SmartSuite

Framework / Cloud Security / FedRAMP

StateRAMP Low+ – Category 2

StateRAMP Low+ Category 2 defines baseline security controls for cloud services handling low-impact state and local government data.

What it is

StateRAMP Low+ Category 2 is a cybersecurity compliance framework that helps U.S. state and local government vendors implement baseline security controls for cloud services handling low-impact data. The framework establishes requirements to safeguard sensitive information, ensure data protection, and reduce overall cybersecurity risk in public sector cloud environments.

Published and managed by the StateRAMP (State Risk and Authorization Management Program) organization, StateRAMP Low+ Category 2 is based on the NIST SP 800-53 low baseline and includes additional control enhancements. The framework is utilized by cloud service providers and government procurement officials to assess, authorize, and monitor vendor security practices, covering areas such as access control, incident response, vulnerability management, and continuous monitoring.

At a glance

PUBLISHER StateRAMP (operating as GovRAMP)	TYPE Framework	VERSION 1.4
EFFECTIVE April 29, 2022	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 vendor security oversight** Enable consistent evaluation and monitoring of third-party cloud vendors to ensure effective implementation of security controls.
- **Enhance data protection practices** Safeguard sensitive government data in cloud environments by requiring baseline security measures and regular risk assessments.
- **Improve compliance alignment** Support alignment with federal and industry cybersecurity frameworks, reducing compliance gaps and the risk of regulatory violations.
- **Increase audit readiness** Streamline documentation and evidence collection, making it easier to demonstrate security compliance during governmental audits.

How SmartSuite supports StateRAMP Low+ Cat 2

StateRAMP Control Library (Low+)

Structure Low+ baseline controls aligned to NIST 800-53 requirements for state government cloud services.

System Security Plan and Boundary Management

Maintain SSP documentation, system boundaries, and architecture required for StateRAMP authorization.

Control Implementation and Risk Management

Track control implementation status, risk assessments, and remediation activities across cloud environments.

Vulnerability and Security Posture Monitoring

Monitor system security posture, vulnerability findings, and patch management workflows.

StateRAMP Provider and Subcontractor Tracking

Track service providers, subcontractors, and shared responsibility models supporting StateRAMP compliance.

StateRAMP Review and Authorization Readiness Reporting

Provide dashboards summarizing control coverage, open findings, and readiness for StateRAMP review and authorization.

Common framework mappings

CIS Controls v8.1 | FedRAMP Rev. 5 | ISO 27001:2022 | ISO 27002:2022 | ISO 27017 | NIST CSF 2.0 | SOC 2

Official resources

StateRAMP Baseline Controls 2022

Defines security controls required for compliance with StateRAMP Low+ Category 2 standards.

govramp.org/document-library

Frequently asked questions

What is StateRAMP Low+ Category 2 used for?

StateRAMP Low+ Category 2 is designed to establish baseline cybersecurity requirements for cloud service providers working with U.S. state and local government agencies. It ensures low-impact data is protected through structured security controls drawn from NIST SP 800-53 low baseline, with additional enhancements for public sector needs.

Is StateRAMP Low+ Category 2 certification mandatory for vendors?

StateRAMP Low+ Category 2 is not federally mandated but is increasingly required or recommended by state and local government procurement officials when selecting cloud service vendors. Certification demonstrates that a vendor meets recognized security standards, supporting eligibility for government contracts.

What types of organizations or systems does StateRAMP Low+ Category 2 apply to?

The framework applies primarily to cloud service providers and vendors offering solutions that process, store, or transmit low-impact government data. State and local agencies also use it to assess vendor compliance and security posture during procurement and contract management.

What are the key documents and artifacts required for StateRAMP Low+ Category 2 compliance?

Compliance requires organizations to maintain current risk assessments, system security plans (SSP), control implementation summaries, and ongoing evidence of control effectiveness. Documentation is critical for demonstrating both design and operational effectiveness during third-party assessments.

How does an organization implement StateRAMP Low+ Category 2 controls?

Implementation involves mapping NIST SP 800-53 low baseline controls and StateRAMP-specified enhancements to internal policies and technical solutions, conducting regular risk assessments, training personnel, and documenting processes for audit purposes. Organizations should tailor controls based on their specific environments and service offerings.

How does StateRAMP Low+ Category 2 relate to other frameworks like FedRAMP or NIST SP 800-53?

StateRAMP Low+ Category 2 leverages the NIST SP 800-53 low baseline as its core, making it similar to FedRAMP Low but tailored for the unique requirements of state and local governments. It introduces supplemental controls and continuous monitoring practices to align more closely with state-level risk management objectives.

What are the ongoing compliance requirements for StateRAMP Low+ Category 2?

Ongoing compliance includes continuous monitoring of implemented controls, conducting periodic vulnerability assessments, maintaining up-to-date documentation, responding promptly to incidents, and preparing for regular third-party assessments to validate adherence to StateRAMP requirements.

How would SmartSuite support StateRAMP Low+ Category 2?

SmartSuite helps organizations manage StateRAMP Low+ Category 2 by centralizing control libraries, simplifying risk tracking, and automating evidence collection processes. It enables users to efficiently administer policy governance, manage remediation workflows, and maintain audit readiness. Customizable dashboards and integrated reporting features support compliance monitoring and facilitate timely submissions for regulatory reviews.

License included / downloadable: Yes StateRAMP program documentation is publicly available for download on the StateRAMP website.
License included with platform

Full framework page and mappings: smartsuite.com/frameworks/stateramp-low-plus-category-2