FedRAMP & Pursuing a FedRAMP Agency Authorization

The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. government-wide program created to accelerate the adoption of secure cloud services across the Federal government by ensuring that Cloud Service Providers (CSPs) meet the stringent security requirements for Federal Agencies.

Cloud Service Offerings (CSOs) are categorized into one of **three impact levels** (Low, Moderate, High) and across three security objectives (Confidentiality, Integrity, and Availability) based on their **FIPS 199 Data Categorization.**

The **security categories** are based on the potential impact that certain events would have on an organization's ability to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

Key FedRAMP Considerations

1 Partnering with a sponsoring agency is required to achieve a FedRAMP Agency ATO for reuse by Federal Agencies.

2 Once authorized, cloud service providers must submit monthly security reports to demonstrate ongoing compliance.

3 The process for system development, documentation, assessment, and authorization can take 8-24+ months to complete.

4 FedRAMP authorization creates opportunities to sell to other federal agencies and is often part of solicitations for Federal contracts.

5 A FedRAMP recognized 3PAO is required to conduct assessments to obtain FedRAMP authorization.

4.0 FedRAMP Designations

FedRAMP defines three different designations for CSOs:

FedRAMP Ready: A designation provided to CSOs which indicates that a 3PAO attests to a CSO's security capabilities, and that a FedRAMP Readiness Assessment Report (RAR) has been reviewed and deemed acceptable by the FedRAMP PMO. FedRAMP Ready indicates a CSO has a high likelihood of successfully completing an initial FedRAMP authorization with the Joint Authorization Board (JAB) or a federal agency.

FedRAMP In Process: A designation provided to CSOs that are actively working toward a FedRAMP authorization with either the JAB or a federal agency. For updates, agencies can either contact the cloud provider via the email address provided on the CSO's FedRAMP Marketplace page, or reach out directly to the FedRAMP PMO via intake@fedramp.gov.

FedRAMP Authorized: A designation provided to CSOs that have successfully completed the FedRAMP authorization process with the JAB or a federal agency. FedRAMP Authorized CSOs are available for government-wide reuse.

The FedRAMP Agency Authorization Process

01 Preparation

02 Authorization

03 Continuous Monitoring

Readiness Assessment
(Optional, but highly recommended)

- RAR Development
- FedRAMP PMO Review of RAR
- Remediation (if needed)
- ✔ FedRAMP Marketplace Designation - Ready

Pro-Authorization

- Partnership Establishment
- Authorization Planning
- Kick-off Meeting
- ✔ FedRAMP Marketplace Designation - In Process

Full Security Assessment

- Security Authorization Package (SSP, SAP, SAR, POA&M)*

Agency Authorization Process

- Agency Review of Security Authorization Package
- SAR Debrief
- Remediation
- Agency Final review
- Agency Issues ATO
- FedRAMP PMO Review
- Remediation (if needed)
- ✔ FedRAMP Marketplace Designation - Authorized

Post Authorization

- Ongoing Continuous Monitoring Deliverables
- Annual Assessment

*   *The full security assessment may be prepared in advance of the authorization phase, or completed during the authorization phase. This is dependent on the agency's review approach.*

The Prescient 3PAO Advantage:

- Utilizing FedRAMP's **"Do Once – Use Many"** approach, we enable CSPs to reuse successful assessment results across various federal agencies, significantly reducing redundancy and effort.

- Our adherence to the latest FedRAMP templates and guidance ensures your compliance strategies are **always in sync with current federal standards.**

- We can produce a **FedRAMP Readiness Assessment Report (RAR)** or a complete **FedRAMP Security Authorization Report (SAR)** package. A complete security authorization package includes the Security Assessment Plan (SAP), Security Assessment Report (SAR) with all appendices, and a penetration test report.

- Our comprehensive approach includes **compliance configuration and vulnerability scan analysis, penetration testing, and manual control testing** for initial and annual assessments.

- We can assist in completing and maintaining your **Plan of Action & Milestones (POA&M)** monthly, ensuring continuous compliance and monitoring throughout your authorization.