



STATERAMP READY MINIMUM MANDATORY REQUIREMENTS

VERSION:

1.1

DATE:

October 2021



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

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 the same across all 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 Ready Minimum Mandates	Compliant?		
		Yes	No	N/A
1	<p>Are modern cryptographic modules consistently used where cryptography is required?</p> <p>Associated NIST Controls Remote Access Protection of Confidentiality and Integrity Using Encryption [AC-17 (2)] Access Restrictions for Change Signed Components [CM-5 (3)] Authenticator Management Password-Based Authentication [IA-5 (1)] Transmission Confidentiality and Integrity Cryptographic Protection [SC-8 (1)] Cryptographic Key Establishment and Management [SC-12] Cryptographic Key Establishment and Management Symmetric Keys [SC-12 (2)] Cryptographic Key Establishment and Management Asymmetric Keys [SC-12 (3)] Protection of Information at Rest [SC-28]</p> <p>Minimum Required Encryption Cipher Strength AES-256 AES-128</p> <p>Required Encryption-In-Transit Protocols TLS 1.1 (Compliant) TLS 1.2 (Compliant)</p>			
2	<p>Can the system support Single Sign On (SSO)?</p> <p>Associated NIST Control Identification and Authentication (Non-Organizational Users) [IA-8]</p>			
3	<p>Does the SP scan for and consistently remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days, and Low vulnerabilities within 180 days?</p> <p>Associated NIST Control Vulnerability Scanning [RA-5]</p> <p>Required Credentialed scans must be used on all devices, and the credentials used must be validated to work properly for scanning purposes.</p>			
4	<p>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?</p> <p>Associated NIST Controls</p>			



#	StateRAMP Ready Minimum Mandates	Compliant?		
		Yes	No	N/A
	Event Logging [AU-2] Content of Audit Records [AU-3] Time Stamps [AU-8] Audit Record Retention [AU-11] 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 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)]			
7	Does the system ensure secure separation of customer data? Associated NIST Control Information Flow Enforcement [SC-4]			
8	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)]			
9	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]			



#	StateRAMP Ready Minimum Mandates	Compliant?		
		Yes	No	N/A
10	<p>Does the SP have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster?</p> <p>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]</p>			
11	<p>Does the SP maintain a current, complete, and accurate inventory of the information system software, hardware, and network components?</p> <p>Associated NIST Control System Component Inventory [CM-8]</p>			
12	<p>Does the SP follow a formal change control process that includes a security impact assessment?</p> <p>Associated NIST Controls Configuration Change Control [CM-3] Impact Analysis [CM-4]</p> <p>Required Some form of automation must be used within the change control process.</p>			
13	<p>Does the SP employ automated mechanisms to detect inventory and configuration changes?</p> <p>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)]</p>			
14	<p>Does the SP prevent unauthorized changes to the system?</p> <p>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)]</p>			



#	StateRAMP Ready Minimum Mandates	Compliant?		
		Yes	No	N/A
15	<p>Does the SP scan for configuration settings on systems in the environment?</p> <p>Associated NIST Controls Configuration Settings [CM-6]</p> <p>Preference SCAP scans</p>			
16	<p>Does the SP have an Incident Response Plan?</p> <p>Associated NIST Control Incident Response Testing [IR-3]</p>			
17	<p>Does the SP have a Configuration Management Plan?</p> <p>Associated NIST Controls Configuration Management Plan [CM-9] User-Installed Software [CM-11]</p>			
18	<p>Does the SP have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with NIST Special Publication 800-34?</p> <p>Associated NIST Controls Contingency Plan [CP-2] Telecommunications Services [CP-8]</p>			
19	<p>Does the SP conduct code analysis for internally developed code?</p> <p>Associated NIST Control Developer Testing and Evaluation [SA-11]</p>			
20	<p>Does the SP restrict physical system access to only authorized personnel?</p> <p>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]</p> <p>Note</p>			



#	StateRAMP Ready Minimum Mandates	Compliant?		
		Yes	No	N/A
	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.			
21	<p>Does the SP monitor and log physical access to the information system, and maintain access records?</p> <p>Associated NIST Controls Monitoring Physical Access [PE-6] Visitor Access Records [PE-8]</p> <p>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.</p>			
22	<p>Does the SP monitor and respond to physical intrusion alarms and surveillance equipment?</p> <p>Associated NIST Control Monitoring Physical Access Intrusion Alarms & Surveillance Equipment [PE-6 (1)]</p> <p>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.</p>			
23	<p>Does the system have or use alternate telecommunications providers?</p> <p>Associated NIST Controls Telecommunication Services [CP-8] Telecommunication Services Single Point of Failure [CP-8 (2)]</p> <p>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.</p>			
24	<p>Does the system have backup power generation or other redundancy?</p> <p>Associated NIST Controls Emergency Power [PE-11]</p> <p>Note</p>			



#	StateRAMP Ready Minimum Mandates	Compliant?		
		Yes	No	N/A
	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.			
25	<p>Does the SP have service level agreements (SLAs) in place with all telecommunications providers?</p> <p>Associated NIST Control Telecommunications Services Priority of Service Provisions [CP-8 (1)]</p> <p>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.</p>			



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)			
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)			



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