

StateRAMP Moderate – Category 3

StateRAMP Moderate Category 3 defines baseline security controls for assessing and authorizing cloud services for U.S. state and local agencies.



What it is

StateRAMP Moderate Category 3 is a cybersecurity risk management framework that assists U.S. state and local government agencies in assessing and validating the security posture of cloud service providers. It establishes baseline requirements for protecting agency data and ensuring reliable cloud services in accordance with public sector standards.

Developed and governed by the StateRAMP organization, the framework mirrors the Federal Risk and Authorization Management Program (FedRAMP) with controls tailored to state and local government needs. StateRAMP Moderate Category 3 is used by state agencies, cloud vendors, and third-party assessors to evaluate and certify security controls, privacy measures, and compliance with regulatory expectations.

At a glance

PUBLISHER GovRAMP (formerly StateRAMP)	TYPE Framework	VERSION 4.0
EFFECTIVE February 2025	DOMAIN Cloud Security	FAMILY FedRAMP
REGION United States	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://govramp.org/document-library>

Why it matters

- **Strengthen cybersecurity oversight** Establishes standardized processes for evaluating and validating security postures across cloud solutions used by state and local agencies.
- **Enhance compliance alignment** Supports regulatory adherence by mapping security controls to state-specific requirements and demonstrating due diligence during audits.
- **Promote operational resilience** Reduces service disruption by enforcing robust risk management, contingency planning, and incident response procedures tailored to public sector needs.
- **Improve audit readiness** Simplifies preparation for independent assessments by requiring documented security measures and annual verification by authorized assessors.

How SmartSuite supports StateRAMP Moderate (Cat 3)

StateRAMP Moderate Control Library

Structure Moderate baseline controls aligned to NIST 800-53 for higher-impact cloud environments.

System Security Plan and Boundary Governance

Maintain SSP documentation, system architecture, and authorization boundaries for Moderate systems.

Control Implementation and Risk Management

Track control deployment, risk assessments, and remediation activities across systems handling sensitive state data.

Vulnerability and Security Monitoring

Monitor vulnerabilities, security events, and ongoing control effectiveness across cloud environments.

Third-Party and Cloud Responsibility Tracking

Track third-party providers, cloud responsibilities, and supporting evidence for compliance.

StateRAMP Authorization Readiness Reporting

Provide dashboards showing control coverage, POA&M status, and readiness for StateRAMP authorization reviews.

Common framework mappings

CIS Controls v8.1

FedRAMP Rev. 5

ISO 27001:2022

ISO 27002:2022

ISO 27017

ISO 27701

NIST CSF 2.0

NIST 800-53 Rev.5

SOC 2

Official resources

StateRAMP Security Assessment Framework

Provides official specifications and requirements for the StateRAMP Moderate Category 3 framework.

govramp.org/document-library

Frequently asked questions

What is StateRAMP Moderate Category 3 used for?

StateRAMP Moderate Category 3 is designed to help U.S. state and local government agencies assess and validate the cybersecurity posture of cloud service providers. It establishes security control requirements to ensure protection of sensitive government data in cloud environments.

Is StateRAMP Moderate Category 3 certification mandatory?

Certification is not universally mandatory, but many state and local agencies require cloud service providers to achieve StateRAMP Moderate authorization before procurement. Organizations seeking to do business with these agencies often must demonstrate compliance through StateRAMP assessment and certification.

Who does StateRAMP Moderate Category 3 apply to?

StateRAMP Moderate Category 3 applies to cloud service providers supporting U.S. state and local government entities that process, store, or transmit government data categorized as Moderate in terms of confidentiality, integrity, or availability. It is relevant for agencies, vendors, and third-party assessors involved in cloud services.

What are the key controls and artifacts required by StateRAMP Moderate Category 3?

Key controls are based on the FedRAMP Moderate baseline, addressing areas such as access control, incident response, risk assessment, and continuous monitoring. Required artifacts typically include a System Security Plan (SSP), risk assessment reports, assessment results, and ongoing continuous monitoring documentation.

How do organizations implement StateRAMP Moderate Category 3?

Organizations implement StateRAMP Moderate Category 3 by conducting gap assessments against prescribed controls, remediating deficiencies, maintaining documentation, and undergoing independent security assessments by authorized third-party assessment organizations. Continued compliance requires periodic reassessment and ongoing monitoring.

How does StateRAMP Moderate Category 3 relate to FedRAMP?

StateRAMP Moderate Category 3 closely mirrors the FedRAMP Moderate baseline but is tailored for state and local government requirements rather than federal agencies. While both frameworks use a similar control catalog and assessment process, StateRAMP addresses unique needs and regulatory drivers specific to the public sector at the state and local level.

What are the ongoing compliance requirements for StateRAMP Moderate Category 3?

Ongoing compliance requires organizations to maintain documentation of controls, conduct regular risk assessments, implement continuous monitoring, and submit periodic security and vulnerability assessment reports. Remediation of identified issues and annual independent audits are essential to sustaining authorization status.

How would SmartSuite support StateRAMP Moderate Category 3?

SmartSuite helps organizations manage StateRAMP Moderate Category 3 compliance by providing risk tracking tools, centralized control management, and automated evidence collection for audit purposes. It enables teams to monitor audit readiness, maintain up-to-date compliance documentation, and generate dashboards for reporting on compliance status and remediation activities.

License included / downloadable: Yes StateRAMP Security Assessment Framework is publicly available for free download from the StateRAMP (govramp.org) website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/stateramp-moderate-category-3