StateRAMP

STATERAMP READY MINIMUM MANDATORY REQUIREMENTS FOR MODERATE AND HIGH IMPACT LEVELS

VERSION:

2.0

DATE:

April 29, 2022

DOCUMENT REVISION HISTORY

Date	Description	Version	Governance Body
12/17/2020	Original Publication	1.0	StateRAMP Steering Committee
08/11/2021	Added User Guide and SOD to document list.	1.1	Julia Miller
09/16/2021	Style updates to Minimum Mandates table	1.2	Shea Simpson
4/29/2022	Update Requirements for Ready specific to Moderate and High Impact Levels	2.0	StateRAMP Standards & Technical Committee and

This document will be reviewed at the discretion of the StateRAMP Board a frequency no less than annually.

StateRAMP Status Progression

StateRAMP is designed to allow service providers to progress through five security statuses, including: Active, Ready, In Process, Pending, and Authorized. Additionally, a Provisional status may be assigned by a State if the State determines a provider's Security Package meets most critical controls but not all. To be eligible for Provisional Status, the provider must meet the minimum mandatory requirements below.

Achieving Ready Status

To achieve Ready Status, a service provider must meet the minimum mandatory requirements outlined in this document. The minimum mandates are specific to Low Impact Levels and Moderate/High impact levels.

StateRAMP developed the minimum mandatory requirements for Ready with input from State, CSP, and security experts. It is the goal of StateRAMP to help mature and grow the service provider community and in doing so, improve the security profile for state and local government. StateRAMP will verify that providers meet the intent of the security requirements as appropriate and fit for purpose.

Templates and guidance will be maintained and published on www.stateramp.org.

To achieve Ready Status, a service provider must meet these minimum mandatory requirements.

#	StateRAMP Mandates for Ready – Moderate & High Impact Systems	Compliant?		
		Yes	No	N/A
1	Are modern cryptographic modules consistently used where cryptography is required? **Associated NIST Controls** Remote Access [AC-17 (2)] Digital Signatures/Hash [CM-5 (3)] Authentication [IA-5 (1), IA-7] Transmission [SC-8 (1), SC-12, SC-12(2, 3)] Data at Rest [SC-28] **Minimum Required Encryption Cipher Strength** AES-256 AES-128 **Required Encryption-In-Transit Protocols** TLS 1.2 (Compliant) TLS 1.3 (Compliant)			
2	Does the SP use a vulnerability scanner that is updated prior to performing new scans to scan the system for vulnerabilities? **Associated NIST Control** Vulnerability Scanning [RA-5, RA-5 (1), RA-5 (2)] **Required** Credentialed scans must be used on all devices, and credentials used must be validated to work properly for scanning purposes.			
3	Does the SP consistently remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days, and Low vulnerabilities within 180 days? **Associated NIST Control** Vulnerability Scanning [RA-5]			
4	Does the SP and system utilize an audit and event monitoring solution that can support 90 days of online storage and 365 days of event/log data? **Associated NIST Controls** Event Logging [AU-2]			

#	StateRAMP Mandates for Ready – Moderate & High Impact Systems	Compliant?		
		Yes	No	N/A
	Content of Audit Records [AU-3] Time Stamps [AU-8] Audit Record Retention [AU-11] Audit Record Generation [AU-12] Information System Monitoring [SI-4] **Required** Some form of log aggregation is required. A SIEM is recommended but not required.			
5	Does the system's external DNS solution support DNS Security (DNSSEC) to provide origin authentication and integrity verification assurances? **Associated NIST Controls** Secure Name/Address Resolution Service (Auth. Source) [SC-20] Secure Name/Address Resolution Service (Recursive or Caching Resolver) [SC-21]			
6	Does the system enforce logical access according to established access control policies? **Associated NIST Control** Access Enforcement [AC-3]			
7	Does the system enforce a limit on the number of invalid login attempts within a 15 minute time period? **Associated NIST Control** Unsuccessful Logon Attempts [AC-7]			
8	Does the system require multi-factor authentication (MFA) for administrative accounts and functions? **Associated NIST Controls** Identification and Authentication (Organizational Users) [IA-2] Identification and Authentication | MFA for Privileged Accounts [IA-2(1)] Identification and Authentication | Local Access to Privileged Accounts [IA-2(3)]			
9	Does the system support Single Sign-On (SSO/SAML)? **Associated NIST Controls** Identification and Authentication | Non-Organizational Users [IA-8]			
10	Does the system ensure secure separation of customer data? **Associated NIST Control** Information Flow Enforcement [SC-4]			

#	StateRAMP Mandates for Ready – Moderate & High Impact Systems	Compliant?		
		Yes	No	N/A
11	Does the system have the capability to detect, contain, and eradicate malicious software? **Associated NIST Controls** Maintenance Tools | Inspect Media [MA-3 (2)] Malicious Code Protection [SI-3] Malicious Code Protection | Central Management [SI-3 (1)] Malicious Code Protection | Automatic Updates [SI-3 (2)] Malicious Code Protection | Non-signature Based Detection [SI-3 (7)]			
12	Does the system protect audit information from unauthorized access, modification, and deletion? **Associated NIST Controls** Audit Reduction and Report Generation [AU-7] Protection of Audit Information [AU-9]			
13	Does the SP have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? **Associated NIST Controls** Contingency Plan [CP-2] Contingency Plan | Capacity Planning [CP-2 (2)] Contingency Plan | Resume Mission and Business Functions[CP-2 (3)] System Backup [CP-9] System Recovery and Reconstitution [CP-10]			
14	Does the SP maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? **Associated NIST Control** System Component Inventory [CM-8]			
15	Does the SP follow a formal change control process that includes a security impact assessment? **Associated NIST Controls** Configuration Change Control [CM-3] Impact Analysis [CM-4] **Required** Some form of automation must be used within the change control process.			

#	StateRAMP Mandates for Ready – Moderate & High Impact Systems	Compliant?		
		Yes	No	N/A
16	Does the SP employ automated mechanisms to detect inventory and configuration changes? **Associated NIST Controls** Baseline Configuration | Automation [CM-2(2)] Configuration Settings | Automated Mgmt., Application & Verification [CM-6(1)] System Component Inventory | Automated Unauthorized Component Detection [CM-8(3)]			
17	Does the SP prevent unauthorized changes to the system? **Associated NIST Controls** Access Restriction for Change [CM-5] Access Restriction for Change | Automated Access Enforcement & Audit Records [CM-5(1)] Access Restriction for Change | Privilege Limitation for Production and Operation [CM-5(5)]			
18	Does the SP scan for configuration settings on systems in the environment? **Associated NIST Control** Configuration Settings [CM-6] **Preference** SCAP scans			
19	Does the SP ensure that all non-essential services, functions, and ports are disabled on the information system? **Associated NIST Control** Least Functionality [CM-7]			
20	Does the SP perform regular maintenance on the system that is tracked, approved and tested prior to implementation? **Associated NIST Controls** Controlled Maintenance [MA-2] Flaw Remediation [SI-2]			
21	Does the SP have an Incident Response Plan and does the SP perform incident response testing? **Associated NIST Control** Incident Response Testing [IR-3] Incident Response Plan [IR-8]			

#	StateRAMP Mandates for Ready – Moderate & High Impact Systems	Compliant?		
		Yes	No	N/A
22	Does the SP have a Configuration Management Plan? **Associated NIST Controls** Configuration Management Plan [CM-9] User-Installed Software [CM-11]			
23	Does the SP have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with NIST Special Publication 800-34? **Associated NIST Controls** Contingency Plan [CP-2] Telecommunications Services [CP-8]			
24	Does the SP back up the information system and information system documentation? **Associated NIST Control** Information System Backup [CP-9]			
25	Does the SP conduct code analysis for internally developed code? **Associated NIST Control** Developer Testing and Evaluation [SA-11]			
26	Does the SP restrict physical system access to only authorized personnel? **Associated NIST Controls** Physical Access Authorizations [PE-2] Physical Access Control [PE-3] Access Control for Transmission [PE-4] Access Control for Output Devices [PE-5] Monitoring Physical Access [PE-6] Visitor Access Records [PE-8] **Note** This requirement is N/A if the system leverages a StateRAMP or FedRAMP accredited IaaS, however, this information must be obtained from the leveraged system's service provider.			
27	Does the SP monitor and log physical access to the information system, and maintain access records? **Associated NIST Controls** Monitoring Physical Access [PE-6]			

#	StateRAMP Mandates for Ready – Moderate & High Impact Systems	Compliant?		
		Yes	No	N/A
	Visitor Access Records [PE-8] **Note** This requirement is N/A if the system leverages a StateRAMP or FedRAMP accredited IaaS, however, this information must be obtained from the leveraged system's service provider.			
28	Does the SP monitor and respond to physical intrusion alarms and surveillance equipment? **Associated NIST Control** Monitoring Physical Access | Intrusion Alarms & Surveillance Equipment [PE-6 (1)] **Note** This requirement is N/A if the system leverages a StateRAMP or FedRAMP accredited IaaS, however, this information must be obtained from the leveraged system's service provider.			
29	Does the system have or use alternate telecommunications providers? **Associated NIST Controls** Telecommunication Services [CP-8] Telecommunication Services | Single Point of Failure [CP-8 (2)] **Note** This requirement is N/A if the system leverages a StateRAMP or FedRAMP accredited IaaS, however, this information must be obtained from the leveraged system's service provider.			
30	Does the system have backup power generation or other redundancy? **Associated NIST Controls** Emergency Power [PE-11] **Note** This requirement is N/A if the system leverages a StateRAMP or FedRAMP accredited IaaS, however, this information must be obtained from the leveraged system's service provider.			
31	Does the SP have service level agreements (SLAs) in place with all telecommunications providers? **Associated NIST Control** Telecommunications Services | Priority of Service Provisions [CP-8 (1)]			

#	StateRAMP Mandates for Ready – Moderate & High Impact Systems	Compliant?		
		Yes	No	N/A
	Note This requirement is N/A if the system leverages a StateRAMP or FedRAMP accredited IaaS, however, this information must be obtained from the leveraged system's service provider.			
	Does the SP perform exit interviews with terminated personnel to retrieve any security or authentication-related items and disable the terminated individual's system access the day of termination? **Associated NIST Control** Personnel Termination [PS-4]			

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)			
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	User Guide			
9	Separation of Duties (SOD)			
10	Security Policy – Access Control (AC)			

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

#	StateRAMP Documentation (Minimum of 50% Documents Must be Completed for Ready)	Compliant?		
		Yes	No	N/A
43	Security Procedure – Systems & Information Integrity (SI)			