AGENCY AUTHORIZATION

BEST PRACTICES FOR CSPs

FedRAMP

The Agency Authorization process is the most popular route for CSPs to take when working toward a FedRAMP Authorization. In fact, 65 percent of authorized CSPs have an Agency ATO. The Agency Authorization affords a CSP to work one-on-one with one Agency through the review process; the JAB Authorization requires a CSP to work with three Agencies: DoD, DHS, and GSA. The Agency Authorization project workflow/stage gates can also be customized based on the specific needs and available resources of the Agency and CSP.

The following steps detail a recommended workflow from the FedRAMP PMO in establishing, planning, and completing the FedRAMP authorization process with an Agency.

1 ESTABLISH A PARTNERSHIP WITH AN AGENCY

A. Identify an Agency that has a vested interest in your cloud service offering (CSO) to work with for the FedRAMP Authorization.

TIP: Ideal Agency partners tend to be those who are already using your cloud offering or have procured your service for future use. Keep in mind, a FedRAMP Agency Authorization is required prior to an Agency transitioning their production data to your cloud environment.

TIP: If an Agency is currently using an "on-premise" version of your product and there is interest in moving to the cloud, then this could also be a viable candidate to be your partner Agency.

TIP: Agencies could be reluctant to perform the initial "sponsoring" authorization because of the following misconceptions:

MYTH: The level of effort an Agency must perform to issue an authorization is too great.

FACT: CSPs seeking a FedRAMP authorization perform the heavy lift to ensure the system is risk-acceptable and provide all the FedRAMP deliverables to the Agency partner for review, feedback, and risk acceptance. Agencies are in a "review mode" role.

MYTH: The initial Agency is accepting the risk of the system/cloud service for the entire government.

FACT: The initial authorization with an Agency is NOT an authorization for the entire Federal Government. The Agency Authorizing Official (AO) can only authorize the use of the system by their Agency. Additional Agencies that wish to use the service must perform their own risk analysis and issue their own independent authorization that covers their Agency's use of the system. Please ensure the FedRAMP PMO has a copy of all ATO letters.

B. To become "In Process" with an Agency, the FedRAMP PMO must be in receipt of an e-mail from an AO or a FedRAMP PMO-approved designee stating they are actively engaging with the CSP and plan on granting an ATO that meets FedRAMP requirements within 12 months. Additionally, your CSO must meet one of 4 requirements highlighted in our "Obtaining an In Process Designation" policy.

C. Contact the PMO at **info@fedramp.gov** for the following:

- Complete and submit FedRAMP application.
- Obtain OMB MAX Accounts.

2 PLAN AUTHORIZATION

A. Complete FedRAMP **Training**, including the mandatory training: **FedRAMP System Security Plan (SSP) Required Documents (200-A)**.

B. Confirm your resources dedicated to the authorization process. At a minimum, this should include:

- One (1) technical writer
- One (1) technical SME
- One (1) project manager

TIP: Elect a Third Party Assessment Organization (3PAO). A list of FedRAMP-accredited 3PAOs is located on our website.

TIP: If you need extra assistance to complete the various FedRAMP deliverables, you may engage a consultant to assist. This entity must be independent of your 3PAO.

C. Transparency is key. Provide the Agency with updates to the notional authorization timeline given resources, time constraints, etc.

D. Determine the cadence of review of the security documentation (e.g., all at once, or "just in time").

3 DEVELOP YOUR SECURITY PACKAGE

A. Complete and submit the security documentation (System Security Plan (SSP) and attachments) per the agreed upon project plan.

B. Address any questions or comments throughout the process with your partner Agency in a timely manner - the FedRAMP PMO can assist when useful.

4 ASSESS YOUR SYSTEM

A. Coordinate with your 3PAO to develop a Security Assessment Plan (SAP) based on your approved SSP.

B. Once complete, provide the SAP to your partner Agency for review via OMB MAX.

C. Complete testing and review the Security Assessment Report (SAR).

D. Prepare a POA&M and submit the SAR to the Agency for review via OMB MAX.

5 ACHIEVE AN AUTHORIZATION

A. Once you receive an Authorization to Operate (ATO) letter from your partner Agency, ensure the finalized package and letter are uploaded to OMB MAX. This package includes:

- SSP + Attachments, SAP, SAR, POA&M, and ATO letter.

B. Notify the FedRAMP PMO that you have received an authorization and ensure your finalized package is uploaded to OMB MAX.

C. The FedRAMP PMO will perform a cursory review post ATO to ensure all FedRAMP requirements have been met and will confirm the CSO is FedRAMP Authorized.

D. The FedRAMP marketplace will be updated accordingly with the latest status.

The FedRAMP PMO regularly speaks with Agencies and CSPs in the process of finalizing sponsorship to address any questions or concerns your partner Agency has about their authorization roles and responsibilities.

The PMO has resources for you to use, including sample project plans and documents highlighting roles and responsibilities throughout the process.