

FedRAMP AGENCY AUTHORIZATION ROLES & RESPONSIBILITIES FOR FEDRAMP CSPS & AGENCIES

Date: December 5, 2017



CLAUDIO BELLOLI
PROGRAM MANAGER - CYBERSECURITY & JAB

JOHN HAMILTON
PROGRAM MANAGER - OPERATIONS



FedRAMP AGENCY AUTHORIZATION PROCESS – INITIAL AUTHORIZATION

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.”

PHASE	AGENCY	CSP	FedRAMP
Partnership Establishment	<ul style="list-style-type: none">▪ Determine need for services	<ul style="list-style-type: none">▪ Offer services that meet the Agency’s needs	<ul style="list-style-type: none">▪ Assist Agencies and CSPs in identifying potential partnerships▪ Provide overview of FedRAMP and application
Authorization Planning and Security Package Development	<ul style="list-style-type: none">▪ Follow FedRAMP Requirements for Obtaining an In Process Designation policy▪ 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	<ul style="list-style-type: none">▪ Complete FedRAMP training▪ Complete and submit FedRAMP Application to info@fedramp.gov▪ Obtain OMB MAX Accounts▪ Complete SSP and attachments (CSP may engage a “consultant” for assistance) and provide to Agency via OMB MAX▪ Engage 3PAO for security testing▪ Apply SSP and attachments feedback from Agency▪ Provide FedRAMP notional authorization schedule for FedRAMP dashboard	<ul style="list-style-type: none">▪ Update FedRAMP Dashboard with CSP and notional ATO timeline▪ Grant Agency permanent access to CSP documents in OMB MAX▪ Provide ad-hoc/customized support
Assessment	<ul style="list-style-type: none">▪ Review and approve SAP/SAR/POA&M via OMB MAX	<ul style="list-style-type: none">▪ Coordinate with 3PAO to develop SAP based on approved SSP▪ Provide SAP for Agency review via OMB MAX▪ Complete testing and review SAR▪ Prepare POA&M and submit SAR to Agency for review via OMB MAX	<ul style="list-style-type: none">▪ Assist Agency and CSP to answer questions and address concerns as necessary
Authorization and FedRAMP Compliance	<ul style="list-style-type: none">▪ Issue an ATO to the CSP service/system<ul style="list-style-type: none">○ 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	<ul style="list-style-type: none">▪ Ensure finalized package and ATO Letter is uploaded to OMB MAX<ul style="list-style-type: none">○ SSP, SAP, SAR, POA&M, and ATO letter to PMO○ Notify FedRAMP PMO	<ul style="list-style-type: none">▪ Review package to ensure FedRAMP compliance (Agency ATO Report)▪ Meet with the Agency and CSP to discuss Agency ATO Report▪ Update CSP status on FedRAMP Dashboard to “FedRAMP Authorized”
Continuous Monitoring	<ul style="list-style-type: none">▪ Review and approve CSP monthly continuous monitoring deliverables▪ Take responsibility for conducting review of annual assessment materials	<ul style="list-style-type: none">▪ Submit monthly continuous monitoring deliverables▪ Coordinate with 3PAO to conduct annual assessment and update any processes, procedures, and policies as necessary	<ul style="list-style-type: none">▪ Provide continuous monitoring guidance to Agencies



FedRAMP AGENCY AUTHORIZATION PROCESS – RE-USED AUTHORIZATION

PHASE	AGENCY	CSP	FedRAMP
FedRAMP ATO Package Reuse Interest	<ul style="list-style-type: none">Review FedRAMP Marketplace to determine if cloud service is already FedRAMP AuthorizedComplete FedRAMP Access Request Form for each CSP of interest and e-mail form to info@fedramp.gov	<ul style="list-style-type: none">Offer services that meet Agency needsEstablish relationship with Agency	<ul style="list-style-type: none">Assist Agencies and CSPs in identifying potential partnershipsGrant access to CSP authorization packages for review upon Agency request
Package Review	<ul style="list-style-type: none">Conduct risk analysis by reviewing CSP authorization packageDetermine if risk posture is acceptableDetermine if CSP needs to meet additional requirements for Agency mission/business needs	<ul style="list-style-type: none">Address any additional Agency requirements as neededProvide any additional information needed for the Agency to complete their review	<ul style="list-style-type: none">Maintain the repository (OMB MAX) of all FedRAMP Authorized CSPs
Approve and Authorize	<ul style="list-style-type: none">Approve CSP package for authorizationIssue an ATO for CSP service/systemSend ATO letter to PMO: info@fedramp.gov	<ul style="list-style-type: none">Ensure complete package is maintained in repository	<ul style="list-style-type: none">Grant permanent access to CSP documentation and continuous monitoring deliverables once ATO is issuedAdd Agency ATO to CSP information dashboard
Continuous Monitoring	<ul style="list-style-type: none">Review CSP monthly continuous monitoring deliverablesTake responsibility for conducting review of annual assessment materials	<ul style="list-style-type: none">Submit monthly continuous monitoring deliverablesCoordinate with 3PAO to conduct annual assessment and update any processes, procedures, and policies as necessary	<ul style="list-style-type: none">Provide continuous monitoring guidance to Agencies



AGENCY TIPS

- Peruse Key Agency Documents (<https://www.fedramp.gov/resources/documents-2016/>) 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.)

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