STATERAMP READY MINIMUM MANDATORY REQUIREMENTS

VERSION:
1.0

DATE:
December 17, 2020

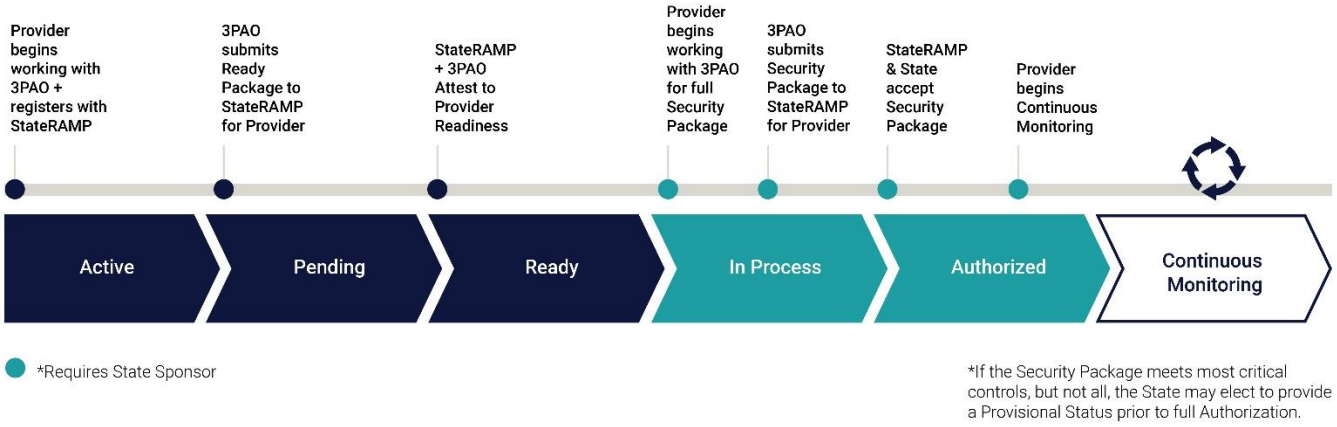
DOCUMENT REVISION HISTORY

Date	Description	Version	Governance Body
12/17/2020	Original Publication	1.0	StateRAMP Steering Committee

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, Pending Ready, Ready, In Process, 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	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-256 AES-128 TLS 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]			

#	StateRAMP Ready Minimum Mandates	Compliant?		
		Yes	No	N/A
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)]			

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	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)			

#	StateRAMP Documentation (Minimum of 50% Documents Must be Completed for Ready)	Compliant?		
		Yes	No	N/A
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)			