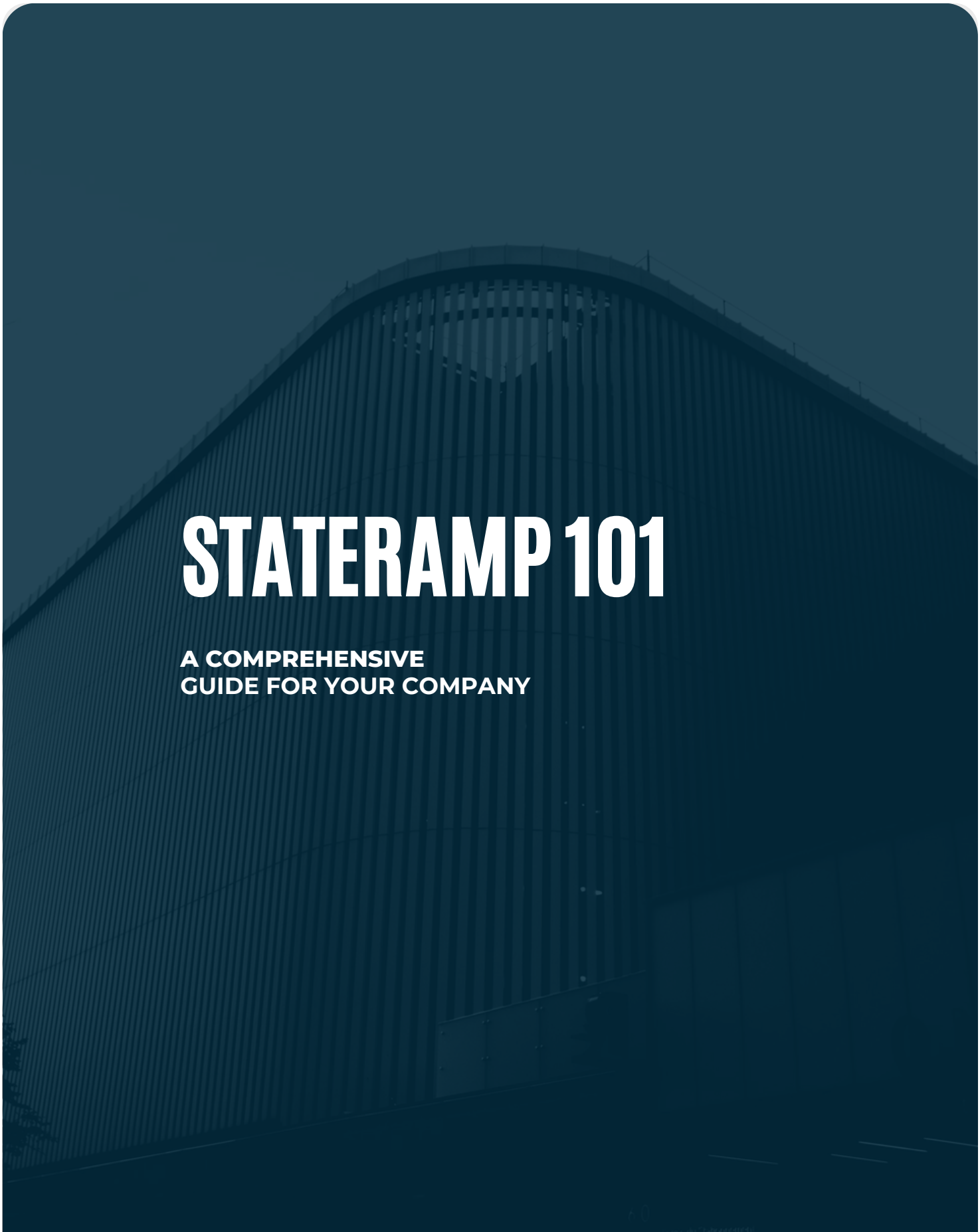
earthlingsecurity



STATERAMP 101

A COMPREHENSIVE GUIDE FOR YOUR COMPANY

INTRODUCTION

How Earthling Security Helps CSPs Achieve StateRAMP Compliance

In today's increasingly connected world, state and local governments rely on cloud services to deliver critical functions. As cloud adoption grows, so too does the need to ensure that these services are secure, protecting sensitive public sector data from escalating cyber threats. That's where StateRAMP comes in. Modeled after FedRAMP (Federal Risk and Authorization Management Program), StateRAMP provides a standardized cybersecurity framework that enables Cloud Service Providers (CSPs) to demonstrate they meet the rigorous security requirements necessary to do business with state and local governments. For CSPs, achieving StateRAMP authorization is becoming a vital step for participating in government contracts, as more states are adopting the framework. At Earthling Security, we specialize in helping CSPs navigate complex compliance landscapes. As an accredited Third-Party Assessment Organization (3PAO) with extensive experience in federal and state cybersecurity assessments, we are uniquely positioned to guide you through the entire StateRAMP process—from initial assessments to full certification and beyond.

What is StateRAMP?

Launched in 2021, StateRAMP (State Risk and Authorization Management Program) is a nonprofit organization designed to bring uniform cybersecurity standards to state and local governments. It ensures that cloud solutions meet the necessary security controls to protect State and Local Government (SLG) data and citizen information. CSPs must undergo a rigorous review and assessment process to become authorized, and that authorization ensures their cloud services comply with NIST SP 800-53 controls tailored to the sensitivity of the data they handle.

StateRamp's Framework:

- Standardized Security: Aligning with NIST SP 800-53, StateRAMP offers consistent and trusted security guidelines, ensuring that all participating CSPs follow the same set of criteria to safeguard data.
- Continuous Monitoring: StateRAMP requires ongoing monitoring and reporting to ensure CSPs remain compliant after receiving authorization, reducing the risk of emerging threats.
- Shared Assessment Model: Once authorized, CSPs can serve multiple government agencies under a "verify once, use many" model, eliminating the need for multiple, redundant security assessments.

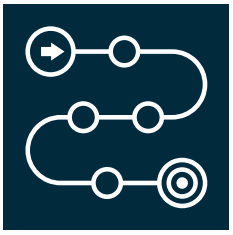
earthlingsecurity

How Earthling Security Helps CSPs Achieve StateRAMP Authorization

As an accredited StateRAMP 3PAO, Earthling Security has the expertise, experience, and tools to help CSPs successfully navigate the entire StateRAMP authorization process. Our holistic approach ensures your cloud services meet the necessary security controls while minimizing disruptions to your business operations. Here's how we help:

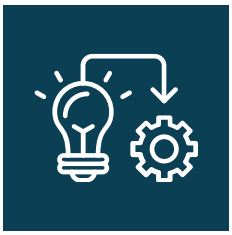
StateRAMP Readiness Assessment

Earthling Security begins by performing an in-depth readiness assessment of your cloud environment. This assessment compares your existing security controls against the StateRAMP control baseline, identifying areas that need improvement. Our team will review your existing policies, procedures, and technical implementations to determine how prepared you are for StateRAMP.



Gap Analysis and Detailed Remediation Plan

After the readiness assessment, we conduct a comprehensive gap analysis to identify specific deficiencies or gaps between your current environment and the requirements of NIST SP 800-53 Rev. 5. Based on this analysis, we develop a customized remediation plan to address those gaps, ensuring your cloud infrastructure aligns with StateRAMP requirements.



Security Control Implementation

Earthling Security provides hands-on support in implementing the necessary security controls to meet StateRAMP's Low, Moderate, or High baselines, depending on the sensitivity of the data handled by your services. This includes technical controls like encryption, secure authentication, access controls, and continuous vulnerability management.

Pre-Assessment & Mock Audits

Before your official StateRAMP audit, we conduct pre-assessment readiness reviews or mock audits. These simulations allow you to identify and fix any potential issues before undergoing the formal assessment. Mock audits help ensure that your documentation, processes, and controls are audit-ready.

Managing the StateRAMP Authorization Process

Earthling Security works with your team throughout the entire StateRAMP authorization process, from gathering the necessary security documentation to submitting the assessment package to the StateRAMP Program Management Office (PMO). Our deep understanding of the process allows us to streamline this step and ensure that everything is in order for final approval.

Continuous Monitoring & Compliance Support

After achieving StateRAMP authorization, the work doesn't stop there. CSPs must continuously monitor their cloud environment to ensure ongoing compliance. Earthling Security offers continuous monitoring services, including real-time vulnerability scanning, incident response planning, and ongoing compliance reporting to ensure your cloud systems stay secure and meet the requirements for annual recertification.

earthlingsecurity

How StateRAMP Works

StateRAMP's process is modeled closely after FedRAMP, but it is specifically tailored to meet the needs of state and local governments. The authorization process consists of several steps:

- **Preliminary Readiness Review:** CSPs must undergo a readiness review to assess their preparedness and identify gaps in their security controls.
- **Full Security Assessment:** CSPs then work with an accredited 3PAO, such as Earthling Security, to undergo a formal assessment of their security posture.
- **Authorization to Operate (ATO):** Once the assessment is complete, CSPs submit their package to the StateRAMP Program Management Office (PMO) for approval. CSPs that meet the necessary security controls are awarded StateRAMP Ready or StateRAMP Authorized status.
- **Continuous Monitoring:** After achieving authorization, CSPs must maintain continuous monitoring and regular reporting to ensure compliance is sustained.

Latest Developments in StateRAMP

StateRAMP continues to evolve as more states and local governments adopt the framework to secure their cloud infrastructure. Key recent developments include:

- **Adoption by Multiple States:** In addition to Arizona, which was an early adopter, many states, including Texas, Indiana, and Georgia, are now using StateRAMP as part of their procurement requirements, making it essential for CSPs looking to offer services to these governments.
- **Increased Focus on Cyber Insurance:** As part of its continuous monitoring and risk management, StateRAMP is increasingly emphasizing the role of cyber insurance as a mitigating factor in security incidents.
- **Alignment with NIST SP 800-53 Revision 5:** StateRAMP has updated its control baselines to align with NIST SP 800-53 Rev. 5, ensuring its security standards remain relevant in addressing modern threats, including enhanced controls around privacy and supply chain risk management.

Why CSPs Need StateRAMP

For CSPs looking to offer services to state and local governments, StateRAMP certification is quickly becoming a de facto requirement. Without StateRAMP certification, many CSPs are disqualified from government contract opportunities.

- Obtaining StateRAMP compliance demonstrates that your cloud environment meets stringent security standards, protecting sensitive state and citizen data. Additionally, StateRAMP-certified providers can enjoy the benefits of the "verify once, use many" model, where they only need to complete one assessment to serve multiple government agencies, reducing overhead and simplifying the sales process.

Detailed Plan for StateRAMP Preparation with Earthling Security

1. Initial Consultation

- Discuss specific StateRAMP statuses (e.g., Ready or Authorized) required based on your CSP's offerings and data risk classification.
- Review existing certifications (FedRAMP or other frameworks) to explore alignment with StateRAMP.

2. Comprehensive Readiness Review & Gap Analysis

- Conduct a thorough NIST SP 800-53 Rev. 5 based assessment of your current cloud infrastructure, policies, and technical controls.
- Identify gaps and areas that need improvement to meet StateRAMP's security requirements for Low, Moderate, or High impact levels.

3. Remediation Strategy & Implementation

- Develop a tailored remediation plan outlining the necessary steps to address gaps.
- Implement security controls such as encryption, access controls, and continuous monitoring in compliance with StateRAMP guidelines.

4. Pre-Assessment & Mock Audits

- Conduct a mock audit or pre-assessment review to simulate the actual StateRAMP audit, allowing your team to identify and address any remaining issues before the formal assessment. This ensures that all documentation, processes, and controls are ready for the official StateRAMP audit.

5. Full Security Assessment and Submission

- Earthling Security will guide you through the formal StateRAMP assessment process by working closely with your team to prepare all necessary documentation, security packages, and evidence. We manage communications with the StateRAMP Program Management Office (PMO) to ensure a smooth submission and review process.
- We also assist with navigating the StateRAMP statuses, whether aiming for StateRAMP Ready (preliminary status showing compliance with minimum requirements) or StateRAMP Authorized (full authorization following a complete security assessment).

6. Continuous Monitoring & Recertification Support

- StateRAMP requires ongoing security monitoring, which includes continuous vulnerability management, incident response testing, and reporting to the PMO. Earthling Security provides continuous monitoring services to ensure you stay compliant with StateRAMP requirements and ready for annual recertification.
- We handle regular compliance checks, vulnerability scans, and updates to your security policies, ensuring that your cloud infrastructure remains secure and StateRAMP-compliant over time.

earthlingsecurity

Why Continuous Monitoring is Essential in StateRAMP

Achieving StateRAMP compliance is only the beginning of your cloud security journey. Maintaining your StateRAMP Authorized status requires a commitment to continuous monitoring and ongoing compliance, ensuring that your cloud environment evolves with emerging threats. Earthling Security's continuous monitoring solutions offer real-time visibility into your cloud infrastructure's security posture, allowing for proactive threat identification and rapid remediation. We help you generate the necessary compliance reports for the StateRAMP PMO while ensuring your security controls remain effective and up to date.

Key Benefits of Earthling Security's Continuous Monitoring Services:

- **Vulnerability Scanning:** Regular scans to detect potential weaknesses in your system, ensuring timely remediation before issues become serious risks.
- **Automated Reporting:** We generate automated compliance reports that meet StateRAMP's continuous monitoring requirements, simplifying the ongoing compliance process for your team.
- **Incident Response Support:** In the event of a security incident, we help you respond quickly and effectively, mitigating risks and ensuring regulatory reporting is handled appropriately.
- **Security Updates:** We continuously review and update your security policies, ensuring your infrastructure is protected against the latest cyber threats and vulnerabilities.

Get Started on Your StateRAMP Journey with Earthling Security

StateRAMP is rapidly becoming a standard for doing business with state and local governments. Achieving StateRAMP authorization opens the door to opportunities across multiple states while ensuring that your cloud services meet the highest cybersecurity standards.

At Earthling Security, we specialize in helping CSPs navigate the complexities of StateRAMP compliance. From readiness assessments to continuous monitoring, our expert team is here to ensure your cloud environment is secure and compliant with StateRAMP.

Contact Earthling Security today to get started on your journey toward StateRAMP certification and unlock new opportunities in the public sector.

earthlingsecurity

Why Earthling Security?

- **Accredited 3PAO Expertise:** With over a decade of experience helping organizations achieve compliance with frameworks like StateRAMP, FedRAMP, and CMMC, Earthling Security brings unparalleled expertise to the StateRAMP process.
- **Comprehensive Support:** From readiness assessments to full-scale audits and continuous monitoring, Earthling Security provides end-to-end support to guide CSPs through every step of the compliance journey.
- **Tailored Solutions:** We understand that every CSP is unique. That's why we tailor our services to your specific infrastructure and security needs, ensuring you're fully prepared for the rigors of the StateRAMP process.

Get Started with StateRAMP Today

With StateRAMP rapidly becoming a standard for cloud services in state and local governments, now is the time to ensure your organization is ready. Earthling Security's experienced team can help you navigate the complexities of StateRAMP, ensuring that your cloud services meet the highest cybersecurity standards. Contact us today to learn how Earthling Security can guide your cloud services through the StateRAMP certification process and position your organization for success in the public sector.

StateRAMP Success Stories: Why Earthling Security is Trusted by CSPs

Earthling Security has a proven track record of helping Cloud Service Providers navigate the StateRAMP certification process, from initial assessments to continuous monitoring and recertification. Our hands-on, tailored approach ensures that every client is supported through the unique challenges they face in achieving StateRAMP compliance. Here's what sets us apart:

- **Accelerated Timelines:** We leverage our deep expertise in federal and state cybersecurity frameworks to streamline the certification process, helping CSPs achieve authorization faster without compromising the quality of their security controls.
- **Cross-Framework Alignment:** Many CSPs also pursue FedRAMP, CMMC, or SOC 2 certifications. Earthling Security's knowledge across multiple compliance frameworks allows us to align security controls, reducing redundancy and saving time and resources for your organization.
- **Trusted by States:** With Earthling Security as your StateRAMP partner, you can be confident that your services will meet the expectations of state and local governments. Our experience working with diverse government agencies ensures that your cloud solutions are trusted and secure.

Resources for CSPs Preparing for StateRAMP

For CSPs beginning their journey to StateRAMP compliance, there are several resources to help you navigate the process:

Earthling Security: As a certified StateRAMP 3PAO, Earthling Security offers full support for StateRAMP readiness assessments, gap analyses, remediation, and continuous monitoring. Our team ensures you have everything needed for a successful StateRAMP journey.

Contact us:

- **Email: info@earthlingsecurity.com**
- **Website: www.earthlingsecurity.com**

StateRAMP Official Website: The official StateRAMP website offers a wealth of resources, including guidelines, documentation, and FAQs to help CSPs understand the requirements and prepare for compliance.
Website: www.stateramp.org

NIST SP 800-53 Revision 5: The foundational document for StateRAMP security controls, NIST SP 800-53 Rev. 5 outlines the technical and administrative controls CSPs must implement to achieve compliance.
Download NIST SP 800-53 Rev. 5: NIST Website

StateRAMP Knowledge Center: The StateRAMP Knowledge Center offers guides, webinars, and training to help CSPs better understand the framework and prepare for certification.
Website: Knowledge Center

National Association of State Chief Information Officers (NASCIO): NASCIO represents state CIOs and IT executives and provides resources related to cybersecurity standards and StateRAMP adoption across states.
Website: www.nascio.org

FedRAMP: Many CSPs are already familiar with FedRAMP, which shares similar security controls with StateRAMP. If you are FedRAMP compliant, you can leverage that compliance toward StateRAMP authorization.
Website: www.fedramp.gov

earthlingsecurity

earthlingsecurity

Contact Us

877-282-2137

info@earthlingsecurity.com

www.earthlingsecurity.com