INDUSTRY USE CASE

Government & Public Sector

Federal Agencies, State Governments & Government Cloud Providers

"FedRAMP authorized. FISMA compliant. StateRAMP ready."

Government agencies and the cloud providers serving them face the most rigorous cybersecurity compliance requirements in any sector. FedRAMP, FISMA, and StateRAMP authorizations require extensive documentation, continuous monitoring, and third-party assessment — processes that consume enormous internal resources without specialized support. Auditerra provides the platform, the process, and the certified human expertise to achieve and maintain government compliance authorizations efficiently.

FedRAMP Moderate | FedRAMP High | StateRAMP | FISMA | NIST 800-53 Rev 5

The Challenge

- FedRAMP Authorization to Operate (ATO) requires extensive System Security Plan documentation across hundreds of controls — a process that takes most cloud providers 12–18 months without experienced guidance.
- FISMA annual reporting requires federal agencies to assess and document security posture across information systems, often with limited internal cybersecurity staff.
- StateRAMP programs are expanding rapidly, with state governments increasingly requiring cloud providers to achieve StateRAMP authorization before contract award.
- Continuous monitoring under FedRAMP requires monthly vulnerability scanning, configuration management reporting, and annual control assessments — an ongoing operational commitment.
- The transition from NIST 800-53 Rev 4 to Rev 5 has left many agencies and cloud providers with control gaps that have not yet been formally remediated or documented.

Compliance Frameworks We Cover

FedRAMP Moderate

Required for cloud services processing Controlled Unclassified Information for federal agencies. Requires independent 3PAO assessment and ongoing continuous monitoring reporting.

FedRAMP High

Required for cloud services handling the government's most sensitive non-classified data. More stringent control requirements and more frequent monitoring obligations than Moderate baseline.

FISMA

Requires federal agencies to develop, document, and implement agency-wide information security programs. Annual FISMA reporting to OMB evaluates agency maturity across NIST 800-53 controls.

StateRAMP

The state government equivalent of FedRAMP — cloud providers seeking state government contracts must achieve StateRAMP authorization, assessed by approved Third-Party Assessment Organizations (3PAOs).

NIST 800-53 Rev 5

The foundational control catalog for federal information systems. Rev 5 introduced significant changes including supply chain risk management, privacy controls integration, and outcome-based control statements.

How Auditerra Engages — Our Process

Step 1 — Demo

A no-pressure, industry-tailored demo so you see exactly how our platform and auditors work together before any commitment.

Step 2 — Readiness Check

We conduct a gap assessment to map your current compliance posture, identify risk areas, and build a prioritized remediation roadmap.

Step 3 — Active Engagement

Our certified auditors don't hand you a to-do list. They work alongside your team — reviewing evidence, walking through controls, and personally resolving gaps in real time.

Step 4 — Continuous Monitoring

Compliance doesn't end at certification. Auditerra monitors your posture year-round, alerts you to drift, and keeps you audit-ready at all times — not just during audit season.

Why Not Big 5 or SaaS-Only?

Provider	What You Get	What's Missing
Big 5 Consulting	Deep expertise, global reach	Enterprise pricing — out of reach for most
SaaS-Only Platforms	Evidence collection platform	No human auditor — you're on your own
Auditerra	Platform + certified human auditors	Nothing. Custom pricing. Full engagement.

ATO Acceleration & Continuous Monitoring Operations

The FedRAMP Authorization to Operate process is one of the most documentation-intensive compliance engagements in any sector. Auditerra's experienced team has worked through the ATO process and understands exactly what JAB reviewers and agency authorizing officials look for in System Security Plans, Security Assessment Reports, and Plan of Action & Milestones. We accelerate the process by building SSP documentation in parallel with control implementation, coordinating directly with approved 3PAO assessors, and establishing the continuous monitoring workflows required post-authorization. For state agencies and StateRAMP applicants, we apply the same methodology at the state level — leveraging FedRAMP work products where applicable to reduce duplication.

What You Get with Auditerra

✓ FedRAMP System Security Plan (SSP) development across all applicable control baselines

✓ 3PAO coordination and assessment preparation for FedRAMP or StateRAMP authorization

✓ FISMA annual assessment support and OMB reporting documentation

✓ Continuous monitoring program implementation — monthly scanning, reporting, and POA&M; management

✓ NIST 800-53 Rev 5 gap assessment and control implementation roadmap

✓ ATO acceleration roadmap with milestone tracking and stakeholder reporting

---

Ready to See It in Action?

Book your no-obligation demo at **auditerra.com/demo** or reach out directly at **compliance@auditerra.com**. We'll tailor the conversation to your industry, your frameworks, and your timeline — no generic pitch decks.