# Strategy Guide for Achieving FedRAMP® Authorization

## Accelerate Your Time to FedRAMP® Approval

*Chris Hughes, Chief Information Security Officer, Aquia*
*Kalid Tarapolsi, Senior Director, Aquia*

# TABLE OF CONTENTS

# FEDRAMP OVERVIEW

The Federal Risk and Authorization Management Program (FedRAMP) plays a crucial role in IT modernization for government agencies seeking to use cloud services. The government's Cloud Smart policy requires federal agencies to prioritize the use of FedRAMP-authorized solutions in order to cut costs and simplify IT procurement. Cloud Smart aims to establish common security and compliance standards for cloud service providers (CSPs) through the Authority to Operate (ATO) and to implement a "do once, use many" framework. The FedRAMP program has undergone changes and introduced new techniques, such as automation, that can make the authorization process quicker, more efficient, and less costly.

## The Benefits of a FedRAMP Authorization

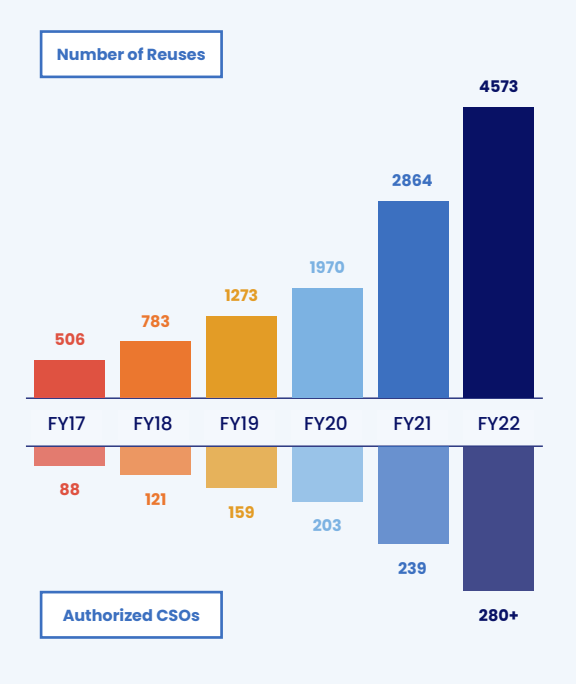
In FY22, FedRAMP authorized cloud products were reused more than **4,500 times** across the federal government, a 60% increase in reuse from FY21 and a **132% increase from FY20.**

By achieving FedRAMP authorized status, CSPs can see a **10x increase in their customer base** by reusing ATO packages across multiple agencies.

Agency demand for vendor-furnished cloud computing goods and services is forecast to grow from $14.5 billion in FY 2022 to $18.6 billion in FY 2024 for a 3-year percentage **growth rate of 28%.**

### Marketplace Growth Over the Years

From FY20 to FY22, FedRAMP has seen an **increase in reuse of 132%** as demand rises.





Sources:
FedRAMP. "FedRAMP Announces the Passing of the FedRAMP Authorization Act!" Jan. 11, 2023. https://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/

FedRAMP. "A Look Back at Fiscal Year 2022." Oct. 27, 2022. https://www.fedramp.gov/blog/2022-10-27-a-look-back-at-FY-22/

GovWin from Deltek. "Federal Cloud Computing Market, 2022-2024."

# The Benefits of FedRAMP Authorization

## Opens the door to do business with federal agencies

FedRAMP authorization is mandatory for all cloud services used by federal agencies. This requirement opens up the opportunity for cloud service providers to do business with the federal government, providing a wide market for their services.

## Adds a level of trust and marketability beyond federal agencies

By meeting the highest standards in cloud security, FedRAMP authorization establishes confidence in the security and privacy of cloud services. This authorization can be used to market the provider's services beyond federal agencies, with many commercial organizations, state, and local governments also looking for FedRAMP authorization when choosing their cloud solution providers.

## Leads to cost, time, and resource savings with a reusable assessment

The FedRAMP assessment is a one-time process that allows for authorization by multiple federal agencies. Once the assessment is completed, it is posted to the Office of Management and Budget (OMB) repository where other federal agencies can review and grant an Authority to Operate (ATO) based on the posted package. This reduces the time and effort required to secure individual authorizations, making it more convenient for providers.

## Streamlines opportunities with other federal and defense programs

Specific federal organizations, such as the Department of Defense (DoD), have additional requirements and guidance for CSPs looking to do business with them. CSPs can leverage their FedRAMP authorization status to meet some of these requirements, making it easier for them to do business with the DoD and other federal programs. For example, a FedRAMP Moderate authorization enables CSPs to obtain an Impact Level 2 (IL2) authorization, while a FedRAMP High authorization enables the CSP to gain an IL4 with the DoD.

## Increases visibility with a FedRAMP Marketplace listing

FedRAMP-authorized businesses can attract more attention when they become listed on the FedRAMP Marketplace. This marketplace is often the first place that government agencies go when looking for new cloud-based solutions, and agencies often prefer choosing a CSP from the FedRAMP Marketplace as it is faster and easier than starting the authorization process from scratch with a new vendor. By becoming listed in the marketplace, providers can increase their visibility and attract more potential clients.

## Getting Started

Obtaining executive sponsorship and developing a comprehensive business strategy are crucial for companies considering FedRAMP, as they establish a clear direction for investing in the needs of federal clients. The process of creating a holistic strategy involves addressing various technical, organizational, and competitive questions to ensure alignment and optimize outcomes. The cost, maintenance expenses, return on investment, technical resources needed, speed of listing on the FedRAMP Marketplace, competitors, differentiation strategies, federal sales strategy, securing agency sponsorship, cloud hosting options, FedRAMP baseline selection, and services to go to market with are all important factors to consider.

Achieving FedRAMP ATO requires extensive collaboration with and participation from the entire organization, with senior leaders providing the overarching vision, mid-level leaders managing projects, and front-line staff developing and implementing the systems. To present a comprehensive security posture to outside auditors, the organization must involve various corporate areas including engineering, operations, human resources, training, physical security, project management, data center operations, and vendor contracting.

## The FedRAMP Process

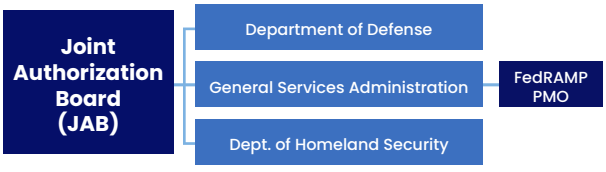
There are two ways to authorize a Cloud Service Offering (CSO) through FedRAMP: through an individual agency or the Joint Authorization Board (JAB).

### The Agency Path

The Agency path involves partnering with a specific agency for CSP documentation review and 3PAO System Assessment Report (SAR) review. This path requires a SAR, but the Readiness Assessment Report (RAR) in Stage 2 is optional.

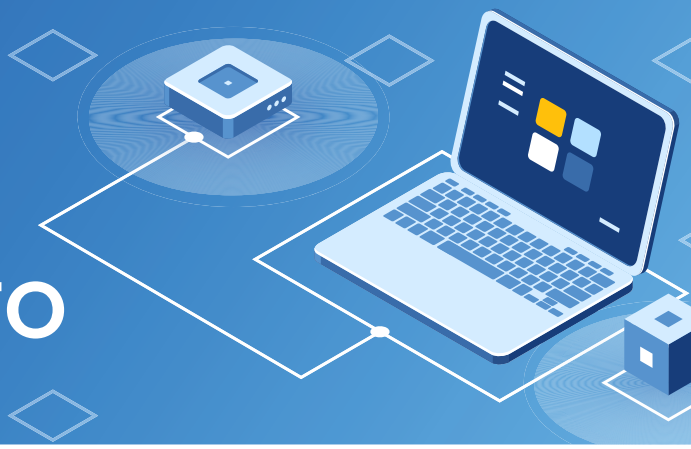

### The Joint Authorization Board Path

The Joint Authorization Board (JAB) may have a slightly higher degree of scrutiny and adherence to the letter of the law for FedRAMP-defined baseline controls. The JAB path involves creating a presentation outlining the federal customers and the security of the architecture, completing the architecture design and security controls implementation, required FedRAMP documentation, and working with a 3PAO to complete a RAR. The JAB reviews the SAR and once approved, a Provisional Authority to Operate (P-ATO) will be awarded, which other agencies can leverage to use the service or offering.


*It is important to note that the JAB only has resources to process 12 CSPs/year.*

# Five Main Phases of Obtaining an ATO



## CONSULTING AND PREPARATION

A chosen advisor provides guidance on business strategy, system architecture, remediation and documentation of the environment, and security controls. The advisor also prepares the system security plan (SSP), policies, and procedures.


## FEDRAMP READINESS ASSESSMENT

A third-party assessment organization (3PAO) conducts an assessment to determine the cloud service offering's readiness for the full FedRAMP assessment. This step is mandatory for the JAB path and optional for agency paths.

## PRE-ASSESSMENT

A 3PAO conducts a quick analysis or inventory of the existing cloud system documentation. The outcome is a high-level plan outlining the next steps and associated levels of effort. This pre-assessment can also be used to apply for FedRAMP Ready status, allowing the CSP to be listed on the General Services Administration (GSA) FedRAMP Marketplace. This indicates to a potential sponsor that you are well on your way to becoming authorized, giving them a high level of confidence in sponsoring the ATO.

## ASSESSMENT

A 3PAO develops the required FedRAMP documentation, including a security assessment plan (SAP), security requirements traceability matrix (SRTM) to document assessment results, vulnerability scanning, penetration test report, security assessment report, and recommendation for authorization.

## CONTINUOUS MONITORING

Ongoing monitoring is necessary to achieve and maintain the ATO, including monthly, quarterly, and annual monitoring.

# FEDRAMP BUDGETING

**The cost of implementing FedRAMP can vary widely depending on a number of factors, and as such, it is difficult to estimate the average financial commitment required. GSA data estimates place the project costs between $200,000 and $5 million for environment creation, FedRAMP preparation, and FedRAMP assessment.**

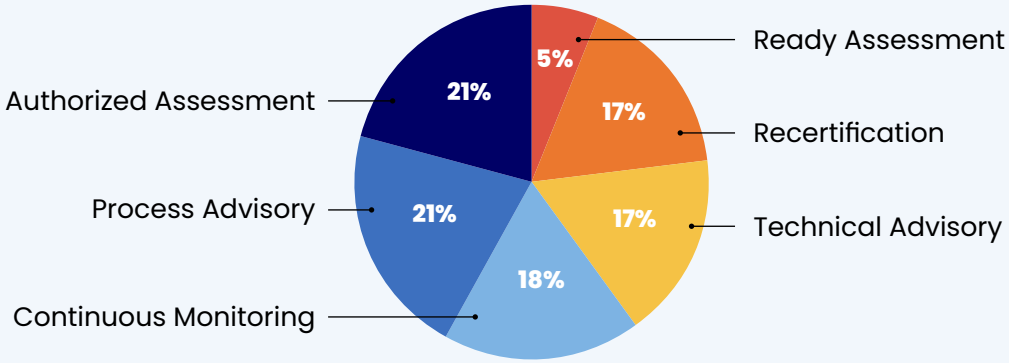
## Budget Breakdown

Much of the variation in timing and price depends on the solution's size and your familiarity with compliance frameworks. If you have experience with other industry regulatory compliance or security assessments then documents, policies, processes, and plans could potentially be reused for FedRAMP efforts, thus reducing the overall cost.

However, even with prior experience, the cost of implementing FedRAMP can still be substantial. Without a comprehensive analysis of the current state of the application and its environment, it can be difficult to determine the average financial commitment required. However, the costs associated with FedRAMP are concentrated in several areas such as environment creation, FedRAMP preparation and assessment, and ongoing monitoring.

One important aspect is the allocation of internal resources, which is necessary to manage and maintain FedRAMP efforts and any required cybersecurity activities that were previously unaccounted for. This includes allocating personnel and financial resources to ensure that your organization is able to meet the ongoing requirements of the FedRAMP program. Another important cost consideration is the technical remediation of information system issues. This includes identifying and addressing vulnerabilities and weaknesses in your systems that may impact your ability to meet FedRAMP requirements. This can involve significant technical work and may require the procurement of new or improved cybersecurity tooling and infrastructure creating a compliant tech stack.

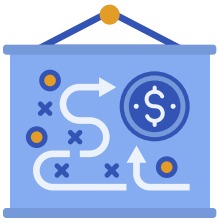
Additionally, the use of third-party advisory and preparation services should be considered. These services can help your organization navigate the FedRAMP process and ensure that you are fully prepared for the assessment. This can include consulting services, training and education, and other support services that can help you to better understand the FedRAMP requirements and how to meet them.



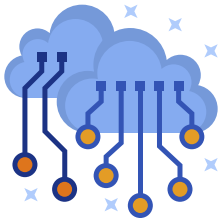
## FedRAMP Budgeting (cont.)

Finally, it's important to consider the cost of an independent 3PAO security assessment. This assessment is a critical step in the FedRAMP process and is designed to ensure that your organization has met all of the necessary security requirements. This assessment is performed by an independent third-party organization and can be costly.

The following additional factors may also have an impact:



Deciding whether to build a new production environment for FedRAMP or uplift current deployment. This process can be costly and require a significant investment in new technology and infrastructure.



Choosing whether to leverage an underlying Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS) provider or maintain control over the entire technical "stack" of the cloud production environment. This decision can have a significant impact on the cost of achieving and maintaining authorization.

Determining how much security automation to proactively invest in when preparing for FedRAMP. Automation can help to reduce the cost and complexity of meeting FedRAMP requirements, but it also requires a significant investment in new technology and infrastructure.

It is important to remember that FedRAMP should not be considered a point-in-time cost, but rather an ongoing operational investment.

Depending on some of the factors discussed in this section, the cost of maintaining authorization can add to initial cost estimates. It's important to have a clear understanding of these costs and to plan accordingly to ensure that your organization is able to meet the ongoing needs of the program.

# LEVERAGING AUTOMATION AND INFRASTRUCTURE AS CODE

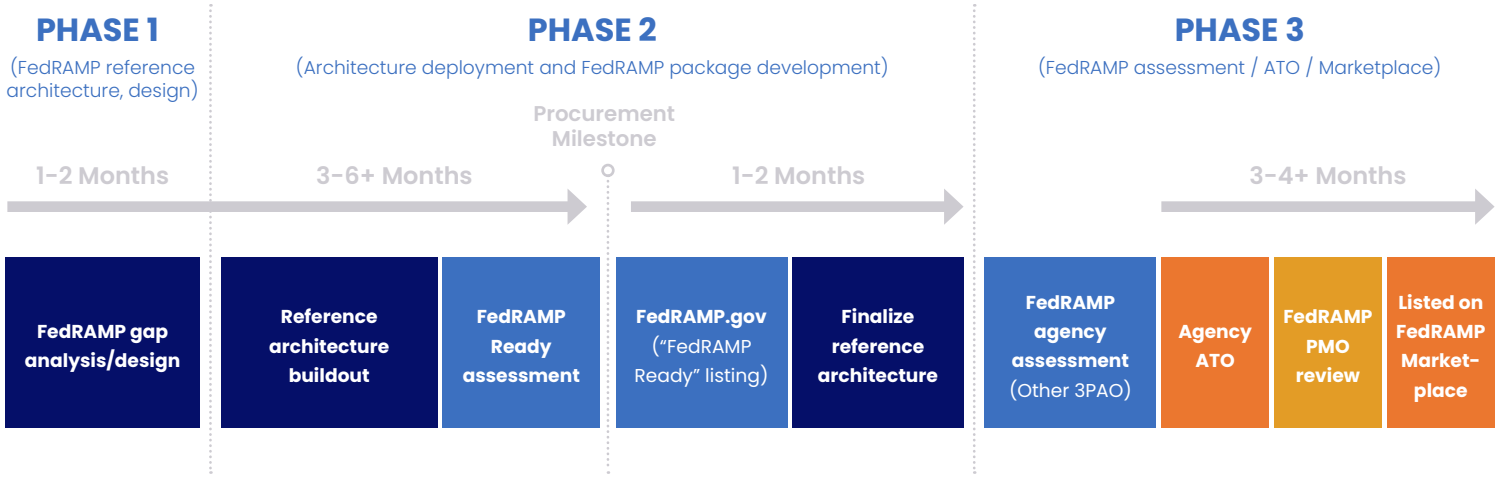
Recent advancements in technology, specifically Infrastructure as Code (IaC) and automation, have greatly improved the ability to implement security controls, thus reducing the time required to achieve compliance. By utilizing automated modules and IaC that have been preconfigured to meet FedRAMP controls and requirements, organizations can speed up the system build and deployment process, which can save both time and costs, and ultimately lead to a shorter time to market.

Implementing a security automation strategy can help organizations stay ahead of FedRAMP requirements and decrease the overall time required to gain authorization. Furthermore, it can also reduce the costs associated with maintaining compliance with FedRAMP and agency-specific cybersecurity requirements. Leveraging automation methodologies during FedRAMP preparation efforts has shown to be an effective way to reduce time to compliance and improve security.

Using preconfigured, cloud-based, compliant security stacks can be a cost-effective and efficient way to achieve compliance. However, considerations must be made that one size does not fit all, and most “FedRAMP in a box” solutions are not customized to your specific organizational needs. A blend of foundational IaC and automation with customizations made for the specific needs of the application is the best approach ensuring compliance and success on the FedRAMP journey.

# FEDRAMP PHASES AND EXPECTED TIMELINE

A FedRAMP project can be divided into two distinct phases: pre-assessment and assessment. Each phase has its own set of activities and is marked by the completion of an initiation request on the cloud system to the FedRAMP Program Management Office (PMO).




## Phase 1-2 | Pre-Assessment

The pre-assessment phase is where the FedRAMP submission package is prepared and created. It includes the following steps:

1. Verifying system boundary definitions
2. Evaluating critical control implementation
3. Educating stakeholders about final assessment requirements, timelines, and likelihood of ATO by chosen sponsor
4. Determining whether the cloud service offering meets the FedRAMP requirements to become "FedRAMP Ready." All FedRAMP requirements must be met and FedRAMP will not waive any requirements, such as:

   - Are FIPS 140-2 validated cryptographic modules consistently used where cryptography is required?
   - Can the system fully support user authentication via agency common access card (CAC) or personal identity verification (PIV) credentials?
   - Can you consistently remediate high vulnerabilities within 30 days, moderate vulnerabilities within 90 days, and low vulnerabilities within 180 days?
   - Is the system operating at digital identity level 2 or higher?
   - Do you and the system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements?
   - Does the system's external DNS solution support DNS security (DNSSEC) to provide origin authentication and integrity verification assurances?

## **Phase 1-2** | Pre-Assessment (cont.)

5. Downloading FedRAMP templates
6. Deciding if you will submit through FedRAMP JAB or obtain a federal agency sponsor. This decision will have a significant impact on the project timeline as elaborated upon in the assessment phase.
7. Submitting the documents for 3PAO review upon completion of the required FedRAMP documentation. The 3PAO examines the most critical security controls and works with you to identify any necessary updates to FedRAMP documentation, which starts the FedRAMP assessment phase (Phase 3).

## **Phase 3** | Assessment

The FedRAMP assessment phase includes several steps to ensure that the system meets the necessary security controls and requirements. These steps include:

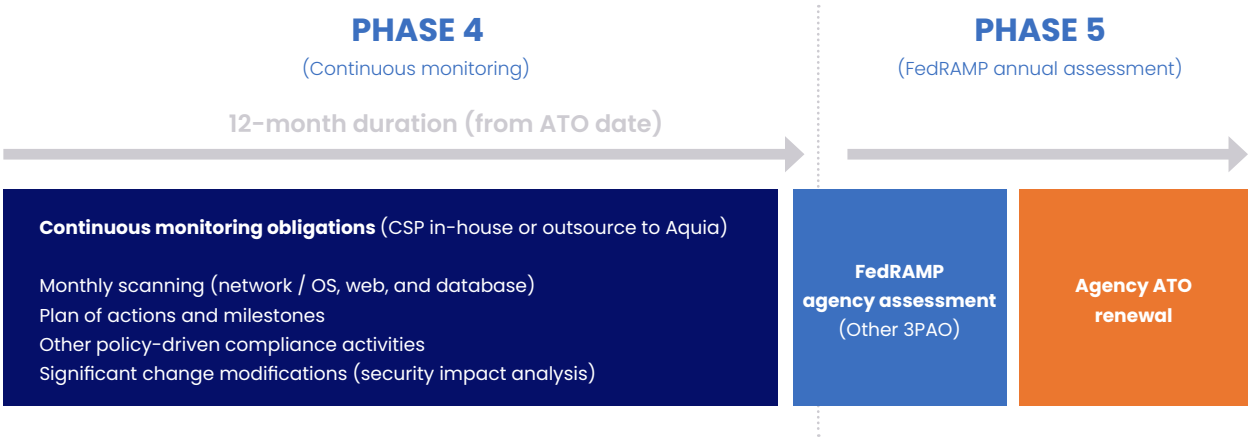
1. Security controls assessment against NIST SP 800-53 Revision 5 (scope dependent on the system impact level of high, moderate, or low). This includes a review of your policies, procedures, and SSP, interviews with your personnel to determine control implementation and effectiveness, and testing and artifact collection to ensure that the required FedRAMP controls and control parameters are met.
2. Vulnerability scanning of all operating systems, network devices, infrastructure, databases, and web applications.
3. Penetration testing to identify any potential vulnerabilities or weaknesses in the system.
4. Source code review, which is required for the initial FedRAMP assessment.

The timeframe of the assessment phase is mainly dictated by the selected path and your readiness to respond to comments throughout each stage. The biggest difference between the two is the level of security package review. Generally, the timeframes for each authorization type are:

- Agency ATOs: One to four or more months
- JAB P-ATOs: Three to nine or more months

Once the assessment is completed, your security package will be listed within the FedRAMP repository for federal agencies to be able to download and review.

# POST-AUTHORIZATION




## Phase 4 | Continuous Monitoring (ConMon)

Once the initial authorization has been obtained, the process of continuous monitoring commences to ensure that the security controls that have been implemented within the system remain effective and adequate over time. This process is critical in maintaining the FedRAMP ATO and it requires regular monitoring and assessment of the security controls in place to detect any new threats or changes that may occur within the system or its environment.

To maintain authorization, it is essential to demonstrate that the security posture of the cloud service offering remains acceptable to FedRAMP. Continuous monitoring provides federal agencies using cloud services with a method for detecting changes to the system's security posture and making risk-based decisions.

In general, the annual activities involved in maintaining authorization include: a thorough review of security policies, planning activities, and security procedures and processes to ensure they are up-to-date and relevant. Incident handling activities, including the maintenance of incident records, reporting of incidents, and timely response to incidents. Regular scanning results from infrastructure, operating systems, web applications, and databases to detect any vulnerabilities or potential threats. Monitoring any changes to the system's security posture that may occur due to changes in hardware or software on the cloud service offering or due to the discovery and provocation of new exploits.

It is important to note that the process of continuous monitoring is not a one-time event, it is ongoing and requires constant attention.

## Phase 5 | Annual Assessment

The FedRAMP ConMon program requires annual assessments for FedRAMP-authorized CSPs. These assessments must comply with the FedRAMP Annual Assessment Guidance; failure to do so may result in escalation actions. The scope of controls for each annual assessment includes:

- FedRAMP-identified critical controls
- Controls that have changed since the last assessment
- Approximately one-third of the remaining applicable controls

The CSP and 3PAO may propose the scope, but the authorizing organization must approve it and may require additional controls. It is recommended that each control be tested regularly, as most leveraging agencies prefer this as well. This ensures that no control becomes extremely dated.

*Reference: FedRAMP Annual Assessment Guidance*

# Accelerate your time to FedRAMP Authorization with Aquia Zero to FedRAMP

**Zero to FedRAMP (Z2F)** is an innovative accelerator program designed to help technology organizations navigate the National Institute of Standards and Technology (NIST) 800-53 compliance journey with confidence, speed, and agility.

Our team combines certified cloud security engineers with seasoned governance, risk, and compliance (GRC) specialists to help our customers address both technical and process gaps quickly and correctly.

We work closely with Datalock, our trusted partner and FedRAMP third-party assessment organization (3PAO), to ensure you are prepared to face your FedRAMP assessments with confidence.

## The Aquia Z2F Difference

We are a service-disabled veteran-owned small business (SDVOSB) trusted by cybersecurity innovators within the federal government and beyond. We pair the industry, technological, and policy expertise that our customers need with the strategy, advice, and thought leadership they desire.

### Top security engineers at your fingertips

Our cloud security engineers leverage their experience at some of the world's top tech companies, like Apple and Amazon Web Services, to provide you with the technical guidance and hands-on support you need to make your FedRAMP authorization process seamless.

### Artifact generation as needed

Aquia's Z2F governance, risk, and compliance (GRC) specialists have decades of experience developing documentation and artifacts and will generate these as needed for your team's review.

### Continuous monitoring you can trust

FedRAMP compliance requires continuous monitoring of many critical NIST 800-53 controls. You can entrust us with this important ongoing task so you can focus on competing priorities.

### Complimentary access to Aquia's GRC Platform

Aquia maintains a robust GRC platform that offers artifact storage, dashboards, and audit reports at the click of a button. Our Z2F customers receive complimentary access to the platform.

### Custom AWS Landing Zone features for FedRAMP

We take Amazon Web Services (AWS) Landing Zone to the next level for regulated environments, with additional custom features. Z2F customers benefit from Aquia's extensive library of automation designed to quickly deploy secure FedRAMP-ready cloud environments.

### No third-party hosting

We stand up FedRAMP controls within your cloud environment, allowing you to maintain ownership and control of your data and reducing your risk.

---

Aquia

**To learn more about how Aquia Z2F can help you navigate the FedRAMP authorization process, contact us at fedramp@aquia.us.**

^
Back to top

## About Aquia

Aquia Inc. is a Service-Disabled Veteran-Owned Small Business committed to Securing the Digital Transformation®. Aquia is a developer-centric company founded in 2021 by military veterans with a passion for the intersection of security and velocity and decades of experience driving transformational change across public sector, enterprise, and top-tier technology companies. At Aquia, we value trust, accountability, transparency, and diversity; and we've built these tenants into the DNA of our company.
For more information, visit www.aquia.us.