



FedRAMP Compliance

All Federal agencies must use the FedRAMP process for doing security assessments, authorizations, and continuous monitoring of cloud services. Agencies must validate compliance with ALL of their cloud services through the FedRAMP PMO. This applies to ALL deployment models (public, private, hybrid, community) and delivery models (infrastructure, platform, software).

There are five requirements for ensuring a cloud system is FedRAMP compliant:

- 1) The agency has granted an Authority to Operate (ATO) to the cloud system
- 2) The system addresses the FedRAMP security control requirements
- 3) The system security package has been created using the required FedRAMP templates
- 4) The system has been assessed by an independent assessor
- 5) A completed security assessment package is in the FedRAMP secure repository for public, hybrid, and community clouds.

Types of FedRAMP Compliance

There are three ways that cloud services can be considered FedRAMP compliant:

1. JAB Provisional Authorizations (JAB P-ATOs)
Cloud systems with a FedRAMP P-ATO path have undergone a rigorous technical review by the FedRAMP PMO, been assessed by a FedRAMP accredited 3PAO, and received a P-ATO from the DHS, DOD, and GSA CIOs.
2. Agency FedRAMP Authorizations (A-ATOs)
Cloud systems listed under the Agency Authorization have worked directly with a customer agency to achieve a FedRAMP compliant ATO that has been verified by the FedRAMP PMO.
3. CSP Supplied Packages
Cloud systems listed under the CSP Supplied Package path have submitted to the FedRAMP PMO a completed Security Assessment Package (SAP) that has been assessed by a FedRAMP accredited 3PAO.

Validation of Agency FedRAMP Compliance

For an agency to validate the cloud system they use is FedRAMP compliant, they must work with the FedRAMP PMO. Agencies must submit the appropriate materials to the FedRAMP PMO for validation through info@FedRAMP.gov. There are two key elements that must be validated by the FedRAMP PMO:

1. Agency ATO letters
For all cloud services an agency uses, the FedRAMP PMO must receive an ATO letter that details the agency's use of that cloud service, details that the cloud service meets the FedRAMP requirements, any associated terms and conditions for the maintenance of the authorization, and it must be signed by an agency authorizing official. A template

for an agency ATO letter is available on www.FedRAMP.gov. Use of this template is not required, but it does contain the minimum information that should be included within any ATO letter provided to the FedRAMP PMO.

2. Security Authorization Packages

For all Multi-Tenant Clouds, the FedRAMP security authorization packages must be validated by the FedRAMP PMO. The FedRAMP PMO validates these based on whether a cloud system’s authorization package can be re-used by other agencies. The easiest way to distinguish this is by defining clouds as either multi-tenant (covering public, hybrid, and community clouds) or a private cloud.

- Multi-Tenant Clouds: For multi-tenant clouds, the FedRAMP PMO must review the security package completed by an agency for completeness and compliance with the FedRAMP Security Assessment Framework (SAF). The FedRAMP PMO then lists these CSPs on FedRAMP.gov and makes the security authorization packages available for re-use by other agencies through the FedRAMP secure repository.
- Private Clouds: For private clouds, these clouds will not be able to be re-used by other Federal agencies and will not be held within the FedRAMP secure repository unless requested by a Federal agency for the FedRAMP PMO to do so. In this case, an Agency ATO letter validated by the FedRAMP PMO, will represent sufficient validation of a completed security authorization package.

Table 1: Summary of Validation of Agency FedRAMP Compliance by Type of Compliance

Type of Compliance	Multi-Tenant Clouds (public, hybrid, community)	Private Clouds (singular agency use)
JAB P-ATO	1. Agency ATO letter on file with the FedRAMP PMO. <i>No validation of a security authorization package is needed because the packages are completed by the JAB.</i>	1. N/A 2. The JAB will not authorize private cloud solutions.
Agency ATO	1. Agency ATO letter on file with the FedRAMP PMO. 2. CSP package is available for leveraging within the FedRAMP secure repository. <i>If the agency is the first agency to use this CSP, then the agency must submit the authorization package for review with the ATO letter.</i>	1. Agency ATO letter on file with the FedRAMP PMO.
CSP Supplied Path	1. N/A <i>If an agency is using a CSP in this category, then an ATO letter should be on file with the FedRAMP PMO and the CSP would then be considered an Agency ATO.</i>	1. N/A <i>For private clouds to receive FedRAMP compliance, they would need to have an agency customer.</i>