FedRAMP AGENCY AUTHORIZATION ROLES & RESPONSIBILITIES FOR FEDRAMP CSPs & AGENCIES

December 5, 2017

FedRAMP

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	▪ Determine need for services	▪ Offer services that meet the Agency's needs	▪ Assist Agencies and CSPs in identifying potential partnerships ▪ Provide overview of FedRAMP and application
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	▪ 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	▪ 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	▪ Review and approve SAP/SAR/POA&M via OMB MAX	▪ 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	▪ Assist Agency and CSP to answer questions and address concerns as necessary

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
		▪ Ensure finalized package and ATO Letter is uploaded to OMB MAX
		  ○ SSP, SAP, SAR, POA&M, and ATO letter to PMO
		  ○ Notify FedRAMP PMO
			▪ 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	▪ Review and approve CSP monthly continuous monitoring deliverables ▪ Take responsibility for conducting review of annual assessment materials	▪ Submit monthly continuous monitoring deliverables ▪ Coordinate with 3PAO to conduct annual assessment and update any processes, procedures, and policies as necessary	▪ Provide continuous monitoring guidance to Agencies

FedRAMP AGENCY AUTHORIZATION PROCESS – RE-USED AUTHORIZATION

PHASE	AGENCY	CSP	FedRAMP
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 e-mail form to info@fedramp.gov	▪ Offer services that meet Agency needs ▪ Establish relationship with Agency	▪ Assist Agencies and CSPs in identifying potential partnerships ▪ Grant access to CSP authorization packages for review upon Agency request
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	▪ Address any additional Agency requirements as needed ▪ Provide any additional information needed for the Agency to complete their review	▪ Maintain the repository (OMB MAX) of all FedRAMP Authorized CSPs
Approve and Authorize	▪ Approve CSP package for authorization ▪ Issue an ATO for CSP service/system ▪ Send ATO letter to PMO: info@fedramp.gov	▪ Ensure complete package is maintained in repository	▪ Grant permanent access to CSP documentation and continuous monitoring deliverables once ATO is issued ▪ Add Agency ATO to CSP information dashboard
Continuous Monitoring	▪ Review CSP monthly continuous monitoring deliverables ▪ Take responsibility for conducting review of annual assessment materials	▪ Submit monthly continuous monitoring deliverables ▪ Coordinate with 3PAO to conduct annual assessment and update any processes, procedures, and policies as necessary	▪ Provide continuous monitoring guidance to Agencies

FedRAMP AGENCY AUTHORIZATION PROCESS – AGENCY TIPS

AGENCY TIPS

- 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.)

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