

TX-RAMP Level 2 – Moderate

TX-RAMP Level 2 assesses and authorizes cloud services used by Texas agencies to secure confidential or regulated data.



What it is

TX-RAMP Level 2 is a cybersecurity and risk management framework established to assess and authorize cloud computing services used by Texas state agencies handling confidential or regulated data. It aims to ensure that service providers implement robust security controls and meet compliance obligations specific to higher-risk data environments.

Published by the Texas Department of Information Resources (DIR), TX-RAMP applies to cloud vendors and state agencies across Texas that process, store, or transmit confidential or regulated information. The framework outlines requirements for cybersecurity controls, privacy safeguards, risk assessment, and ongoing compliance oversight in alignment with state regulations.

At a glance

PUBLISHER Texas Department of Information Resources (DIR)	TYPE Certification / Assurance Program	VERSION TX-RAMP Level 2 Baseline
EFFECTIVE 2021	DOMAIN Cloud Security	FAMILY FedRAMP
REGION Texas	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <http://dir.texas.gov/texas-risk-and-authorization-management-program-tx-ramp>

Why it matters

- **Strengthen third-party risk management** Enable agencies to systematically assess and monitor cloud vendors, reducing exposure to risks from external service providers.
- **Enhance data protection practices** Require robust controls that support secure processing, storage, and transmission of confidential and regulated information.
- **Increase audit readiness** Maintain thorough documentation and compliance evidence, supporting timely and efficient responses during regulatory audits and assessments.
- **Improve regulatory alignment** Align security practices with Texas state requirements and national standards, simplifying compliance efforts across multiple frameworks.

How SmartSuite supports TX-RAMP Level 2

Moderate-Risk Scope and Boundary

Define Level 2 scope, sensitive data handling, and service dependencies.

Level 2 Control Baseline Library

Track controls with owners, implementation details, and proof of operation.

Assessment and Remediation Workflow

Manage findings, remediation plans, retesting, and closure evidence.

Continuous Monitoring Operations

Schedule scanning, monitoring, and recurring evidence capture to prevent drift.

Vendor Obligation and Review Tracking

Track vendor obligations, evidence, and ongoing reviews for dependencies.

Audit-Ready Reporting

Report readiness, gaps, and monitoring status for assessors and stakeholders.

Common framework mappings

CIS Controls v8.1

FISMA

FedRAMP Rev. 5

HITRUST CSF v11.5

ISO 27001:2022

NIST CSF 2.0

NIST 800-171 Rev. 3

NIST 800-53 Rev.5

Official resources

TX-RAMP Level 2 Requirements

Describes the cybersecurity and compliance requirements for cloud services handling sensitive state data.

dir.texas.gov/texas-risk-and-authorization-management-program-tx-ramp

Texas Department of Information Resources: TX-RAMP Overview

Provides detailed information about the TX-RAMP framework and its application to Texas state agencies.

dir.texas.gov/texas-risk-and-authorization-management-program-tx-ramp-overview

TX-RAMP Compliance Guidelines

Outlines the steps and documentation needed for achieving TX-RAMP Level 2 compliance.

dir.texas.gov/tx-ramp-compliance-guidelines

Texas DIR's Security Control Standards Catalog

Defines the security controls required for TX-RAMP compliance, aligned with state regulations.

dir.texas.gov/security-control-standards-catalog

Frequently asked questions

What is TX-RAMP Level 2 used for?

TX-RAMP Level 2 is used to assess, authorize, and monitor cloud computing services that handle confidential or regulated data for Texas state agencies. Its primary purpose is to ensure that cloud vendors implement strong cybersecurity controls and meet regulatory compliance obligations for higher-risk data environments.

Is TX-RAMP Level 2 required for cloud service providers?

Yes, TX-RAMP Level 2 is mandatory for cloud vendors contracting with Texas state agencies if their services process, store, or transmit confidential, regulated, or otherwise sensitive information. Agencies are required to verify that their cloud service providers have achieved and maintain Level 2 authorization.

What organizations and data types does TX-RAMP Level 2 apply to?

TX-RAMP Level 2 applies to all Texas state agencies and higher education institutions utilizing third-party cloud services for regulated or confidential data. It covers any systems that handle sensitive state-regulated data such as personal, financial, or protected health information.

What are the key requirements and artifacts for TX-RAMP Level 2 compliance?

Key requirements include implementation of defined security controls, maintaining detailed documentation, performing third-party assessments, and compiling an authorization package. Artifacts include risk assessment reports, evidence of control operation, continuous monitoring plans, and authorization to operate letters.

How do organizations implement TX-RAMP Level 2 controls?

Organizations implement TX-RAMP Level 2 by mapping prescribed security controls—aligned with NIST SP 800-53—to existing policies and procedures, conducting risk assessments, and remediating gaps. Continuous monitoring, vulnerability management, and incident response processes are established to maintain ongoing compliance.

How does TX-RAMP Level 2 relate to other security frameworks?

TX-RAMP Level 2 is closely aligned with the NIST SP 800-53 control framework and the FedRAMP Moderate baseline, facilitating interoperability with established federal and state security programs. This alignment helps streamline compliance efforts for organizations already familiar with these standards.

What are the ongoing compliance requirements for TX-RAMP Level 2?

Ongoing compliance includes recurring risk assessments, continuous monitoring of controls, periodic third-party reassessments, and timely remediation of identified vulnerabilities. Organizations must maintain up-to-date documentation and provide evidence of ongoing adherence to security and privacy requirements.

How would SmartSuite support TX-RAMP Level 2?

SmartSuite facilitates TX-RAMP Level 2 compliance by providing configurable control libraries, centralized risk management, and automated evidence collection workflows. It enables teams to track remediation, prepare for audits, maintain compliance documentation, and generate real-time reports to demonstrate posture and regulatory adherence.

License included / downloadable: Yes TX-RAMP documentation is publicly available through the Texas Department of Information Resources.

Full framework page and mappings: smartsuite.com/frameworks/tx-ramp-level-2-texas-risk-and-authorization-management-program