The Imperative Role of StateRAMP Authorization in Implementing Registry Software

As more and more services move online, governments and institutions need to deliver services and manage data differently. Fundamental to an online presence is the use of a registry platform - a robust system designed to collect large volumes of often sensitive data and manage that data through a secure lifecycle while managing a relationship with those who supply the data.

In their fiduciary role as trustees of public and private data, custodians of critical infrastructure and vital services, public sector entities operating registry systems must follow stringent security and data protection regulations. The State Risk and Authorization Management Program (StateRAMP) was created to ensure these non-Federal public service entities follow cybersecurity best practices.

StateRAMP was launched in 2021. It was modelled on FedRAMP, a federal-level product authorisation program. While FedRAMP focuses only on cloud providers wishing to do business with Federal government agencies, StateRAMP is tailored to state and local governments. Both programs demand that any cloud provider offering considered for use by a government agency addresses a specified set of NIST (National Institute of Standards and Technology) 800-53 security requirements which are a comprehensive set of safeguarding measures for federal information systems, covering management, operational, and technical security controls, organized into 18 control families. Examples include access control, awareness and training, audit and accountability, identification and authentication, and system and communications protection. Failure to comply simply means a "no-go".

Elements of StateRAMP

StateRAMP is a security assessment framework tailored for cloud-based products and services. It ensures software and infrastructure compliance with standards that safeguard data integrity, confidentiality, availability, and non-repudiation. StateRAMP authorisation becomes even more critical in the context of registry software, as this software is a repository of sensitive and often confidential information.

Firstly, StateRAMP authorisation is instrumental in bolstering the security architecture of registry software. As a gatekeeper of sensitive information, this software must be resistant to a myriad of cyber threats. StateRAMP authorisation mandates that the software undergoes rigorous testing and evaluation to guarantee its resilience against security breaches. This rigorous assessment serves to protect the integrity of the data held within the registry software, thereby ensuring public trust in the system's capability to guard against unauthorised access and data breaches.

Secondly, StateRAMP authorisation ensures that the software maintains high data privacy standards. The authorisation's stringent requirements necessitate the implementation of robust privacy controls. These controls range from solid encryption algorithms to protect the data in transit and at rest to strict access control measures ensuring that only authorised personnel can access the data. In essence, StateRAMP authorisation ensures that the registry software is designed to prioritise and uphold the privacy rights of individuals whose data is stored within the system.

To become StateRAMP authorised, a cloud provider must follow several steps and build certain elements into its offering. Here is a breakdown of the official steps involved:

Initial Preparation

Research: The provider should first understand StateRAMP and the assessment process.

Obtain a Sponsor: This is optional. Sponsors are individuals or agencies responsible for reviewing a security package and approving StateRAMP authorised status. Sponsors are usually the state agency or organisations using the cloud product. Alternatively, the provider may use StateRAMP's Approvals Committee.

Find a Third-Party Assessment Organisation (3PAO): StateRAMP assessments must be completed by a 3PAO. This organisation has gained special authorisation to conduct assessments on behalf of the StateRAMP program. Any FedRAMP 3PAO is eligible to conduct the assessments but must register with StateRAMP.

Complete a Readiness Assessment (optional): This is an initial assessment where a 3PAO looks at the provider's environment to determine if it is technically capable of meeting the StateRAMP requirements. This step can help identify gaps in controls before the official 3PAO assessment.

After having been through the assessment for StateRAMP, the following steps are typically taken:

Submit Security Review Request: The service provider completes and submits the Security Review Request Form. Once this form is submitted, the StateRAMP Program Management Office (PMO) team will initiate an intake call and commence their security review.

Government Sponsor or Approvals Committee: In order to obtain an Authorised status, the security package needs to be approved by either the Approvals Committee or a Government Sponsor. These entities act as the authorisation officials and ensure that the package fulfils StateRAMP requirements.

Obtain a StateRAMP Verified Status: If the Third-Party Assessment Organisation (3PAO) confirms that the provider meets all required security controls, and the StateRAMP PMO verifies these findings, a government sponsor or the StateRAMP Approvals Committee accepts the provider's security package, and all outstanding issues and inquiries have been resolved, the provider's security status on the StateRAMP Authorised Product List (APL) will be updated to Authorised. A Ready status suggests that the product satisfies StateRAMP's minimum mandatory requirements and most critical controls.

Continuous Monitoring: After the provider has achieved a verified status, they must begin providing the required documentation for monthly continuous monitoring reporting to maintain their StateRAMP security status. This is outlined in the StateRAMP Continuous Monitoring Guide.

In the contemporary digital landscape, StateRAMP authorisation has emerged as a vital component for companies building US state registries. The significance of this authorisation can be attributed to the rising cybersecurity threats and the urgent need for standardisation and stringent security protocols.

StateRAMP authorisation has rapidly been adopted by a growing number of states, which leverage it to ensure their third-party suppliers meet baseline cyber requirements and maintain published cybersecurity policies. This helps state and local governments validate the cybersecurity posture of their providers' cloud-based solutions without incurring additional costs or resources.

Best Practice

Moreover, StateRAMP authorisation offers transferrable credentials through standardised cybersecurity verification, allowing providers to verify once and serve many. This creates a streamlined process for suppliers and a shared service for governments, enhancing overall efficiency and security. The interest in

StateRAMP authorisation has far exceeded initial expectations, with an increasing number of states recognising its value in strengthening cybersecurity nationwide. StateRAMP also benefits service providers by allowing them to demonstrate their commitment to best practices in cloud security, thereby enhancing their reputation and trustworthiness. It is important to note that the specific security controls and technical requirements that must be met to achieve StateRAMP authorisation will vary depending on the impact level of the cloud service offering (Low, Moderate, High) and are aligned with the NIST 800-53 security control baseline. These include, among other things, access controls, audit and accountability measures, incident response procedures, and system and information integrity practices.

In conclusion, StateRAMP authorisation will be indispensable in US state registries going forward. It fosters a safer digital environment, instils stakeholder confidence, and paves the way for a more secure and reliable future in the face of escalating cybersecurity threats.

At Foster Moore, we recognize that it is widely accepted that the area of security vulnerability is constantly fluid. For every tool that is developed to close a security hole, there are new malicious attempts to exploit other weaknesses in security. As technology advances, each advance provides an opportunity for malicious exploitation. StateRAMP is a continuation of Foster Moore's commitment to security, privacy and interoperability standards that have been key in the development of our products to date. Foster Moore's work towards the authorisation further validates that the software is robust, reliable, and fit for purpose. While StateRamp is applicable in the US, the validation is relevant for others that care about IST, ISO, StateRAMP, and SOC2. Therefore, in the digital transformation era, the significance of StateRAMP authorisation in implementing registry software cannot be overstated. It represents a regulatory requirement and a commitment to uphold the highest data management standards, fostering public trust in digital services. For more information on StateRAMP and its components, visit stateramp.org