FedRAMP Readiness Assessment Report (RAR)



<CSP Name or Logo>

<System Name>

Version 1.0

<Date>

**Company Sensitive and Proprietary**

**For Authorized Use Only**



# 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 of 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.

|  |
| --- |
| [3PAO name] attests to [CSP name and system name]’s readiness to meet the FedRAMP requirements as described in this FedRAMP Readiness Assessment Report. [3PAO name] recommends that the FedRAMP PMO grant [CSP system name] “FedRAMP-Ready” status.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 Readiness Assessment Report 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> |

# 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, 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.

The 3PAOs should consider the following when evaluating a CSP’s overall readiness:

* 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.

Table of Contents

[Third Party Assessment Organization (3PAO) Attestation i](#_Toc458001239)

[Executive Summary ii](#_Toc458001240)

[1. Introduction 1](#_Toc458001241)

[1.1. Purpose 1](#_Toc458001242)

[1.2. Outcomes 1](#_Toc458001243)

[1.3. FedRAMP Approach and Use of This Document 1](#_Toc458001244)

[2. General Guidance and Instructions 2](#_Toc458001245)

[2.1. Embedded Document Guidance 2](#_Toc458001246)

[2.2. Additional Instructions to 3PAOs 2](#_Toc458001247)

[3. CSP System Information 3](#_Toc458001248)

[3.1. Relationship to Other CSP 3](#_Toc458001249)

[3.2. Authorization Boundary and Data Flow Diagrams 3](#_Toc458001250)

[3.2.1. Authorization Boundary 3](#_Toc458001251)

[3.2.1.1. Boundary Exclusions 4](#_Toc458001252)

[3.2.2. Data Flow Diagrams 4](#_Toc458001253)

[3.2.3. Separation Measures 4](#_Toc458001254)

[3.3. System Interconnections 4](#_Toc458001255)

[4. Capability Readiness 5](#_Toc458001256)

[4.1. Federal Mandates 5](#_Toc458001257)

[4.2. FedRAMP Requirements 5](#_Toc458001258)

[4.2.1. Approved Cryptographic Modules [SC-13] 5](#_Toc458001259)

[4.2.2. Transport Layer Security [NIST SP 800-52, Revision 1] 6](#_Toc458001260)

[4.2.3. Identification and Authentication, Authorization, and Access Control 6](#_Toc458001261)

[4.2.4. Audit, Alerting, Malware, and Incident Response 7](#_Toc458001262)

[4.2.5. Contingency Planning and Disaster Recovery 8](#_Toc458001263)

[4.2.6. Configuration and Risk Management 9](#_Toc458001264)

[4.2.7. Data Center Security 10](#_Toc458001265)

[4.2.8. Policies, Procedures, and Training 10](#_Toc458001266)

[4.3. Additional Capability Information 13](#_Toc458001267)

[4.3.1. Staffing Levels 13](#_Toc458001268)

[4.3.2. Change Management Maturity 13](#_Toc458001269)

[4.3.3. Vendor Dependencies and Teaming Agreements 13](#_Toc458001270)

[4.3.4. Continuous Monitoring (ConMon) Capabilities 14](#_Toc458001271)

[4.3.5. Status of System Security Plan (SSP) 15](#_Toc458001272)

List of Tables

[Table 3-1. System Information 3](#_Toc458001273)

[Table 3-2. Relationship to Other CSP 3](#_Toc458001274)

[Table 3-3. System Interconnections 4](#_Toc458001275)

[Table 3-4. Interconnection Security Agreements (ISAs) 4](#_Toc458001276)

[Table 4-1. Federal Mandates 5](#_Toc458001277)

[Table 4-2. Cryptographic Modules 5](#_Toc458001278)

[Table 4-3. Transport Layer Security 6](#_Toc458001279)

[Table 4-4. Identification and Authentication, Authorization, and Access Control 6](#_Toc458001280)

[Table 4-5. Audit, Alerting, Malware, and Incident Response 7](#_Toc458001281)

[Table 4-6. Contingency Planning and Disaster Recovery 8](#_Toc458001282)

[Table 4-7. Configuration and Risk Management 9](#_Toc458001283)

[Table 4-8. Data Center Security 10](#_Toc458001284)

[Table 4-9. Policies and Procedures 11](#_Toc458001285)

[Table 4-10. Missing Policy and Procedure Elements 12](#_Toc458001286)

[Table 4-11. Security Awareness Training 12](#_Toc458001287)

[Table 4-12. Staffing Levels 13](#_Toc458001288)

[Table 4-13. Change Management 13](#_Toc458001289)

[Table 4-14. Vendor Dependencies and Teaming Agreements 13](#_Toc458001290)

[Table 4-15. Vendor Dependency Details 14](#_Toc458001291)

[Table 4-16. Teaming Agreements Details 14](#_Toc458001292)

[Table 4-17. Continuous Monitoring Capabilities 14](#_Toc458001293)

[Table 4-18. Continuous Monitoring Capabilities – Additional Details 15](#_Toc458001294)

[Table 4-19. Maturity of the System Security Plan 15](#_Toc458001295)

[Table 4-20. Controls Designated “Not Applicable” 15](#_Toc458001296)

[Table 4-21. Controls with an Alternative Implementation 15](#_Toc458001297)

# 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 (CSP) system based on organizational processes and the security capabilities of the 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) Provisional Authorization-to-Operate (P-ATO) or Agency ATO for the system.

## Outcomes

A Third Party Assessment Organization (3PAO) should only submit this report to FedRAMP if it determines the CSP’s system is likely to achieve a JAB P-ATO or Agency ATO. 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 Readiness Assessment Report (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 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 National Institute of Science and Technology (NIST) Special Publication (SP) 800 series documents 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 the completion of 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, but before it is submitted to FedRAMP.

## Additional Instructions to 3PAOs

The 3PAO must adhere to the following instructions when preparing the RAR:

1. 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.
	4. The 3PAO’s attestation to the CSP’s readiness to meet FedRAMP requirements.
2. 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.
3. The 3PAO must assess the system’s technical, management, and operational capabilities using a combination of methods, including interview, observation, demonstration, inspection, and onsite visits (e.g., in-person interviews and data center visits as needed). The 3PAO may use CSP-provided diagrams, but must validate the diagrams as though the 3PAO created the diagrams. The 3PAO 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.
4. The 3PAO must complete all sections and answer all capability questions unless otherwise specified. If a capability is fully inherited, answer “yes” and write *fully inherited* in the column provided for the capability description.
5. Control references are provided with each of the questions in Section 4.2*, FedRAMP Requirements*. These 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.
6. 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

Table 3-1. System Information

|  |
| --- |
| CSP Name:System Name:Service Model: (IaaS, PaaS, SaaS)FIPS PUB 199 System Security Level: (Low, Moderate or High)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 CSP

If this system resides in another CSP’s environment or is inheriting security capabilities, please provide the relevant details below.

Table 3-2. 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 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. |

The 3PAO must perform full authorization boundary validation for the RAR; must 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 and in person interviews and physical inspections where appropriate.

* + 1. Authorization Boundary

Insert 3PAO-validated network and architecture diagram(s). The 3PAO must ensure each diagram:

* includes a clearly defined authorization boundary;
* clearly defines services 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; and
* is validated against the inventory.
	+ - 1. Boundary Exclusions

The 3PAO must clearly describe the following:

* all shared corporate services with explicit rationale of any that are **not** within the boundary, such as a corporate Security Operations Center (SOC) or corporate security awareness training; and
* all systems related to, but excluded from the boundary.

In addition to describing these, they must be depicted either in the Authorization Boundary diagrams above or in separate diagrams here.

* + 1. Data Flow Diagrams

Insert 3PAO-validated data flow diagram(s). Each diagram should:

* clearly identify anywhere Federal data is to be processed, stored, or transmitted;
* clearly delineate how data comes into and out of the system boundary; and
* depict how all ports, protocols, and services of all inbound and outbound traffic are represented and managed.
	+ 1. Separation Measures

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.

## System 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 system connect to the Internet? |  |  |  |
| Does the system connect to a corporate network? |  |  |  |
| Does the system have an existing Trusted Internet Connection (TIC) capability? |  |  |  |
| Does the system connect to external systems? |  |  |  If “yes”, Table 3-4. ISAs below must be filled out. |

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 3-4. Interconnection Security Agreements (ISAs)

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

# 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.

Table 4-1. Federal Mandates

|  |  |
| --- | --- |
| **Compliance Topic** | **Fully Compliant?** |
| **Yes** | **No** |
| Are FIPS 140-2 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used? |  |  |
| Can the system fully support user authentication via Agency Common Access Card (CAC) or Personal Identity Verification (PIV) credentials? |  |  |
| Is the system operating at the minimum eAuth level for its FIPS-199 designated level of operation (Level 3 for Moderate, Level 4 for High)? |  |  |
| Does the CSP have the ability to consistently remediate High vulnerabilities in 30 days and Moderate vulnerabilities in 90 days? |  |  |
| 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 Implementation(if applicable)** | **Describe Missing Elements or N/A Justification** |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **Yes** | **No** |  |  |
| Data at Rest [SC-28] |  |  |  |  |  |  |
| Transmission [SC-8 (1), SC-12, SC-12(2, 3) ] |  |  |  |  |  |  |
| Remote Access [AC-17 (2)] |  |  |  |  |  |  |
| Authentication [IA-5 (1), IA-7] |  |  |  |  |  |  |
| 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** |
| SSL (Non-Compliant) |  |  |  |
| TLS 1.0 (Non-Compliant) |  |  |  |
| **TLS 1.1 (Compliant)** |  |  |  |
| **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** |
| --- | --- | --- | --- |
| Does the system identify and authorize users in a manner that cannot be repudiated and which sufficiently reduces the risk of impersonation? [IA-2] |  |  |  |
| Does the system require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2(1), IA-2(3)] |  |  |  |
| Does the system uniquely identify each individual user? [IA-4, IA-4(4)] |  |  |  |
| Does the system fully comply with eAuth Level 3 or higher? [NIST SP 800-63] |  |  |  State the eAuth Level, and provide sufficient details that justify this level, consistent with NIST SP 800-63. |
| Does the system restrict non-authorized personnel’s access to resources? [AC-6(2)] |  |  |  |
| Does the system restrict non-privileged users from performing privileged function? [AC-6(10)] |  |  |  |
| Does the system ensure secure separation of customer data? [SC-4] |  |  |  |
| Does the system ensure secure separation of customer processing environments? [SC-2, SC-3] |  |  |  |
| 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)] |  |  |  |

* + 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** |
| --- | --- | --- | --- |
| 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)]  |  |  |  |
| 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] |  |  |  |
| 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), SI-7, SI-7 (7)] |  |  |  |
| Does the CSP have an Incident Response Plan, and is it tested at least annually? [IR-3, IR-8] |  |  |  Describe how the plan is tested. |
| Does the CSP have the capability to perform code analysis scans for code written in-house (non-COTS products)? [SA-11 (1), SA-11 (8)] |  |  |  |
| Does the CSP implement automated mechanisms for incident handling and reporting? [IR-4 (1), IR-6 (1)] |  |  |  |
| 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-7, AU-7 (1), AU-11] |  |  |  |
| 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*] |  |  |  |

* + 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** |
| --- | --- | --- | --- |
| 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] |  |  |  |
| Does the CSP have a Contingency Plan, and is a functional test completed at least annually (for Moderate systems) in accordance with NIST Special Publication 800-34? [CP-2, CP-8] |  |  |  |
| Does the system have alternate storage and processing facilities? [CP-6, CP-7] |  |  |  |
| Does the system have or use alternate telecommunications providers? [CP-8, CP-8 (2)] |  |  |  |
| Does the system have backup power generation or other redundancy? [PE-11] |  |  |  |
| 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** |
| --- | --- | --- | --- |
| Does the CSP maintain a current, complete, and accurate baseline configuration of the information system? [CM-2] |  |  |  |
| Does the CSP maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8] |  |  |  |
| Does the CSP have a Configuration Management Plan? [CM-9, CM-11] |  |  |  |
| Does the CSP follow a formal change control process that includes a security impact assessment? [CM-3, CM-4] |  |  |  |
| Does the CSP employ automated mechanisms to detect inventory and configuration changes? [CM-2(2), CM-6(1), CM-8(3)] |  |  |  |
| Does the CSP prevent unauthorized changes to the system? [CM-5, CM-5(1), CM-5(5)] |  |  |  |
| 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.” |
| 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] |  |  |  |
| Does the CSP perform authenticated operating system/ infrastructure, web, and database vulnerability scans at least monthly, as applicable? [RA-5] |  |  |  |
| Does the CSP adhere to a risk management program which is incorporated system-wide and can support the timely remediation of vulnerabilities? [RA-5, *FedRAMP Continuous Monitoring Guide*] |  |  |  |

* + 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** |
| --- | --- | --- | --- |
| Does the CSP restrict physical system access to only authorized personnel? [PE-2 through PE-6, PE-8] |  |  |  |
| Does the CSP monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8] |  |  |  |
| Does the CSP monitor and respond to physical intrusion alarms and surveillance equipment [PE-6 (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.

For any family with a policy or procedure gap, please describe the gap in Table 4-10 below.

Table 4-9. Policies and Procedures

| **Family** | **Policy** | **Procedure** | **Title Version and Date**  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Yes** | **No** |
| Access Control [AC-1] |  |  |  |  | Policy: Procedure(s):  |
| Awareness & Training [AT-1] |  |  |  |  | Policy: Procedure(s):  |
| Audit & Accountability [AU-1] |  |  |  |  | Policy: Procedure(s):  |
| Security Assessment & Authorization [CA-1] |  |  |  |  | Policy: Procedure(s):  |
| Configuration Management [CM-1] |  |  |  |  | Policy: Procedure(s):  |
| Contingency Planning [CP-1] |  |  |  |  | Policy: Procedure(s):  |
| Identification & Authentication [IA-1] |  |  |  |  | Policy: Procedure(s):  |
| Incident Response [IR-1] |  |  |  |  | Policy: Procedure(s):  |
| Maintenance [MA-1] |  |  |  |  | Policy: Procedure(s):  |
| Media Protection [MP-1] |  |  |  |  | Policy: Procedure(s):  |
| Physical & Environment Protection [PE-1] |  |  |  |  | Policy: Procedure(s):  |
| Personnel Security [PS-1] |  |  |  |  | Policy: Procedure(s):  |
| Risk Assessment [RA-1] |  |  |  |  | Policy: Procedure(s):  |
| System & Services Acquisition [SA-1] |  |  |  |  | Policy: Procedure(s):  |
| System & Communications Protection [SC-1] |  |  |  |  | Policy: Procedure(s):  |
| System & Information Integrity [SI-1] |  |  |  |  | Policy: Procedure(s):  |
| 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** |
|  |

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 full-time dedicated, 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 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.** |
| --- | --- | --- | --- |
| Does the CSP’s change management capability include a fully functioning Change Control Board (CCB)? |  |  |  |
| Does the CSP have and use development and or test environments to verify changes before implementing them into the production environment? |  |  |  |

* + 1. Vendor Dependencies and Teaming Agreements

The 3PAO must answer the questions below.

Table 4-14. Vendor Dependencies and Teaming Agreements

| **Question** | **Yes** | **No** | Instructions |
| --- | --- | --- | --- |
| Does the system have any dependencies on other vendors, such as for hypervisor and operating system patches? |  |  | If “yes,” please complete Table 4-15. Vendor Dependencies below. |
| Within the system, 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? |  |  | If “yes,” please complete Table 4-16. 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 4-15. Vendor Dependency Details

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

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

Table 4-16. Teaming Agreements Details

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

* + 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** |
| --- | --- | --- | --- |
| Does the CSP have a lifecycle management plan that ensures products are updated before they reach the end of their vendor support period? |  |  |  |
| Does the CSP have the ability to scan all hosts in the inventory? |  |  |  |
| Does the CSP have the ability to provide scan files in a structure data format, such as CSV, XML or .nessus files? |  |  |  |
| 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 no details are entered, please sate, “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** |
|  |