Should your application become StateRAMP compliant?

PROJECT HOSTS™
Security Compliant Clouds

www.projecthosts.com

info@projecthosts.com

Introduction

You don't need to be an independent software vendor (ISV) to know that business is booming when it comes to the cloud. Organizations of all verticals and sizes are migrating away from complex and expensive on-premise technologies in favor of cloud-based solutions. In fact, Gartner predicts global cloud spending will close in on nearly $500 billion by the end of 2022.[1]

But cloud adoption isn't so simple for state and local governments in the U.S. Despite their impatience to embrace cloud computing, many agencies in this emerging market are requiring Independent Software Vendors (ISVs) to comply with the State Risk and Authorization Management Program (StateRAMP) before doing business.

As a rigorous framework, StateRAMP can be difficult, costly and time-consuming to achieve. Yet, it's increasingly expected that ISVs follow this approach to cloud security. This begs the question: Why is StateRAMP necessary for state and local governments? And why should your application become StateRAMP compliant?

This white paper examines these questions while walking you through the purpose of StateRAMP. We'll discuss the requirements of StateRAMP verification and what you need to simplify the compliance process as you break into the state and local markets.

[1] https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022

Setting the stage for StateRAMP

Eager to leverage the scalability and efficiency of cutting-edge cloud technology, all levels of government are increasing their expense budgets and welcoming ISVs into their IT infrastructure. Following in the footsteps of the federal government — which upped its cloud spending to well over $11 billion in 2022 [2] — state and local agencies are completing their own race to the cloud.

But at the same time, increasingly daring and sophisticated cybercriminals are targeting sensitive data — such as that stored in state and local government clouds — to devastating results. In 2020, ransomware attacks on U.S. government agencies resulted in over $18 billion in damages, with every minute of downtime costing an estimated $8,662.[3] Altogether, over 70 million Americans may have been impacted. By the end of 2021, ransomware attacks increased 1,885% worldwide and are only expected to continue.

Why? Because government data is an extremely lucrative target. From personally identifiable information (PII) and personal health information (PHI) to confidential research and sensitive records, government clouds are rife with the type of intelligence that threat actors want to get their hands on.[4]

In response, dozens of current and former CIOs and CISOs bound together to form the StateRAMP Alliance, a nonprofit organization whose mission is to:

- Protect citizen data.
- Save taxpayer and service provider dollars.
- Lessen the burden on state and local governments.
- Promote cybersecurity education and best practices.

StateRAMP establishes a common standard for states and local governments to verify the effectiveness of their cybersecurity posture. Similar to the FedRAMP framework, the initiative aims to create a uniform strategy through which government agencies can better assess ISVs and protect their infrastructure.

> *Following in the footsteps of the federal government — which upped its cloud spending to well over $11 billion in 2022 [2] — state and local agencies are completing their own race to the cloud.*

[2] https://www.nextgov.com/it-modernization/2022/07/federal-agencies-invest-more-each-year-cloud-benefits-outweigh-challenges/374672/
[3] https://www.comparitech.com/blog/information-security/government-ransomware-attacks/
[4] https://www.sonicwall.com/2022-cyber-threat-report/

Should you become StateRAMP compliant?

StateRAMP's security verification model is based on the National Institute of Standards and Technology (NIST) publication 800-53 Rev. 4 — the same cybersecurity guideline used to develop FedRAMP. **And much like its federal counterpart, StateRAMP recognizes three verified statuses:**

Ready: The ISV meets StateRAMP's minimum requirements and most critical controls.

Provisional: The ISV has submitted a package for authorization consideration but is found to meet most but not all requirements.

Authorized: As the highest verification level, the ISV meets all requirements and is in compliance with all of the necessary security controls.

Ideally, ISVs earn Authorized status to signify complete compliance with StateRAMP's strict framework. However, many states, agencies and local governments require ISVs to at least achieve Ready status.

Consequently, you'll need to complete the following steps if you want to sell cloud services to state and local governments:

1. ISVs must engage a Third-Party Assessment Organization (3PAO), which is responsible for objectively assessing the security posture of the ISV and its services.
2. The 3PAO conducts an assessment of the application and reports its findings to StateRAMP.
3. The StateRAMP Project Management Office (PMO) reviews the security report and verifies the status of the application.
4. StateRAMP adds the application to the Authorized Product List (APL).

Without a spot on the APL, you may not be able to do business with state and local governments. That's why StateRAMP compliance is essential. As the key that unlocks an entire market of organizations eager to deploy state-of-the-art cloud technologies, StateRAMP verification helps assure potential clients that you're a forward-thinking and security-conscious provider.

StateRAMP not only breaks down one of the biggest barriers to entering the public sector, but it also enables you to grow your business at scale. The standard's "verify once, serve many" model eliminates the need to recertify compliance for every individual agency, making it easier to capitalize on opportunities and penetrate the market. With this advantage, you can create a level playing field in an increasingly competitive cloud marketplace.

All told, StateRAMP provides clients with the confidence that they're working with an ISV who's already achieved a predetermined level of compliance through an unbiased review process. And with more states holding partners to that higher standard, StateRAMP is quickly becoming a must-have for government vendors.

Challenges in the process

When it comes to achieving StateRAMP compliance, ISVs tend to try and do it themselves. However, the StateRAMP assessment process is much more complex than the steps outlined above may lead you to believe.

In truth, compliance isn't easy. It takes time, costs a lot of money and diverts your attention away from innovating and delivering a unique solution to your end users. By the end of the process, which can take upwards of two years to complete, you may run up a tab worth millions of dollars. That's in addition to the cost of continuous monitoring and 3PAO assessments, as required to maintain StateRAMP Authorized status.

Indeed, ongoing compliance requires ongoing effort. One of the most time-consuming and difficult steps that need completing is evidence collection. This critical step alone can be extremely draining, as it requires you to produce documentation and proof for everything being done to implement StateRAMP's security controls. With hundreds of StateRAMP controls to account for, it's no wonder that many organizations fall short of achieving compliance.[5]

To reach and maintain StateRAMP verification, ISVs need to adhere to the framework's strict requirements. These include, but are not limited to:

- Managing Access Control and Authentication.
- Monthly baseline compliance scanning.
- Regular patching and vulnerability management.
- Having a dedicated incident response and analysis team.
- Implementing malware and intrusion prevention.
- Reviewing audit logs and alerts.
- Monthly scanning and testing performed by a 3PAO.

All the while, it's easy to get caught in the weeds of compliance and lose sight of what matters most: Innovating and delivering valuable solutions to end customers. Compliance is important, but it also requires a lot of attention, which can get in the way of productivity and growth.

[5] https://stateramp.org/wp-content/uploads/2021/12/StateRAMP-Continuous-Monitoring-Guide-v1.3.pdf

A simplified path toward StateRAMP

ISVs fortunately have a smarter, simpler alternative to managing compliance on their own. Outsourcing the entire certification process to a third party with StateRAMP expertise may not only streamline the process, but could also become an enabler of long-term growth and sustainability.

Project Hosts' compliance-as-a-service offering removes the burden of managing cloud compliance. By partnering with Project Hosts, you can simplify StateRAMP in three ways:

Compliance Inheritance:

When you connect your applications to Project Hosts' General Support System (GSS), you're putting them on a platform that's already StateRAMP Authorized. In turn, 80% of all security controls are already handled, meaning that the StateRAMP PMO only needs to review the remaining 20% at the software level. With the GSS, you can rest assured that your application security is up to par.

Compliance by Certification:

The Project Hosts' turnkey certification service takes the trouble out of certification. Our team engages with a 3PAO on your behalf, prepares you for the audit and assists in the difficult evidence collection process so that you don't have to worry about sorting it all out on your own.

Continuous Compliance:

After migrating your applications to our StateRAMP Authorized platform, our teams will continuously monitor performance, prevent intrusions and take care of critical cybersecurity operations such as incident management, reporting or patching.

The benefits of compliance-as-a-service

When you leverage compliance-as-a-service to your advantage, you may find yourself reaping the rewards of a straightforward and less daunting certification process. Here's how you can stand to gain from outsourcing StateRAMP compliance to Project Hosts:

Faster time-to-compliance:

Rather than spending years of your growth concentrating on StateRAMP, outsourcing 80% of security controls to us allows you to complete the process in just 2-6 months.

More cost savings:

Ultimately, compliance-as-a-service costs far less than working through the long, difficult certification process on your own. Not only is this better for your bottom line, it also means you can allocate more resources to growth-driving areas of the business.

More time to innovate:

With less attention devoted to compliance, your organization is free to focus on developing cutting-edge technologies for your customers and growing your company.

Streamline compliance with Project Hosts

When you work with Project Hosts, you gain immediate access to a team of expert engineers who can manage compliance on your behalf. In turn, you can stay ahead of changing StateRAMP requirements, eliminate the risk of deauthorization and devote your time and energy toward what matters most: The continued growth and success of your business.

Altogether, Project Hosts is here to help you simplify compliance and capitalize on the emerging state and local government market. For more information about how Project Hosts can help your organization achieve compliance, reach out to our team today.