



ATO on AWS

Customer Profile



authority to
operate

“SecureIT’s FedRAMP offerings are designed to help cloud service providers of all sizes succeed in their readiness and authorization efforts with less risk and less organizational impact.

As with all of our compliance and cybersecurity offerings, you can expect a partner that will understand your business and provide practical, efficient solutions that work for the specific needs of your organization.”

David Trout

CEO, SecureIT

SecureIT and ATO on AWS

As an accredited 3PAO with extensive experience on AWS, SecureIT is proud to be part of the ATO on AWS program. The ATO on AWS initiative is focused on reducing time and cost while improving security capabilities of cloud systems running on AWS that must be compliant with FedRAMP. SecureIT delivers full lifecycle FedRAMP solutions that are tailored for specific cloud systems running on AWS, including both advisory services and assessment services.

An ATO on AWS Success Story



Pegasystems engaged SecureIT to refocus the FedRAMP readiness initiative for their Pega Cloud for Government system (running on AWS GovCloud) and to help drive the project to a successful and timely conclusion with an Agency authorization. The project began with a review of the boundary and the use of AWS services. Then, SecureIT’s advisory consultants worked hand-in-hand with Pega’s technical and compliance teams to determine how the controls were actually implemented, identify gaps and deficiencies in controls, devise a remediation approach that complied with FedRAMP requirements, and validate successful remediation.

Remediation steps often included procedures specifically focused on AWS related services, including the following:

- Assessing the risk of using AWS services that have not yet been FedRAMP authorized
- Ensuring that client systems and services were configured properly across all management system and customer tenant systems to leverage and inherit AWS-provided controls
- Participating in the design of the remote access architecture that met requirements for availability, multifactor authentication, and FIPS validation
- Verifying appropriate audit trails through CloudTrail to provide full accountability
- Verifying CloudFormation templates for provisioning a new customer stack
- Assisting with configuration compliance scanning (and hardening the configuration of) RDS databases



Our consultants led the effort to produce the complete FedRAMP documentation package, including the System Security Plan (SSP) and the required attachments and plans. We also developed a detailed listing of all ongoing control tasks for the continuous monitoring plan. To help ensure a successful assessment, we also performed a “dry run” pre-audit and then served as a liaison during the assessment to manage the request list and communications between Pega and the third-party assessor (3PAO). By leveraging AWS services and working with SecureIT, Pega achieved FedRAMP Ready status and then obtained a FedRAMP Agency authorization on time.

SecureIT FedRAMP Advisory Services

SecureIT’s range of FedRAMP Advisory services address the needs of CSPs at various stages in their FedRAMP journey. Our experts remove the guesswork from your FedRAMP authorization pursuit and help you accomplish the most important goal: new business opportunities with Federal Agency customers. SecureIT has a deep understanding of controls and control requirements, and how AWS services and automation can be leveraged to meet those requirements. We also know the hurdles that organizations typically face with compliance, and how to leverage existing processes and artifacts to increase efficiency. In addition to strategic advice and development of required documentation, our consultants can stand together with you during the 3PAO assessment. With SecureIT on your side, you can be confident that your FedRAMP authorization initiative is efficient and effective while keeping key personnel focused on the core mission.

Lifecycle Phase	Advisory Service Offerings	Description
Plan	Baseline Assessment	Assess the current status of the FedRAMP program and control capability indicators and provide a roadmap for moving forward
Design	Gap Analysis	Identify all material gaps in the system boundary, control design, and documentation as part of a comprehensive “punch list” of corrective actions
Build	Real-time Input	Guide and actively support IT engineering efforts to remediate FedRAMP gaps by providing real-time input as solutions are designed and implemented
Document	Package Creation	Prepare a complete FedRAMP documentation package that meets all PMO requirements and will be useful for Agencies and the 3PAO
Validate	Pre-Audit	Perform a pre-validation of FedRAMP controls and documentation and identify problems that can be fixed quickly before the official assessment begins
Assess	3PAO Facilitation	Serve as a liaison between the CSP and 3PAO to achieve a positive assessment outcome
Maintain	Continuous Monitoring	Manage periodic controls that are required by FedRAMP continuous monitoring, especially the reports that must be submitted monthly for review

SecureIT FedRAMP 3PAO Offerings

SecureIT is an accredited third-party assessment organization (3PAO) for all types of FedRAMP assessments. We fully understand that assessments can be viewed as a necessary evil. Our goal is to complete the assessment according to published guidance as efficiently and painlessly as possible. Although request lists are unavoidable, we can minimize the request list by pulling information ourselves from the AWS CLI or API with read-only access keys. We also focus our control testing and penetration testing efforts on the areas of the cloud system that present the most risk. For example, rather than merely check-the-box that security groups are in place, we will actually examine the security group filters that are applied to various instances (and any network ACLs that are applied to subnets) and assess the validity of the traffic flows that are permitted.

Such additional focus helps to avoid requests from the PMO, Agency, or JAB for additional work that needlessly delays authorization, and also helps to reduce the likelihood of a surprise security incident that could have serious and long-lasting impacts on the reputation of the cloud system and the CSP.



3PAO Service Offerings	Description
FedRAMP 3PAO Readiness Assessment (RAR)	Provide a FedRAMP readiness assessment and issue a RAR according to the FedRAMP PMO's published guidance
FedRAMP 3PAO Initial Assessment	Perform an initial FedRAMP Assessment according to the FedRAMP PMO's published guidance for an Agency authorization or JAB P-ATO covering all controls in a FedRAMP baseline (LI-SaaS, Low, Moderate, or High) or overlay (IL4 or IL5)
FedRAMP 3PAO Annual Assessment	Perform the annual assessment according to the FedRAMP PMO's published guidance of the 97 core controls and ~1/3 of the remaining controls selected by the CSP

A True Partner for FedRAMP Success

Choosing SecureIT FedRAMP Advisory services provides your organization with experienced professionals who partner with you to develop a plan for success and provide the appropriate resources and expertise to achieve FedRAMP authorization for your AWS-hosted cloud system. Regardless of whether you have a dozen questions and are just beginning to investigate what FedRAMP means to you, or you need an expert to validate in-house efforts for leveraging AWS services, or you're looking for a 3PAO with AWS experience to perform your assessment, SecureIT is the partner you can count on for practical, flexible FedRAMP and AWS expertise.

About SecureIT

SecureIT provides risk, compliance, and cybersecurity services to enterprises, government entities, and cloud service providers. Our certified professionals assess cyber risk, conduct targeted security assessments, and ensure compliance with regulatory requirements. Every day, we partner with our clients to deliver solutions critical to protecting and growing business.

12110 Sunset Hills Road, Suite 600
 Reston, VA USA 20190
 703.464.7010
www.secureit.com