Acquia Renews FedRAMP Authority to Operate

The company remains the only non-governmental Drupal hosting provider with FedRAMP certification

As federal agencies elevate the user experience on their .gov sites, the security and integrity of their digital platforms remains paramount. As a technology provider to the federal sector, Acquia's greatest priority is meeting its security and compliance demands of our customers. In the United States, the gold standard for government website security is the Federal Risk and Authorization Management Program (FedRAMP), the set of standards and rules that any vendor who wants to provide products and services to a federal agency must meet.

Acquia has been a FedRAMP Compliant Cloud Service Provider (CSP) since April 2016, when we received our first Authority to Operate (ATO) from the U.S. Department of Treasury. Since then, that certification has applied to our customers in the federal sector who use Acquia Cloud Platform and Acquia Site Factory. In 2022, we added Acquia Site Studio and Acquia Platform Email capabilities to the FedRAMP boundary, then, in 2023, the latest versions of Acquia Search with Solr 8. Acquia also secured a positive recommendation from a FedRAMP third-party assessment organization (3PAO).

For Acquia, FedRAMP has enabled our customers to host critical applications in the cloud, use open source Drupal, and leverage our platform-as-a-service (PaaS) capabilities with confidence. To date, we remain the only non-governmental Drupal offering with a FedRAMP certification.

The federal government spends hundreds of millions of dollars a year securing the use of IT systems; FedRAMP assures agencies that the appropriate security and risk management practices are in place for their cloud properties. FedRAMP compliance requires Acquia's security team to ensure that we're meeting the required parameters.

What is FedRAMP?

FedRAMP was created in 2011 to establish standards and efficiencies for cloud security practices. The government-wide program provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

The close collaboration of cloud experts from both the private sector and the government organizations listed below brought FedRAMP into being:

- General Services Administration (GSA)
- National Institute of Standards and Technology (NIST)
- Department of Homeland Security (DHS)
- Department of Defense (DOD)
- National Security Agency (NSA)
- Office of Management and Budget (OMB)
- Federal Chief Information Officer (CIO) Council

Its creation accelerated the adoption of secure cloud solutions, provided a baseline set of standards for cloud product approval, increased confidence in the security of cloud solutions, ensured consistent application of existing security practices, and increased the automation of near real-time data for continuous monitoring.

How did Acquia secure an ATO?

To secure FedRAMP Authority to Operate, Acquia had to meet the robust and detailed set of security controls outlined within the NIST SP 800-53 Revision 4 standard. Our team underwent a rigorous independent, third-party audit and approval process before getting FedRAMP Authorization. The process included three steps:

1. Security Assessment
2. Leveraging and Authorization
3. Ongoing Assessment and Authorization

These FedRAMP processes are designed to help agencies meet the Federal Information Security Management Act of 2002 (FISMA) requirements for cloud systems and to address the specific challenges that cloud systems face when trying to become FISMA-compliant. An agency that begins this process with a FedRAMP compliant platform has already put certain security measures in place that will aid them in securing their own ATO.

What does this mean for you?

FedRAMP delivers a number of benefits to federal, state, and local government agencies, as well as other governmental applications. It offers a significant cost and time savings, as well as a uniform approach to risk-based management. FedRAMP also improves real-time security visibility and enhances transparency between the government and CSPs.

Every government application requires an ATO, but some platforms — like Acquia Cloud Platform — can make the process much faster and more affordable. If your organization deploys your application in an on-premise data center, then you'll require an ATO for the infrastructure, platform, and application. If you've deployed your application with AWS, which is also FedRAMP-compliant, the controls are only in place through the IaaS level, so your organization is still responsible for platform and application certification. With the Acquia Platform, however, FedRAMP controls are in place up to the PaaS level, so your organization is only responsible for certification at the application level.

So, if you're an Acquia customer, you can leverage a best-in-class platform that's compliant with federal security standards out-of-the-box. Your Certification and Accreditation (C&A) efforts will require significantly less time and cost compared with trying to accredit an on-premise solution or even a system built on a FedRAMP-compliant IaaS. In short, you get a safe and secure cloud platform to power your organization.

Overall, with FedRAMP in place, your organization experiences improved trustworthiness, reliability, consistency, and quality of the federal security authorization process. For more information about Cloud Platform, Site Studio, and Acquia's other products for building and supporting Drupal applications, explore our Drupal Cloud offerings.

Public sector agencies that want to learn more about how they can deliver safe, personalized experiences to constituencies can download the free e-book From Customer Experience to Citizen Experience: A Roadmap for Government Agencies to Become Digital Leaders.