

template

StateRAMP Readiness Assessment Report

(RAR)

Service Provider Name

Information System Name

**Version:**

X.X

**Date:**

YYYYMMDD

TABLE OF CONTENTS

[1. Third PArty Assessor Attestation 3](#_Toc69906165)

[2. Readiness Assessment Activities 4](#_Toc69906166)

[3. Executive Summary 4](#_Toc69906167)

[4. About The Document 7](#_Toc69906168)

[4.1 Purpose 7](#_Toc69906169)

[4.2 Outcomes 7](#_Toc69906170)

[4.3 StateRAMP Approach and Use of This Document 7](#_Toc69906171)

[5. General Guidance and Instructions 7](#_Toc69906172)

[5.1 Embedded Document Guidance 7](#_Toc69906173)

[5.2 Additional Instructions to 3PAOs 8](#_Toc69906174)

[6. Assessment Information 9](#_Toc69906175)

[6.1 System Information 9](#_Toc69906176)

[6.2 Authorization Boundary 9](#_Toc69906177)

[6.3 Leveraged StateRAMP Authorizations 10](#_Toc69906178)

[6.4 External Systems and Services 11](#_Toc69906179)

[6.5 APIs 13](#_Toc69906180)

[6.6 Data Flow Diagrams 13](#_Toc69906181)

[6.7 Separation Measures [AC-4, SC-7] 14](#_Toc69906182)

[6.8 StateRAMP Mandates 15](#_Toc69906183)

[6.9 StateRAMP Requirements 17](#_Toc69906184)

[6.9.1 Cryptographic Modules [SC-13] 17](#_Toc69906185)

[6.9.2 Transport Layer Security [NIST SP 800-52, Revision 1] 17](#_Toc69906186)

[6.9.3 Identification, Authentication, and Access Control 18](#_Toc69906187)

[6.9.4 Audit, Alerting, Malware, and Incident Response 19](#_Toc69906188)

[6.9.5 Contingency Planning and Disaster Recovery 20](#_Toc69906189)

[6.9.6 Configuration and Risk Management 21](#_Toc69906190)

[6.9.7 Data Center Security 22](#_Toc69906191)

[6.9.8 Policies, Procedures, and Training 23](#_Toc69906192)

[6.10 Additional Capability Information 25](#_Toc69906193)

[6.10.1 Staffing Levels 25](#_Toc69906194)

[6.10.2 Change Management Maturity 25](#_Toc69906195)

[6.10.3 Vendor Dependencies and Agreements 26](#_Toc69906196)

[6.10.4 Continuous Monitoring (ConMon) Capabilities 27](#_Toc69906197)

[6.10.5 Status of System Security Plan (SSP) 27](#_Toc69906198)

List of Tables

[Table 3‑1. System Information viii](#_Toc69194944)

[Table 3‑2. Leveraged StateRAMP Authorizations x](#_Toc69194945)

[Table 3‑3. External Systems and Services i](#_Toc69194946)

[Table 3‑4. APIs 1](#_Toc69194947)

[Table 4‑2. Cryptographic Modules 5](#_Toc69194948)

[Table 4‑3. Transport Layer Security 5](#_Toc69194949)

[Table 4‑4. Identification, Authentication, and Access Control 6](#_Toc69194950)

[Table 4‑5. Audit, Alerting, Malware, and Incident Response 7](#_Toc69194951)

[Table 4‑6. Contingency Planning and Disaster Recovery 8](#_Toc69194952)

[Table 4‑7. Configuration and Risk Management 9](#_Toc69194953)

[Table 4‑8. Data Center Security 11](#_Toc69194954)

[Table 4‑9. Policies, Procedures & Documentation 11](#_Toc69194955)

[Table 4‑10. Missing Policy and Procedure Elements 13](#_Toc69194956)

[Table 4‑11. Security Awareness Training 13](#_Toc69194957)

[Table 4‑12. Staffing Levels 14](#_Toc69194958)

[Table 4‑13. Change Management 14](#_Toc69194959)

[Table 4‑14. Vendor Dependencies and Agreements 15](#_Toc69194960)

[Table 4‑15. Vendor Dependency Details 15](#_Toc69194961)

[Table 4‑16. Formal Agreements Details 15](#_Toc69194962)

[Table 4‑17. Continuous Monitoring Capabilities 16](#_Toc69194963)

[Table 4‑18. Continuous Monitoring Capabilities– Additional Details 16](#_Toc69194964)

[Table 4‑19. Maturity of the System Security Plan 16](#_Toc69194965)

[Table 4‑20. Controls Designated “Not Applicable” 17](#_Toc69194966)

[Table 4‑21. Controls with an Alternative Implementation 17](#_Toc69194967)

# Third Party Assessor Attestation

[3PAO name] attests to the accuracy of the information provided in this StateRAMP Readiness Assessment Report (RAR) and the [service provider name and system name] readiness to meet the StateRAMP requirements as described in this RAR. [3PAO name] recommends that the StateRAMP PMO grant [service provider system name] StateRAMP Ready status, based on the service provider’s security capabilities as of [assessment completion date].

This attestation is based on [3PAO name] 3PAO Accreditation by the American Association of Laboratory Accreditation (A2LA) and StateRAMP, experience and knowledge of the StateRAMP requirements, and knowledge of industry cybersecurity best practices.

The StateRAMP RAR was created in alignment with StateRAMP requirements and guidance. While this report only contains summary information regarding a service provider’s ability to meet the StateRAMP requirements, it is based on [3PAO name] active validation of [service provider’s name and system name] security capabilities through observations, evidence reviews, personnel interviews, and demonstrated capabilities of security implementations. This StateRAMP Readiness Assessment Report (RAR) is valid for one calendar year after designation from the StateRAMP PMO.

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, 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 SP’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 StateRAMP, including notable strengths and other areas for consideration.At a minimum, the 3PAOs must describe the following:* Overall alignment with the National Institute of Standards 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;
* Risks associated with interconnections used to transmit federal data/metadata or sensitive system data/metadata;
* Risks associated with the use of external systems and services that are not StateRAMP authorized;
* 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.
 |

# About The Document

## Purpose

This report and its underlying assessment are intended to enable StateRAMP to reach a StateRAMP-Ready decision for a specific service provider’s system, based on organizational processes and the security capabilities of the information system. StateRAMP grants a StateRAMP Ready designation when the information in this report indicates the service provider is likely to achieve a StateRAMP Authorization for the system.

## Outcomes

A 3PAO should only submit this report to StateRAMP if it determines the service provider’s system is fully ready to pursue, and likely to achieve, a StateRAMP Authorization. Submission of this report by the 3PAO does not guarantee a StateRAMP-Ready designation, nor does it guarantee a StateRAMP Authorization. The StateRAMP PMO will make a determination, based on the RAR, if the service provider is suitable for a StateRAMP Ready designation.

## StateRAMP Approach and Use of This Document

The RAR identifies clear and objective security capability requirements, where possible, while also allowing for the presentation of subjective information. The clear and objective requirements enable the 3PAO to concisely identify whether a service provider is achieving the most important StateRAMP Moderate baseline requirements. The combination of objective requirements and subjective information enables StateRAMP to render a readiness decision based on a more complete understanding of the service provider’s security capabilities. Section 4, Capability Readiness, is organized into three sections:

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

# General Guidance and Instructions

## Embedded Document Guidance

This document contains embedded text intended to instruct the 3PAO on how to complete each section. These instructions ensure StateRAMP receives all the information necessary to render a StateRAMP Ready decision.

The instructional text is in blue and should be removed after the report is fully developed, and before it is submitted to StateRAMP.

## Additional Instructions to 3PAOs

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

1. Do NOT submit the completed Moderate RAR without first coordinating with the StateRAMP PMO via pmo@StateRAMP.org.
2. On the Title Page, enter the service provider 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.
3. The RAR must provide:
	1. An overview of the system;
	2. A subjective summary of the service provider’s overall readiness, including rationale such as notable strengths and other areas for consideration;
	3. An assessment of the service provider’s ability to meet the StateRAMP Mandates identified in Section 4.1, the StateRAMP Requirements identified in Section 4.2, and Additional Capabilities identified in Section 4.3;
	4. A clear description and diagram of system components and services within the authorization boundary, as well as any interconnections to external systems and services that are outside of the authorization boundary;
	5. A clear Data Flow diagram(s) and description(s) that accounts for all federal information, data, and metadata that flows through the authorization boundary and to/from external systems and services; and
	6. The 3PAO’s attestation regarding the service provider’s readiness to meet StateRAMP Moderate baseline requirements.
4. StateRAMP will not consider a service provider for a StateRAMP Ready designation unless all the requirements in Section 4.1, Federal Mandates, are met. Please note: Meeting these requirements does not guarantee a StateRAMP 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 the service provider’s diagrams but must validate the diagrams as though the 3PAO created them.
6. 3PAOs must **not** conduct this Readiness Assessment exclusively by reviewing a service provider’s written documentation and performing interviews. **Active validation of all information provided within this report is required**.
7. 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 service provider 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.
8. Control references are provided with each of the questions in Section 4.2*,* StateRAMP Requirements. These references are provided to help the 3PAO understand the basis for each question; however, the 3PAO is expected to consider all relevant StateRAMP security controls and capabilities when assessing the service provider’s capabilities.
9. StateRAMP 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.

# Assessment Information

## System Information

Instruction: Provide and validate the information below. For example, if the deployment model is Government only, ensure there are no non-Government customers.

Table 3‑1. System Information

|  |
| --- |
| SP Name:System Name:Service Model: (IaaS, PaaS, SaaS)Data Classification Level: (Category 1,2,3)Fully Operational as of: Enter the date the system became fully operationalNumber of Customers (US Federal/Others): Enter # of US Government customers / # of other customersDeployment Model: Public Cloud, Government-Only CloudSystem Functionality: Briefly describe the functionality of the system and service being provided |

## Authorization Boundary

|  |
| --- |
| **IMPORTANT:** Ensuring authorization boundary accuracy in the RAR is critical to StateRAMP authorization activities. Inaccuracies within the RAR may give authorizing officials and StateRAMP grounds for removing a service provider from assessment and authorization activities. |

An authorization boundary provides a diagrammatic illustration of a service provider’s internal services, components, and other devices, along with connections to external services and systems. An authorization boundary accounts for all federal information, data, and metadata that flow through a service provider.

The 3PAO must perform full authorization boundary validation for the RAR, ensure nothing is missing from the provider-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.

|  |
| --- |
| Instruction: Insert 3PAO-validated network and architecture diagram(s) and provide a written description of the Authorization Boundary. The 3PAO must ensure the diagram:* Includes a clearly defined authorization boundary that accounts for the flow of all federal information, data, and metadata through the system;
* Clearly defines services wholly within the boundary;
* identifies all interconnections to external systems and services (including corporate shared services);
* Depicts all major physical components or groups within the boundary;
* Depicts all major software/virtual components (or groups of) within the boundary; and
* Is validated against the inventory.

**NOTE:** The diagram must include a predominant border drawn around all system components and services included in the authorization boundary. The diagram must be easy to read and understand. If necessary, adjust the page orientation to landscape and/or use multiple diagrams to provide the best representation of the authorization boundary. |

## Leveraged StateRAMP Authorizations

|  |
| --- |
| If this Moderate system leverages another StateRAMP Authorized SP (for example, an IaaS that provides compute, network, and storage; or a SaaS that provides operational support services), provide the relevant details in Table 3-2 below. Please note:* The service provider must be listed on the StateRAMP Authorized Vendor List (AVL) with a Status of “Authorized”;
* 3PAOs must validate that all sub-services listed in Table 3-2 are included in the leveraged service provider’s authorization boundary. (Refer to the service provider’s Service Description on the StateRAMP AVL.) Services that are not included in a StateRAMP-authorized boundary must be listed in Table 3-3; and
* If the system is leveraging external services from a StateRAMP authorized system, the interfaces to the services must be included in the boundary and must also be assessed by the 3PAO.
 |

|  |
| --- |
| **IMPORTANT:** If there is a leveraged service provider, be sure to note every capability in Section 4 that partially or fully leverages the service provider. When doing so, indicate the capability is fully inherited or describe both the inherited and non-inherited aspects of the capability. |

Table 3‑2. Leveraged StateRAMP Authorizations

| # | SP and SP Name | SP Service | StateRAMP Package ID |
| --- | --- | --- | --- |
| 1 | Provide the names of the leveraged Cloud Service Provider and Cloud Service Offering (i.e., system name) | Describe the capabilities and services provided by the service provider (e.g., storage, networking, database, vulnerability scanning, SIEM). | Provide the service provider’s StateRAMP Package ID.  |
| 2 |  |  |  |
| 3 |  |  |  |

## External Systems and Services

Service providers often establish interconnections to external systems and services to (i) exchange data and information or (ii) augment system functionality and operational support services.

3PAOs must identify all interconnections to external systems and services in Table 3-3. 3PAOs should not rely solely on boundary diagrams or interviews provided by the service provider, but should use a combination of methods, such as analyzing data flows and ingress/egress rules, reviewing all open ports and service accounts, and examining solutions used to manage and operate the system. Interconnections to all external systems and services should also be depicted on the authorization boundary diagram in Section 4.1.

**NOTE:** StateRAMP defines an **interconnection** as any communication path used to push, pull, or exchange data and/or information, including Application Programming Interfaces (APIs). For example, the collection of traffic information via the Microsoft Bing Maps API set or integration with the DocuSign service via the DocuSign Enterprise API set are both considered interconnections. 3PAOs must identify all API sets in Section 3.4, Table 3-4.

Table 3‑3. External Systems and Services

| # | System/Service Name | Interconnection Details | Data Types | Data Categorization | Authorized Users & Authentication Method | Compliance Programs |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Provide the name of the system or service. Include the vendor’s name if different from the system or service name. | Provide connectivity details. | List the service provider data types transmitted to, stored, or processed by the system/service, including federal data/metadata and system data/metadata. | Identify the security impact level of the data (Low, Moderate, High) in accordance with FIPS 199.  | List the user roles (for example, SecOps Engineers) authorized to access the service, and provide the authentication method. | List any certifications for this service (for example, PCI SOC 2, CSA STAR Level 2), and provide the certification date. |
|  | **Description:** Describe the purpose of the external system/service and the hosting environment (for example, corporate network, IaaS, or self-hosted).**Risk/Impact/Mitigation:** Describe potential risks introduced by the external system/service and impact to the service provider or federal customer data if the confidentiality, integrity, or availability (CIA) of the system/service were compromised. Please note: 3PAOs should carefully consider impact levels associated with metadata and the risk to the SP or customer data if CIA of the metadata were compromised. Describe any mitigations or compensating controls in place to reduce risk.**Agreements:** Indicate whether an Interconnection Security Agreement (ISA), Service Level Agreement (SLA), or other contractual agreement exists for this system/service. |
| 2 | Service Name | Interconnection Details | Data Types | Data Categorization | Authorized Users & Authentication Method | Compliance Programs |
|  | Description:Risk/Impact/Mitigation:Agreements: |
| 3 | Service Name | Interconnection Details | Data Types | Data Categorization | Authorized Users & Authentication Method | Compliance Programs |
|  | Description:Risk/Impact/Mitigation:Agreements: |

## APIs

Service providers often leverage public or custom APIs to push, pull, or exchange data and information with external resources. Service providers may use publicly available API sets provided by vendors such as Amazon, Microsoft, and Google, or may develop custom APIs.

Examples of public API sets are provided in Table 3-4 and the URL below. 3PAOs must identify all public or custom service provider-leveraged API sets that allow data to flow to and from the system. Remove the examples and use the blank rows in Table 3-4 to enter the API sets. Add new rows as needed. <https://www.programmableweb.com/apis/directory>

Table ‑. APIs

| API/CLI | Protocol | Description |
| --- | --- | --- |
| Microsoft Bing Maps API | TCP/NNN | Build maps that can include routes and traffic info |
| Google App Engine API | TCP/NN | Run web apps on Google infrastructure |
| DocuSign Enterprise API | TCP/NN | Allows an application to connect DocuSign service or embed parts of DocuSign user experience |
| NX-OS CLI | TCP/NN | Main commands for building and designing a datacenter Layer 2 and Layer 3 infrastructure with Cisco Nexus® products |
| VMware CIM API | TCP/NNN | CIM API provides a Common Information Model (CIM) interface for building management applications |
|  |  |  |
|  |  |  |
|  |  |  |

## 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 into and out of the system boundary, including data transmitted to/from all external systems and services;
* Clearly identify data flows for privileged, non-privileged, and customer access; and
* Depict how **all ports, protocols, and services** of all inbound and outbound traffic are represented and managed.

**NOTE:** The data flow diagram must be easy to read and understand. If necessary, adjust the page orientation to landscape and/or use multiple diagrams to provide the best representation of the data flows. |

## Separation Measures [AC-4, 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 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.

## StateRAMP Mandates

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

| # | StateRAMP Ready Minimum Mandates | Compliant? |
| --- | --- | --- |
| Yes | No | N/A |
| 1 | Are modern cryptographic modules consistently used where cryptography is required?Data at Rest [SC-28]Transmission [SC-8 (1), SC-12, SC-12(2, 3)]Remote Access [AC-17 (2)]Authentication [IA-5 (1)]Digital Signatures/Hash [CM-5 (3)]AES-256AES-128TLS 1.1 (Compliant)TLS 1.2 (Compliant) |  |  |  |
| 2 | Can the system support Single Sign On (SSO/SAML)? [IA-08] |  |  |  |
| 3 | Does the CSP scan for and consistently remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days, and Low vulnerabilities within 180 days? [RA-5]Required: Credentialed scan shall be used on all devices and validated that credentials work properly. |  |  |  |
| 4 | Do you scan for configuration settings on systems in the environment? [CM-6] |  |  |  |
| 5 | Does the CSP and system utilize and audit and event monitoring solution (SIEM) that can support 90 days of online storage and 365 days of event/log data? [AU-2, AU-3, AU-8, AU-11]SIEM is preferred, but some form of log aggregation is required |  |  |  |
| 6 | Does the system’s external DNS solution support DNS Security (DNSSEC) to provide origin authentication and integrity verification assurances? [SC-20, SC-21] |  |  |  |
| 7 | Does the system ensure secure separation of customer data? [SC-4] |  |  |  |
| 8 | 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)]  |  |  |  |
| 9 | Does the system protect audit information from unauthorized access, modification, and deletion? [AU-7, AU-9] |  |  |  |
| 10 | 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] |  |  |  |
| 11 | Does the CSP maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8] |  |  |  |
| 12 | Does the CSP follow a formal change control process that includes a security impact assessment? [CM-3, CM-4]Expectation: Automated Include examples of acceptable criteria – SharePoint, excel |  |  |  |
| 13 | Does the CSP employ automated mechanisms to detect inventory and configuration changes? [CM-2(2), CM-6(1), CM-8(3)] |  |  |  |
| 14 | Does the CSP prevent unauthorized changes to the system? [CM-5, CM-5(1), CM-5(5)] |  |  |  |
| 15 | Does the system require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2(1), IA-2(3)] |  |  |  |
| 16 | Does the CSP have an Incident Response Plan and Incident Response Testing Plan [IR-3] [IR-8] (SR Template) |  |  |  |
| 17 | Does the CSP have a Configuration Management Plan? [CM-9, CM-11] |  |  |  |
| 18 | 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] |  |  |  |
| 19 | Do you conduct code analysis for internally-developed code? [SA-11] |  |  |  |
| 20 | Does the CSP restrict physical system access to only authorized personnel? [PE-2 through PE-6, PE-8] |  |  |  |
| 21 | Does the CSP monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8] |  |  |  |
| 22 | Does the CSP monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6 (1)] |  |  |  |
| 23 | Does the system have or use alternate telecommunications providers? [CP-8, CP-8 (2)]If on SR/FR IaaS (N/A), if in non-authorized IaaS, they will have to gather this info from the IaaS |  |  |  |
| 24 | Does the system have backup power generation or other redundancy? [PE-11] |  |  |  |
| 25 | Does the CSP have service level agreements (SLAs) in place with all telecommunications providers? [CP-8 (1)] |  |  |  |

## StateRAMP Requirements

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

### Cryptographic Modules [SC-13]

Table 4‑2. Cryptographic Modules

| # | Cryptographic Module Type | Modern Encryption | Describe encryption type | Describe Missing Elements or N/A Justification |
| --- | --- | --- | --- | --- |
| Yes | No |
| 1 | Data at Rest [SC-28] |  |  |  |  |
| 2 | Transmission [SC-8 (1), SC-12, SC-12(2, 3)] |  |  |  |  |
| 3 | Remote Access [AC-17 (2)] |  |  |  |  |
| 4 | Authentication [IA-5 (1)] |  |  |  |  |
| 5 | Digital Signatures/Hash [CM-5 (3)] |  |  |  |  |

### 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) |  |  |  |

### Identification, Authentication, 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, Authentication, and Access Control

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
| --- | --- | --- | --- | --- |
| 1 | Does the system support Single Sign on/SAML [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)] |  |  |  |
| 5 | Does the system restrict non-authorized personnel’s access to resources? [AC-6(2)] |  |  |  |
| 6 | Does the system restrict non-privileged users from performing privileged function? [AC-6(10)] |  |  |  |
| 7 | Does the system ensure secure separation of customer data? [SC-4] |  |  | The capability description is not required here, but must be included in Section 3.7, Separation Measures. |
| 8 | Does the system ensure secure separation of customer processing environments? [SC-2, SC-3] |  |  | The capability description is not required here, but must be included in Section 3.7, Separation Measures. |
| 9 | 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)] |  |  |  |

### 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 protect audit information from unauthorized access, modification, and deletion? [AU-7, AU-9] |  |  |  |
| 3 | Does the SP 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)] |  |  |  |
| 4 | Does the SP have an Incident Response Plan and a fully developed Incident Response test plan? [IR-3, IR-8] |  |  |  |
| 5 | Does the SP 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 Y or N. Instead, state “NO CUSTOM CODE” here. |
| 6 | Does the SP implement automated mechanisms for incident handling and reporting? [IR-4 (1), IR-6 (1)] |  |  |  |
| 7 | Does the SP 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] |  |  |  |
| 8 | Does the SP have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations? [*StateRAMP Incident Communications Procedure*] |  |  |  |

### 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 service provider 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 service provider 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 or use alternate telecommunications providers? [CP-8, CP-8 (2)] |  |  |  |
| 5 | Does the system have backup power generation or other redundancy? [PE-11] |  |  |  |
| 6 | Does the service provider have service level agreements (SLAs) in place with all telecommunications providers? [CP-8 (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 service provider maintain a current, complete, and accurate baseline configuration of the information system? [CM-2] |  |  |  |
| 2 | Does the service provider maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8] |  |  |  |
| 3 | Does the service provider have a Configuration Management Plan? [CM-9, CM-11] |  |  |  |
| 4 | Does the service provider follow a formal change control process that includes a security impact assessment? [CM-3, CM-4] |  |  |  |
| 5 | Does the service provider employ automated mechanisms to detect inventory and configuration changes? [CM-2(2), CM-6(1), CM-8(3)] |  |  |  |
| 6 | Does the service provider prevent unauthorized changes to the system? [CM-5, CM-5(1), CM-5(5)] |  |  |  |
| 7 | Does the service provider establish configuration settings for products employed that reflect the most restrictive mode consistent with operational requirements? [CM-6] |  |  | If “yes,” describe whether 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.” |
| 8 | Does the service provider 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 9 | Does the service provider perform authenticated operating system/ infrastructure, web, and database vulnerability scans at least monthly, as applicable? [RA-5, RA-5(5)] |  |  | Describe how the 3PAO validated that vulnerability scans were fully authenticated. |
| 10 | Does the service provider demonstrate the capability to remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days and Low vulnerabilities within 180 days? [RA-5, *StateRAMP Continuous Monitoring Guide*] |  |  | Describe how the 3PAO validated that the service provider remediates High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days. |
| 11 | When a High vulnerability is identified as part of ConMon activities, does the service provider consistently check audit logs for evidence of exploitation? [RA-5(8)] |  |  |  |

### 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 service provider restrict physical system access to only authorized personnel? [PE-2 through PE-6, PE-8] |  |  |  |
| 2 | Does the service provider monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8] |  |  |  |
| 3 | Does the service provider monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6 (1)] |  |  |  |

### Policies, Procedures, and Training

The 3PAO must indicate the status of policy and procedure coverage for the NIST 800-53, Rev 4, control 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 “dash one” controls 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.

SPs 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, Procedures, and Documentation

To achieve Ready Status, a service provider must have the required Ready Documentation.

| # | StateRAMP Required Ready Documentation | Completed? |
| --- | --- | --- |
| Yes | No | N/A |
| 1 | Boundary Diagram |  |  |  |
| 2 | StateRAMP Inventory Worksheet |  |  |  |
| 3 | Roles & Permissions Matrix |  |  |  |

To achieve Ready Status, a service provider must complete, at minimum, 50% or 21 of the StateRAMP Documents.

| # | StateRAMP Documentation (Minimum of 50% Documents Must be Completed for Ready) | Compliant? |
| --- | --- | --- |
| Yes | No | N/A |
| 1 | System Security Plan (SSP) & Operational Controls Matrix |  |  |  |
| 2 | Incident Response Plan |  |  |  |
| 3 | Information System Contingency Plan |  |  |  |
| 4 | Configuration Management Plan |  |  |  |
| 5 | Rules of Behavior |  |  |  |
| 6 | Control Implementation Summary |  |  |  |
| 7 | Continuous Monitoring Plan |  |  |  |
| 8 | Security Policy – Access Control (AC) |  |  |  |
| 9 | Security Policy – Awareness & Training (AT) |  |  |  |
| 10 | Security Policy – Audit & Accountability (AU) |  |  |  |
| 11 | Security Policy – Security Assessment & Authorization (CA) |  |  |  |
| 12 | Security Policy – Configuration Management (CM) |  |  |  |
| 13 | Security Policy – Contingency Planning (CP) |  |  |  |
| 14 | Security Policy – Identification & Authentication (IA) |  |  |  |
| 15 | Security Policy – Incident Response (IR) |  |  |  |
| 16 | Security Policy – Maintenance (MA) |  |  |  |
| 17 | Security Policy – Media Protection (MP) |  |  |  |
| 18 | Security Policy – Personnel Security (PS) |  |  |  |
| 19 | Security Policy – Physical & Environmental (PE) |  |  |  |
| 20 | Security Policy – Planning (PL) |  |  |  |
| 21 | Security Policy – Risk Assessment (RA) |  |  |  |
| 22 | Security Policy – Systems & Services Acquisition (SA) |  |  |  |
| 23 | Security Policy – Systems & Communications Protection (SC) |  |  |  |
| 24 | Security Policy – Systems & Information Integrity (SI) |  |  |  |
| 25 | Security Procedure – Access Control (AC) |  |  |  |
| 26 | Security Procedure – Awareness & Training (AT) |  |  |  |
| 27 | Security Procedure – Audit & Accountability (AU) |  |  |  |
| 28 | Security Procedure – Security Assessment & Authorization (CA) |  |  |  |
| 29 | Security Procedure – Configuration Management (CM) |  |  |  |
| 30 | Security Procedure – Contingency Planning (CP) |  |  |  |
| 31 | Security Procedure – Identification & Authentication (IA) |  |  |  |
| 32 | Security Procedure – Incident Response (IR) |  |  |  |
| 33 | Security Procedure – Maintenance (MA) |  |  |  |
| 34 | Security Procedure – Media Protection (MP) |  |  |  |
| 35 | Security Procedure – Personnel Security (PS) |  |  |  |
| 36 | Security Procedure – Physical & Environmental (PE) |  |  |  |
| 37 | Security Procedure – Planning (PL) |  |  |  |
| 38 | Security Procedure – Risk Assessment (RA) |  |  |  |
| 39 | Security Procedure – Systems & Services Acquisition (SA) |  |  |  |
| 40 | Security Procedure – Systems & Communications Protection (SC) |  |  |  |
| 41 | Security Procedure – Systems & Information Integrity (SI) |  |  |  |

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 service provider train personnel on security awareness and role-based security responsibilities? |  |  |  |

## Additional Capability Information

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

### Staffing Levels

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

It should be noted in the organizational structure who has the authority to perform activities on the system and how these differ between staff or teams of staff (e.g., who has authority to apply patches; who has authority over configuration management; who has authority over making changes to the environment; who is in charge of compliance reporting).

Table 4‑12. Staffing Levels

| Staffing Levels |
| --- |
|  |

### Change Management Maturity

While the following change management capabilities are not required, they indicate a more mature change management capability and may influence a StateRAMP 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 function is accomplished. |
| --- | --- | --- | --- | --- |
| 1 | Does the service provider’s change management capability include a fully functioning Change Control Board (CCB)? |  |  |  |
| 2 | Does the service provider have and use development and/or test environments to verify changes before implementing them in the production environment? |  |  |  |

### 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 service provider 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 service provider’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 |  |  |

### Continuous Monitoring (ConMon) Capabilities

In the tables below, please describe the current state of the service provider’s ConMon capabilities, as well as the length of time the service provider 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 service provider have a lifecycle management plan that ensures products are updated before they reach the end of their vendor support period? |  |  |  |
| 2 | Does the service provider have the ability to scan all hosts in the inventory? |  |  |  |
| 3 | Does the service provider have the ability to provide scan files in a structured data format, such as CSV, XML, or .nessus files? |  |  |  |
| 4 | Is the service provider properly maintaining their Plan of Actions and Milestones (POA&M), including timely, accurate, and complete information entries for past due 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 StateRAMP’s understanding of the service provider’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 |
|  |

### 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 service provider has not yet developed. If the maturity of the SSP is low, or there is a high percentage that is not complete, please describe any risks the 3PAO believes this introduces to a full assessment.

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 |
|  |