FedRAMP Sponsoring Agency’s Roles & Responsibilities

EXECUTIVE SUMMARY

Broadly speaking, the agency sponsor’s role/responsibility in the ATO process includes:

- Indicating that they want to utilize the cloud solution
- Ensuring that the agency leadership is on board with the plan and there will be no major roadblocks in adoption once authorization is achieved
- Define any agency-specific security requirements
- Obtain OMB MAX accounts to review supporting documentation throughout the authorization process
- Thoroughly review all assessment packages and security deliverables
- Have an open line of communication with the CSP, 3PAO, and FedRAMP PMO including attending some formalized meetings
- Accept risk after careful consideration of all security deliverables
- After ATO is achieved, they must also review subsequent continuous monitoring reports on a monthly/annual basis

The program was designed so that sponsoring agencies are mainly in “review mode” for most of the authorization process.

WHAT DOES IT MEAN TO BE AN INITIAL AGENCY PARTNER?

An Initial Agency Partner or initial authorizing agency refers to the **first** agency to grant an Authority to Operate (ATO) using FedRAMP standards and baselines for the Cloud Service Offering (CSO). Some stakeholders use the term "Agency Sponsor.” FedRAMP does not recognize the concept of an agency sponsor because the ATO granted by the initial authorizing agency is not a government-wide risk acceptance. As described in FedRAMP's Reuse Quick Guide, OMB Circular A-130 requires agencies to individually authorize operation of an information system and to explicitly accept the risk. Each agency that wishes to use the CSO will conduct its own risk review of the authorization package and grant its own ATO.

IS THERE AN ADDITIONAL LEVEL OF EFFORT ASSOCIATED WITH BEING THE INITIAL AUTHORIZATION AGENCY?

It depends on the quality of the authorization package. Because the initial authorizing agency is the first agency to review the authorization package, the process for getting to an informed risk-based decision may take longer and require more effort if there are aspects of the authorization package that are unclear, incomplete, inaccurate, or inconsistent.

The FedRAMP Program Management Office (PMO) provides guidance to Cloud Service Providers (CSPs) and Third Party Assessors (3PAOs) on how to deliver a high quality authorization package, but if the agency team is unable to determine the actual security posture of the Cloud Service Offering (CSO) due to poor quality, the agency will provide feedback. The feedback may result in modifications to the package deliverables and/or additional testing, and additional review cycles.

IS THE INITIAL AUTHORIZATION AGENCY RESPONSIBLE FOR PERFORMING CONTINUOUS MONITORING OVERSIGHT ON BEHALF OF OTHER LEVERAGING AGENCIES?

No. It is not the initial authorizing agency’s responsibility to conduct Continuous monitoring (ConMon) oversight on behalf of all other agencies. OMB Circular A-130 requires federal agencies to implement the Risk Management Framework (RMF) described in NIST SP 800-37. The RMF process includes a Monitor step. The purpose of this step is to maintain ongoing situational awareness about the security posture of the system in support of risk management decisions. Each agency that issues an ATO or ATU for a cloud offering must review the Cloud Service Provider’s (CSP’s) ConMon activities to ensure the security posture remains sufficient for its own use and supports an ongoing authorization. This includes reviewing the monthly Plan of Action and Milestones (POA&M), approving deviation requests and significant change requests, and reviewing the results of the annual assessment. The FedRAMP Program Management Office (PMO) encourages CSPs who have more than one customer agency to streamline the ConMon process and potentially minimize duplicative efforts in a way that helps each agency still perform their due diligence related to ConMon. The PMO developed a recommended Collaborative ConMon approach. This approach is described in the Guide for Multi-Agency Continuous Monitoring. Collaborative ConMon benefits agencies by allowing them to share responsibility for ConMon oversight, and it benefits the CSP by creating a central forum for addressing questions and achieving consensus related to deviation requests, significant change requests and the annual assessment - versus having to coordinate with each agency separately.

ADVANTAGES OF ISSUING AN AGENCY FEDRAMP ATO:

- Allows the Agency to align the FedRAMP requirements with existing Agency requirements
- No additional expense to serving as a sponsor – CSP pays for assessment and prepares all documentation, and the Agency reviews
- Authorizes only for Agency data/use and not for all of government

CSPs make the authorization process easy for Agencies; **Agencies are in "review mode."**

AGENCY ROLES & RESPONSIBILITIES SUMMARY CHART:

Authorization Phase	Sponsoring Agency Roles & Responsibilities
Partnership Establishment	• Determine need for services
Authorization Planning and Security Package Development	• Follow Guidance for In Process Requirements Listed in FedRAMP Marketplace Designations for Cloud Service Providers • Obtain OMB MAX Accounts • Coordinate with CSP to define Agency/ CSP security roles and responsibilities • Identify Agency-specific requirements (e-AUTH, + controls) • Understand and agree to Agency responsible controls • Review and approve SSP and attachments via OMB MAX
Assessment	• Review and approve SAP/SAR/POA&M via OMB MAX
Authorization and FedRAMP Compliance	• Issue an ATO to the CSP service/system ○ If ATO is for a Saas/PaaS, ATO applies to entire "stack" ○ ATO is for Agency data/use only, not for all of government • Notify FedRAMP of final package and ATO letter
Continuous Monitoring	• Review and approve CSP monthly continuous monitoring deliverables • Take responsibility for conducting review of annual assessment materials
FedRAMP ATO Package Reuse Interest	• Review FedRAMP Marketplace to determine if cloud service is already FedRAMP Authorized • Complete FedRAMP Access Request Form for each CSP of interest and email form to info@fedramp.gov
Package Review	• Conduct risk analysis by reviewing CSP authorization package • Determine if risk posture is acceptable • Determine if CSP needs to meet additional requirements for Agency mission/business needs
Approve and Authorize	• Approve CSP package for authorization • Issue an ATO for CSP service/system • Send ATO letter to PMO: info@fedramp.gov
Continuous Monitoring	• Review CSP monthly continuous monitoring deliverables • Take responsibility for conducting review of annual assessment materials

"AGENCY TIPS" ACCORDING TO THE FEDRAMP PMO:

- Peruse Key Agency Documents (https://www.fedramp.gov/documents/) for more information and guidance on Agency authorizations.
- Set up a schedule with CSP to coordinate and manage milestones for authorization efforts
- Conduct a kickoff meeting and establish expectations with CSP about deliverables and roles and responsibilities for FedRAMP authorization (internal review process, timeline of events, uploading of package/documentation to OMB MAX, notifications to FedRAMP, etc.).
- Request and review CSP security artifacts/documentation to enhance understanding of CSP policies and procedures
- Conduct informal reviews with CSP to ensure CSP practices are consistent with Agency expectations.
- Work with CSP to ensure Agency roles and responsibilities for security controls are clear/reasonable.
- Engage the FedRAMP PMO (info@fedramp.gov), when needed, to provide clarification on FedRAMP authorization process/procedures.
- Establish expectations with CSP for Continuous Monitoring (scanning; agency review of scan reports; approval for POA&Ms, changes, and deviations, etc.)

JAB P-ATO VS AGENCY ATO RESPONSIBILITY COMPARISON

NO.	Description	JAB P-ATO	Agency ATO
1.	Package is reviewed for completeness, accuracy, and acceptable level of risk by FedRAMP PMO, and JAB (DOD, DHS, and GSA CIOs)	X	
2.	Package is reviewed for completeness only		X
3.	Authorizing agency reviews package for acceptable level of risk	X	X
4.	Authorizing agency reviews package to determine if additional agency-specific controls and delta assessment is required	X	X
5.	Grants authorization and accepts risk		X

RESOURCES

Date	Resource Title	Type
N/A	FAQ Page	Website
N/A	AGENCY AUTHORIZATION ROLES & RESPONSIBILITIES	Guide