federal Mandates 7](#_Toc478479895)

[4.2. FedRAMP Requirements 7](#_Toc478479896)

[4.2.1. Approved Cryptographic Modules [SC-13] 7](#_Toc478479897)

[4.2.2. Transport Layer Security [NIST SP 800-52, Revision 1] 8](#_Toc478479898)

[4.2.3. Identification and Authentication, Authorization, and Access Control 8](#_Toc478479899)

[4.2.4. Audit, Alerting, Malware, and Incident Response 9](#_Toc478479900)

[4.2.5. Contingency Planning and Disaster Recovery 10](#_Toc478479901)

[4.2.6. Configuration and Risk Management 11](#_Toc478479902)

[4.2.7. Data Center Security 12](#_Toc478479903)

[4.2.8. Policies, Procedures, and Training 13](#_Toc478479904)

[4.3. Additional Capability Information 15](#_Toc478479905)

[4.3.1. Staffing Levels 15](#_Toc478479906)

[4.3.2. Change Management Maturity 15](#_Toc478479907)

[4.3.3. Vendor Dependencies and Agreements 16](#_Toc478479908)

[4.3.4. Continuous Monitoring (ConMon) Capabilities 16](#_Toc478479909)

[4.3.5. Status of System Security Plan (SSP) 17](#_Toc478479910)

List of Tables

[Table 3-1. System Information 4](#_Toc478479912)

[Table 3-2. Leveraged Systems 4](#_Toc478479913)

[Table 3-3. Leveraged Services 5](#_Toc478479914)

[Table 3-4. System Interconnections 6](#_Toc478479915)

[Table 3-5. Interconnection Security Agreements (ISAs) 6](#_Toc478479916)

[Table 4-1. Federal Mandates 7](#_Toc478479917)

[Table 4-2. Cryptographic Modules 7](#_Toc478479918)

[Table 4-3. Transport Layer Security 8](#_Toc478479919)

[Table 4-4. Identification and Authentication, Authorization, and Access Control 8](#_Toc478479920)

[Table 4-5. Audit, Alerting, Malware, and Incident Response 9](#_Toc478479921)

[Table 4-6. Contingency Planning and Disaster Recovery 10](#_Toc478479922)

[Table 4-7. Configuration and Risk Management 11](#_Toc478479923)

[Table 4-8. Data Center Security 12](#_Toc478479924)

[Table 4-9. Policies and Procedures 13](#_Toc478479925)

[Table 4-10. Missing Policy and Procedure Elements 15](#_Toc478479926)

[Table 4-11. Security Awareness Training 15](#_Toc478479927)

[Table 4-12. Staffing Levels 15](#_Toc478479928)

[Table 4-13. Change Management 15](#_Toc478479929)

[Table 4-14. Vendor Dependencies and Agreements 16](#_Toc478479930)

[Table 4-15. Vendor Dependency Details 16](#_Toc478479931)

[Table 4-16. Formal Agreements Details 16](#_Toc478479932)

[Table 4-17. Continuous Monitoring Capabilities 16](#_Toc478479933)

[Table 4-18. Continuous Monitoring Capabilities – Additional Details 17](#_Toc478479934)

[Table 4-19. Maturity of the System Security Plan 17](#_Toc478479935)

[Table 4-20. Controls Designated “Not Applicable” 17](#_Toc478479936)

[Table 4-21. Controls with an Alternative Implementation 17](#_Toc478479937)

# Introduction

## Purpose

This report and its underlying assessment are intended to enable FedRAMP to reach a FedRAMP-Ready decision for a specific Cloud Service Provider’s system based on organizational processes and the security capabilities of the High-impact information system. FedRAMP grants a FedRAMP-Ready designation when the information in this report indicates the CSP is likely to achieve a Joint Authorization Board (JAB) P-ATO or Agency ATO for the system.

## Outcomes

A 3PAO should only submit this report to FedRAMP if it determines the CSP’s system is fully ready to pursue, and likely to achieve, a JAB P-ATO or Agency ATO at the High security impact level. Submission of this report by the 3PAO does not guarantee a FedRAMP-Ready designation, nor does it guarantee a FedRAMP Authorization.

## FedRAMP Approach and Use of This Document

The RAR identifies clear and objective security capability requirements, where possible, while also allowing for the presentation of more subjective information. The clear and objective requirements enable the 3PAO to concisely identify whether a CSP is achieving the most important FedRAMP High baseline requirements. The combination of objective requirements and subjective information enables FedRAMP to render a readiness decision based on a more complete understanding of the CSP’s security capabilities.

Section 4, Capability Readiness, is organized into three sections:

* **Section 4.1, Federal Mandates**, identifies a small set of the Federal mandates a CSP must satisfy. FedRAMP will not waive any of these requirements.
* **Section 4.2, FedRAMP Requirements**, identifies an excerpt of the most compelling requirements from the NIST Special Publication (SP) 800 document series and FedRAMP guidance. A CSP is unlikely to achieve a FedRAMP Authorization if any of these requirements are not met.
* **Section 4.3, Additional Capability Information**, identifies additional information that is not tied to specific requirements, yet has typically reflected strongly on a CSP’s ability to achieve a FedRAMP Authorization.

# General Guidance and Instructions

## Embedded Document Guidance

This document contains embedded guidance intended to instruct the 3PAO on how to complete each section. This guidance ensures FedRAMP receives all the information necessary to render a FedRAMP-Ready decision.

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

## Additional Instructions to 3PAOs

3PAOs must adhere to the following instructions when preparing the RAR:

1. Do NOT submit the completed High RAR without first coordinating with the FedRAMP PMO via info@fedramp.gov.
2. On the Title Page, enter the CSP name, system name, version number, and date of this RAR submission. If this is a re-submission, be sure to increment the version number and adjust the date. Do not modify the title and version number in the template header.
3. The RAR must provide:
   1. An overview of the system;
   2. A subjective summary of the CSP’s overall readiness, including rationale such as notable strengths and other areas for consideration;
   3. An assessment of the CSP’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; and
   4. The 3PAO’s attestation regarding the CSP’s readiness to meet FedRAMP High baseline requirements.
4. FedRAMP will not consider a CSP for a FedRAMP-Ready designation unless all the requirements in Section 4.1, *Federal Mandates*, are met. Please note, meeting these requirements does not guarantee a FedRAMP-Ready designation.
5. 3PAOs must assess the system’s technical, management, and operational capabilities using a combination of methods, including interview, observation, demonstration, examination, and onsite visits (for example, 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 the diagrams. 3PAOs must **not** conduct this readiness assessment exclusively by reviewing a CSP’s written documentation and performing interviews. Active validation of all information provided within this report is required.
6. 3PAOs must complete all sections and address **all elements of each question**. 3PAOs must also describe observations of any missing elements (for example, if the CSP fails to meet all of the question elements). If a capability is fully inherited, answer *“yes”* and write *"fully inherited"* in the column provided for the capability description.
7. Control references are provided with each of the questions in Section 4.2*, FedRAMP Requirements*. These references are provided to help the 3PAO understand the basis for each question; however, the 3PAO is expected to consider all relevant FedRAMP security controls and capabilities when assessing the CSP’s capabilities.
8. FedRAMP believes a typical level of effort for conducting a readiness assessment for mid-size, straightforward systems is between two and four weeks, with the first half focused on information gathering and the second half focused on analysis and report development.

# CSP System Information

Provide and validate the information below. For example, if the deployment model is Government only, ensure there are no non-Government customers. This RAR template is intended for systems categorized at the **High** security impact level, in accordance with the FIPS Publication 199 Security Categorization.

Table 3-1. System Information

|  |
| --- |
| CSP Name:  System Name:  Service Model: (IaaS, PaaS, SaaS)  FIPS PUB 199 System Security Level: (High)  Fully Operational as of: Enter the date the system became fully operational.  Number of Customers (US Federal/Others): Enter # of US Federal customers / # of other customers  Deployment Model: Is the service a Public Cloud, Government-Only Cloud, Federal Government-Only Cloud, or DOD Cloud?  System Functionality: Briefly describe the functionality of the system and service being provided. |

## Relationship to Other CSPs

If this High baseline system resides in another CSP’s environment or inherits security capabilities, please provide the relevant details in Tables 3-2 and 3-3 below. Please note, the leveraged system itself must be FedRAMP-Authorized by having a FedRAMP P-ATO or an Agency ATO and not just the vendor. For example, a large CSP may have a commercial service offering and a separate service offering with a FedRAMP Authorization. Only the service offering with the FedRAMP Authorization may be leveraged.

|  |
| --- |
| **IMPORTANT:** If there is a leveraged system, be sure to note every capability in Section 4 that partially or fully leverages the underlying system. When doing so, indicate the capability is fully inherited or describe both the inherited and non-inherited aspects of the capability. If the CSP’s service offering leverages another system that does not have a JAB P-ATO or Agency ATO, the CSP is then responsible for the entire “stack”. |

Table 3-2. Leveraged Systems

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Question** | **Yes** | **No** | **N/A** | **If Yes, please describe.** |
| 1 | Is this system leveraging an underlying provider? |  |  |  | If “yes,” identify the underlying system. |
| 2 | If “yes,” does the leveraged system have a JAB P-ATO? |  |  |  | Enter the date the leveraged system received FedRAMP JAB P-ATO.  If there is no underlying provider, indicate “N/A”.  If the leveraged system does not have a JAB P-ATO, please refer to question 3. |
| 3 | 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.  If there is no underlying provider, indicate “N/A.” |

List all **services** leveraged. The system from which the service is leveraged must be listed in Table 3-2 above.

Table 3-3. Leveraged Services

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Service** | **Service Capability** | **System** |
| 1 | State what is being leveraged or “None” if no service is leveraged or if the CSP is responsible for the stack. | List the capability the service provides (e.g., load balancer, database, audit logging). | Identify the system from which the service is being leveraged. |
| 2 |  |  |  |

## Authorization Boundary and Data Flow Diagrams

|  |
| --- |
| **IMPORTANT:**   * Ensuring authorization boundary accuracy in the RAR is critical to FedRAMP authorization activities. Inaccuracies within the RAR may give authorizing officials and FedRAMP grounds for removing a vendor from assessment and authorization activities. * All services must be included in the CSP’s authorization boundary and must be assessed by the 3PAO. If the system is leveraging external services from a FedRAMP authorized system, the interfaces to these services must be included in the boundary and must also be assessed by the 3PAO. |

The 3PAO must perform full authorization boundary validation for the RAR, ensure nothing is missing from the CSP-identified boundary, and ensure all included items are actually present and are part of the system inventory. To achieve this, the 3PAO must perform activities including, but not limited to, discovery scans, in-person interviews, and physical examinations where appropriate.

In the space below, the 3PAO must provide a statement verifying that all services are within the CSP’s authorization boundary and/or within the boundary of a leveraged FedRAMP authorized system, AND no other services are being leveraged by the CSP.

* + 1. Authorization Boundary

Insert 3PAO-validated network and architecture diagram(s) and provide a written description of the Authorization Boundary. The 3PAO must ensure each diagram:

* includes a clearly defined authorization boundary;
* clearly defines services as wholly within the boundary;
* depicts all major components or groups within the boundary;
* identifies all interconnected systems;
* depicts all major software/virtual components (or groups of) within the boundary;
* is validated against the inventory; and
* identifies all systems related to, but excluded from the boundary.
  + 1. Data Flow Diagrams

Insert 3PAO-validated data flow diagram(s), and provide a written description of the data flows. The diagram(s) must:

* clearly identify anywhere Federal data is to be processed, stored, or transmitted;
* clearly delineate how data comes in to and out of the system boundary;
* clearly identify data flows for privileged, non-privileged, and customers’ access; and
* depict how **all ports, protocols, and services** of all inbound and outbound traffic are represented and managed.

## Separation Measures [AC-4, SC-2, SC-3, SC-7]

Assess and describe the strength of the physical and/or logical separation measures in place to provide segmentation and isolation of tenants, administration, and operations; addressing user-to-system; admin-to-system; and system-to-system relationships.

The 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. The 3PAO must describe the methods used to verify the strength of separation measures.

## System Interconnections

A System Interconnection is a dedicated connection between information systems, such as between a SaaS/PaaS and underlying IaaS.

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 3-5 below.

Table 3-4. System Interconnections

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Question** | **Yes** | **No** | **If Yes, please describe.** |
| 1 | Does the system connect to the Internet? |  |  |  |
| 2 | Does the system connect to a corporate network? |  |  |  |
| 3 | Could the system support a Trusted Internet Connection (TIC) requirement from a Federal Agency? |  |  |  |
| 4 | Does the system connect to external systems? |  |  | If “yes,” complete Table 3-5 below. |

If there are connections to external systems, please list each in the table below, using one row per interconnection. If there are no external system connections, please type “None” in the first row.

Table 3-5. Interconnection Security Agreements (ISAs)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **Does an ISA Exist?** | |  |
| **#** | **External System Connection** | **Yes** | **No** | **Interconnection Description.  If no ISA, please justify below.** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

# Capability Readiness

## Federal Mandates

This section identifies Federal requirements applicable to all FedRAMP authorized systems. All requirements in this section must be met. Some of these topics are also covered in greater detail in Section 4.2, *FedRAMP Requirements,* below.

Only answer “Yes” if the requirement is fully and strictly met. The 3PAO must answer “No” if an alternative implementation is in place.

Table 4-1. Federal Mandates

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Compliance Topic** | **Fully Compliant?** | |
| **Yes** | **No** |
| 1 | Are FIPS 140-2 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required? |  |  |
| 2 | Can the system fully support user authentication via Agency Common Access Card (CAC) or Personal Identity Verification (PIV) credentials? |  |  |
| 3 | Is the system operating at eAuth Level 4? |  |  |
| 4 | Does the CSP have the ability to consistently remediate High vulnerabilities within 30 days and Moderate vulnerabilities within 90 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? |  |  |

## FedRAMP Requirements

This section identifies additional FedRAMP Readiness requirements. All requirements in this section must be met; however, alternative implementations and non-applicability justifications may be considered on a limited basis.

* + 1. Approved Cryptographic Modules [SC-13]

The 3PAO must ensure FIPS 140-2 **Validated** or NSA-Approved algorithms are used for all encryption modules. FIPS 140-2 **Compliant** is **not** sufficient. The 3PAO may add rows to the table if appropriate, but must not remove the original rows. The 3PAO must identify all non-compliant cryptographic modules in use.

Table 4-2. Cryptographic Modules

| **#** | **Cryptographic Module Type** | **FIPS 140-2 Validated?** | | **NSA Approved?** | | **Describe Any Alternative Implementations (if applicable)** | **Describe Missing Elements or N/A Justification** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Yes** | **No** | **Yes** | **No** |  |  |
| 1 | Data at Rest [SC-28] |  |  |  |  |  |  |
| 2 | Transmission [SC-8 (1), SC-12, SC-12(1, 2, 3), SC-13] |  |  |  |  |  |  |
| 3 | Remote Access [AC-17 (2)] |  |  |  |  |  |  |
| 4 | Authentication [IA-5 (1), IA-7] |  |  |  |  |  |  |
| 5 | Digital Signatures/Hash [CM-5 (3)] |  |  |  |  |  |  |

* + 1. Transport Layer Security [NIST SP 800-52, Revision 1]

The 3PAO must identify all protocols in use. The 3PAO may add rows to the table if appropriate, but must not remove the original rows.

Table 4-3. Transport Layer Security

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **The** **Cryptographic Module Type** | **Protocol In Use?** | | **If “yes,” please describe use for both internal and external communications** |
| **Yes** | **No** |
| 1 | SSL (Non-Compliant) |  |  |  |
| 2 | TLS 1.0 (Non-Compliant) |  |  |  |
| 3 | TLS 1.1 (Compliant) |  |  |  |
| 4 | TLS 1.2 (Compliant) |  |  |  |

* + 1. Identification and Authentication, Authorization, and Access Control

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.

Table 4-4. Identification and Authentication, Authorization, and Access Control

| **#** | **Question** | **Yes** | **No** | **Describe capability, supporting evidence, and any missing elements** |
| --- | --- | --- | --- | --- |
| 1 | Does the system support federal user authentication via CAC/PIV credentials? [IA-2(12)] |  |  |  |
| 2 | Does the system uniquely identify and authorize organizational users (or processes acting on behalf of organizational users) in a manner that cannot be repudiated and which sufficiently reduces the risk of impersonation? [IA-2, IA-4, IA-4(4)] |  |  |  |
| 3 | Does the system require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2(1), IA-2(3), IA-2(11)] |  |  |  |
| 4 | Does the system fully comply with eAuth Level 4? [NIST SP 800-63] |  |  | State the eAuth Level and provide sufficient details demonstrating that the system complies with this level, consistent with NIST SP 800-63. |
| 5 | Does the system employ automated mechanisms to support Account Management? [AC-2(1), PS-4(2)] |  |  |  |
| 6 | Does the system restrict non-authorized personnel’s access to resources? [AC-6(2)] |  |  |  |
| 7 | Does the system restrict non-privileged users from performing privileged functions? [AC-6(10)] |  |  |  |
| 8 | Does the system ensure secure separation of customer data? [SC-4] |  |  | The capability description is not required here, but must be included in Section 3.3, Separation Measures. |
| 9 | Does the system ensure secure separation of customer processing environments? [SC-2] |  |  | The capability description is not required here, but must be included in Section 3.3, Separation Measures. |
| 10 | Does the system isolate security functions from nonsecurity functions? [SC-3] |  |  |  |
| 11 | Does the system restrict access of administrative personnel in a way that limits the capability of individuals to compromise the security of the information system? [AC-2(7)] |  |  |  |
| 12 | Does the remote access capability include CSP-defined and implemented usage restrictions, configuration guidance, and authorization procedure? [AC-17] |  |  |  |

* + 1. Audit, Alerting, Malware, and Incident Response

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.

Table 4-5. Audit, Alerting, Malware, and Incident Response

| **#** | **Question** | **Yes** | **No** | **Describe capability, supporting evidence, and any missing elements** |
| --- | --- | --- | --- | --- |
| 1 | Does the system have the capability to detect, contain, and eradicate malicious software? [SI-3, SI-3 (1), SI-3 (2), SI-3 (7), MA-3 (2)] |  |  |  |
| 2 | Does the system store audit data in a tamper-resistant manner which meets chain of custody and any e-discovery requirements? [AU-7, AU-9] |  |  |  |
| 3 | Does the CSP have the capability to detect unauthorized or malicious use of the system, including insider threat and external intrusions? [SI-4, SI-4 (4)] |  |  |  |
| 4 | Does the CSP have the capability to automatically detect and respond to unauthorized system changes? [SI-7, SI-7(2), SI-7(5)] |  |  |  |
| 5 | Does the CSP have the capability to analyze outbound communications traffic for anomalies? [SI-4(11)] |  |  |  |
| 6 | Does the CSP have the capability to detect and prevent covert exfiltration of information? [SC-7(10), SI-4(18)] |  |  |  |
| 7 | Does the CSP have an Incident Response Plan and a fully developed Incident Response test plan? [IR-3, IR-8] |  |  |  |
| 8 | Does the CSP have a plan and capability to perform security code analysis and assess code for security flaws, as well as identify, track and remediate security flaws? [SA-11, SA-11 (1), SA-11 (8)] |  |  | If the system contains no custom software development, do not answer “Yes” or “No.” Instead, state “NO CUSTOM CODE” here. |
| 9 | Does the CSP implement automated mechanisms for incident tracking, handling, reporting, and analysis? [IR-4 (1), IR-5(1) IR-6 (1)] |  |  |  |
| 10 | Does the CSP implement automated tools, such as Security Information and Event Management (SIEM) technologies, to support the integrated auditing, logging, and real time analysis of security-related events and alerts? [AU-6(1), SI-4(2)] |  |  |  |
| 11 | Does the CSP retain online audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and offline for at least one year to meet regulatory and organizational information retention requirements? [AU-4, AU-6, AU-7, AU-7 (1), AU-11] |  |  |  |
| 12 | Does the CSP have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations? [*FedRAMP Incident Communications Procedures*] |  |  |  |
| 13 | Does the CSP employ automated mechanisms to make security alert and advisory information available throughout the organization? [SI-5(1)] |  |  |  |

* + 1. Contingency Planning and Disaster Recovery

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.

Table 4-6. Contingency Planning and Disaster Recovery

| **#** | **Question** | **Yes** | **No** | **Describe capability, supporting evidence, and any missing elements** |
| --- | --- | --- | --- | --- |
| 1 | Does the CSP have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? [CP-2, CP-2 (2), CP-2 (3), CP-9, CP-10] |  |  |  |
| 2 | Does the CSP have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with NIST Special Publication 800-34? [CP-2, CP-8] |  |  |  |
| 3 | Does the system have alternate storage and processing facilities? [CP-6, CP-7] |  |  |  |
| 4 | Does the system have primary and alternate telecommunications services from different providers? [CP-8, CP-8 (2), CP-8 (3)] |  |  |  |
| 5 | Does the system have backup power generation or other redundancy? [PE-11] |  |  |  |
| 6 | Does the CSP have service level agreements (SLAs) in place with all telecommunications providers? [CP-8 (1)] |  |  |  |

* + 1. Configuration and Risk Management

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.

Table 4-7. Configuration and Risk Management

| **#** | **Question** | **Yes** | **No** | **Describe capability, supporting evidence, and any missing elements** |
| --- | --- | --- | --- | --- |
| 1 | Does the CSP employ automated mechanisms to maintain a current, complete, and accurate baseline configuration of the information system? [CM-2, CM-2(2)] |  |  |  |
| 2 | Does the CSP employ automated mechanisms to maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8, CM-8(2)] |  |  |  |
| 3 | Does the CSP employ automated mechanisms to detect inventory and configuration changes? [CM-6(1), CM-8(3)] |  |  |  |
| 4 | Does the CSP have a Configuration Management Plan? [CM-9, CM-11] |  |  |  |
| 5 | Does the CSP employ automated mechanisms to implement a formal change control process? [CM-3, CM-3(1)] |  |  |  |
| 6 | Does the CSP’s formal change control process include a security impact assessment? [CM-4] |  |  |  |
| 7 | Does the CSP prevent unauthorized changes to the system? [CM-5, CM-5(1), CM-5(5), CM-11, CM-11(1)] |  |  |  |
| 8 | Does the CSP establish configuration settings for products employed that reflect the most restrictive mode consistent with operational requirements? [CM-6] |  |  | If “yes,” describe if the configuration settings are based on Center for Internet Security (CIS) Benchmarks or United States Government Configuration Baseline (USGCB), or “most restrictive consistent with operational requirements.” |
| 9 | Does the CSP ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP)-validated or SCAP-compatible (if validated checklists are not available)? [CM-6] |  |  |  |

For the following questions, 3PAOs may use Table 4-18 (Continuous Monitoring Capabilities – Additional Details) to enter the capability descriptions, supporting evidence and missing elements.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 10 | Does the CSP perform **authenticated** operating system/ infrastructure, web, and database vulnerability scans at least monthly, as applicable? [RA-5, RA-5(5), SI-2(2)] |  |  | Describe how the 3PAO validated that vulnerability scans were fully authenticated. |
| 11 | Does the CSP demonstrate the capability to remediate High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days? [RA-5, *FedRAMP Continuous Monitoring Guide*] |  |  | Describe how the 3PAO validated that the CSP remediates High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days. |
| 12 | When a High vulnerability is identified as part of ConMon activities, does the CSP consistently check audit logs for evidence of exploitation? [RA-5(8)] |  |  |  |

* + 1. Data Center Security

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.

Table 4-8. Data Center Security

| **#** | **Question** | **Yes** | **No** | **Describe capability, supporting evidence, and any missing elements** |
| --- | --- | --- | --- | --- |
| 1 | Does the CSP restrict physical system access to only authorized personnel? [PE-2 through PE-6, PE-8] |  |  |  |
| 2 | Does the CSP monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8, PE-8(1)] |  |  |  |
| 3 | Does the CSP monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6 (1)] |  |  |  |
| 4 | Does the CSP implement automatic mechanisms to handle water or fire incidents? [PE-13(1), PE-13(2), PE-13(3) PE-15(1)] |  |  |  |

* + 1. Policies, Procedures, and Training

The 3PAO must indicate the status of policy and procedure coverage for the NIST 800-53 Rev 4 families listed in Table 4-9 below.

**To answer “yes” to a policy**, it must be fully developed, documented, and disseminated; and it must address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. A single policy document may address more than one family provided the NIST requirements of each “-1” are fully addressed.

**To answer “yes” to a procedure**, it must be fully developed and consistently followed by the appropriate staff. List all applicable procedure documents for each family.

CSPs must establish their own set of Policies and Procedures (P&Ps). They cannot be inherited from a leveraged system, nor can they be provided by the customer. Any exceptions and/or missing policy and procedure elements must be explained in Table 4-10 below.

Table 4-9. Policies and Procedures

| **#** | **Family** | **Policy** | | **Procedure** | | **Title Version and Date** |
| --- | --- | --- | --- | --- | --- | --- |
| **Yes** | **No** | **Yes** | **No** |
| 1 | Access Control [AC-1] |  |  |  |  | Policy:  Procedure(s): |
| 2 | Awareness & Training [AT-1] |  |  |  |  | Policy:  Procedure(s): |
| 3 | Audit & Accountability [AU-1] |  |  |  |  | Policy:  Procedure(s): |
| 4 | Security Assessment & Authorization [CA-1] |  |  |  |  | Policy:  Procedure(s): |
| 5 | Configuration Management [CM-1] |  |  |  |  | Policy:  Procedure(s): |
| 6 | Contingency Planning [CP-1] |  |  |  |  | Policy:  Procedure(s): |
| 7 | Identification & Authentication [IA-1] |  |  |  |  | Policy:  Procedure(s): |
| 8 | Incident Response [IR-1] |  |  |  |  | Policy:  Procedure(s): |
| 9 | Maintenance [MA-1] |  |  |  |  | Policy:  Procedure(s): |
| 10 | Media Protection [MP-1] |  |  |  |  | Policy:  Procedure(s): |
| 11 | Physical & Environmental Protection [PE-1] |  |  |  |  | Policy:  Procedure(s): |
| 12 | Personnel Security [PS-1] |  |  |  |  | Policy:  Procedure(s): |
| 13 | Risk Assessment [RA-1] |  |  |  |  | Policy:  Procedure(s): |
| 14 | System & Services Acquisition [SA-1] |  |  |  |  | Policy:  Procedure(s): |
| 15 | System & Communications Protection [SC-1] |  |  |  |  | Policy:  Procedure(s): |
| 16 | System & Information Integrity [SI-1] |  |  |  |  | Policy:  Procedure(s): |
| 17 | Planning [PL-1] |  |  |  |  | Policy:  Procedure(s): |

For any family with a policy or procedure gap, please describe the gap below.

Table 4-10. Missing Policy and Procedure Elements

|  |
| --- |
| **Missing Policy and Procedure Elements** |
|  |

The 3PAO must answer the questions below.

Table 4-11. Security Awareness Training

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Yes** | **No** | **Describe capability, supporting evidence, and any missing elements** |
| Does the CSP train personnel on security awareness and role-based security responsibilities? |  |  |  |

## Additional Capability Information

FedRAMP will evaluate the responses in this section on a case-by-case basis relative to a FedRAMP-Ready designation decision.

* + 1. Staffing Levels

In the table below, the 3PAO must describe the CSP’s organizational structure, staffing levels currently dedicated to the security of the system, as well as any planned changes to these staffing levels. This description must clearly indicate role and number of individuals as well as identify which staff is dedicated full-time, and which are performing their role as a collateral duty.

Table 4-12. Staffing Levels

|  |
| --- |
| **Staffing Levels** |
|  |

* + 1. Change Management Maturity

While the following change management capabilities are not required, they indicate a more mature change management capability and may influence a FedRAMP-Readiness decision, especially for larger systems.

The 3PAO must answer the questions below.

Table 4-13. Change Management

| **#** | **Question** | **Yes** | **No** | **If “no”, please describe how this is accomplished.** |
| --- | --- | --- | --- | --- |
| 1 | Does the CSP’s change management capability include a fully functioning Change Control Board (CCB)? |  |  |  |
| 2 | Does the CSP have and use development and/or test environments to verify changes before implementing them in the production environment? |  |  |  |

* + 1. Vendor Dependencies and Agreements

The 3PAO must answer the questions below.

Table 4-14. Vendor Dependencies and Agreements

| **#** | **Question** | **Yes** | **No** | Instructions |
| --- | --- | --- | --- | --- |
| 1 | Does the system have any dependencies on other vendors such as a leveraged service offering, hypervisor and operating system patches, physical security and/or software and hardware support? |  |  | If “yes,” please complete Table 4-15. Vendor Dependency Details below. |
| 2 | Within the system, are all products still actively supported by their respective vendors? |  |  | If any are not supported, answer “No.” |
| 3 | Does the CSP have a formal agreement with a vendor, such as for maintenance of a leveraged service offering? |  |  | If “yes,” please complete Table 4-16, Formal Agreements Details 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 4-15. Vendor Dependency Details

|  |  |  | **Still Supported?** | |
| --- | --- | --- | --- | --- |
| **#** | **Product and Vendor Name** | **Nature of Dependency** | **Yes** | **No** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

If there are formal vendor agreements in place, please list each in the table below, using one row per agreement. If there are no formal agreements, please type “None” in the first row.

Table 4-16. Formal Agreements Details

| **#** | **Organization Name** | **Nature of Agreement** |
| --- | --- | --- |
| 1 |  |  |
| 2 |  |  |

* + 1. Continuous Monitoring (ConMon) Capabilities

In the tables below, please describe the current state of the CSP’s ConMon capabilities, as well as the length of time the CSP has been performing ConMon for this system.

Table 4-17. Continuous Monitoring Capabilities

| **#** | **Question** | **Yes** | **No** | **Describe capability, supporting evidence, and any missing elements** |
| --- | --- | --- | --- | --- |
| 1 | Does the CSP have a lifecycle management plan that ensures products are updated before they reach the end of their vendor support period? |  |  |  |
| 2 | Does the CSP have the ability to scan all hosts in the inventory? |  |  |  |
| 3 | Does the CSP have the ability to provide scan files in a structure data format, such as CSV, XML, or .nessus files? |  |  |  |
| 4 | Is the CSP 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? |  |  |  |

In the table below, provide any additional details the 3PAO believes to be relevant to FedRAMP’s understanding of the CSP’s Continuous Monitoring Capabilities. If the 3PAO has no additional details, please state, “None.”

Table 4-18. Continuous Monitoring Capabilities – Additional Details

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

* + 1. Status of System Security Plan (SSP)

In the table below, explicitly state whether the SSP is fully developed, partially developed, or non-existent. Identify any sections that the CSP has not yet developed.

Table 4-19. Maturity of the System Security Plan

|  |
| --- |
| **Maturity of the System Security Plan** |
|  |

In the table below, state the number of controls identified as “Not applicable” in the SSP. List the Control Identifier for each, and indicate whether a justification for each has been provided in the SSP control statement.

Table 4-20. Controls Designated “Not Applicable”

|  |
| --- |
| **<x> Controls are Designated “Not Applicable”** |
|  |

In the table below, state the number of controls with an alternative implementation. List the Control Identifier for each.

Table 4-21. Controls with an Alternative Implementation

|  |
| --- |
| **<x> Controls have an Alternative Implementation** |
|  |