Federal Risk and Authorization Management Program (FedRAMP) United States

Microsoft was granted FedRAMP P-ATOs and ATOs.

Microsoft and FedRAMP

Microsoft government cloud services, including Azure Government, Office 365 U.S. Government, and Dynamics 365 U.S. Government, meet the demanding requirements of the US Federal Risk and Authorization Management Program (FedRAMP), enabling US federal agencies to benefit from the cost savings and rigorous security of the Microsoft Cloud.

Azure and Azure Government have earned a P-ATO from the Joint Authorization Board (JAB)

The JAB is the primary governance and decision-making body for FedRAMP. Representatives from the Department of Defense, the Department of Homeland Security, and the General Services Administration serve on the board. The board grants a P-ATO to cloud service providers (CSPs) that have demonstrated FedRAMP compliance.

Azure maintains a P-ATO at the Moderate Impact Level. (Azure was the first public cloud with infrastructure and platform services to receive a P-ATO.) The JAB has also granted Azure Government a P-ATO at the High Impact Level, the highest bar for FedRAMP accreditation, which authorizes the use of Azure Government to process highly sensitive data. The mandatory NIST 800-53 standards establish security categories of information systems—confidentiality, integrity, and availability—to assess the potential impact on an organization should its information and information systems be compromised. The FedRAMP audit of Azure and Azure Government included the Information Security Management System that encompasses infrastructure, development, operations, management, and support of in-scope services.

Once a P-ATO is granted, a CSP still requires an authorization—an ATO—from any government agency it works with. In the case of Azure, a government agency can leverage the Azure P-ATO in its own security authorization process and rely on it as the basis for issuing an Agency ATO that also meets FedRAMP requirements.

Dynamics 365 U.S. Government has received an ATO from HUD

Dynamics 365 U.S. Government was granted a FedRAMP Agency ATO at the High Impact Level by the Department of Housing and Urban Development (HUD). (Note that although the scope of the certification is limited to the Government Community Cloud, Dynamics 365 U.S. Government business and enterprise plans operate following the same set of stringent FedRAMP controls.)

Office 365, Office 365 U.S. Government have an ATO from DHHS. Office 365 U.S. Government Defense has a P-ATO from Defense Information Systems Agency (DISA)

Office 365 (Enterprise and Business plans) and Office 365 U.S. Government have a FedRAMP Agency ATO at the Moderate Impact Level from the Department of Health and Human Services (DHHS) Office of the Inspector General. Office 365 U.S. Government was the first cloud-based email and collaboration service to obtain this authorization.

Any customer wishing to deploy O365 U.S. Government Defense may use the DISA P-ATO to generate an Agency ATO to document their acceptance of O365.

Microsoft in-scope cloud services

- Azure and Azure Government: Learn more
  Note: The use of Azure Active Directory within Azure Government requires the use of components that are deployed outside of Azure Government on the Azure public cloud.
- Dynamics 365 U.S. Government: Learn more
- Intune
- Office 365 and Office 365 U.S. Government: Learn more
- Office 365 U.S. Government Defense
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

Audits, reports, and certificates

Microsoft is required to re-certify its cloud services each year to maintain its P-ATOs and ATOs. To do so, Microsoft must monitor and assess its security controls continuously, and demonstrate that it remains in compliance.

- Microsoft cloud services authorizations
- Microsoft FedRAMP Audit Reports

How to implement

- **Azure FEDRAMP Blueprint**
  Get help automating the deployment and configuration of Azure resources in a FedRAMP environment.
  Learn more
- **Improve security & compliance**
  Microsoft developed Control Companions to help you find Office 365 features that map to FedRAMP controls.
  User Guide and Control Companions

About FedRAMP

The US Federal Risk and Authorization Management Program (FedRAMP) was established to provide a standardized approach for assessing, monitoring, and authorizing cloud computing services under the Federal Information Security Management Act (FISMA), and to accelerate the adoption of secure cloud solutions by federal agencies.

The Office of Management and Budget now requires all executive federal agencies to use FedRAMP to validate the security of cloud services. (Other agencies have also adopted it, so it is useful in other areas of the public sector as well.) The National Institute of Standards and Technology (NIST) 800-53 sets the standard, and FedRAMP is the program that certifies that a CSP meets that standard.

CSPs desiring to sell services to a federal agency can take three paths to demonstrate FedRAMP compliance: earn a Provisional Authority to Operate (P-ATO) from the Joint Authorization Board (JAB); receive an Authority to Operate (ATO) from a federal agency; or work independently to develop a CSP Supplied Package that meets program requirements. Each of these paths requires a stringent technical review by the FedRAMP Program Management Office (PMO) and an assessment by an independent third-party organization that is accredited by the program.

FedRAMP authorizations are granted at three impact levels based on NIST guidelines—low, medium, and high. These rank the impact that the loss of confidentiality, integrity, or availability could have on an organization—low (limited effect), medium (serious adverse effect), and high (severe or catastrophic effect).

Frequently asked questions

Do Microsoft cloud services comply with the Federal Information Security Management Act (FISMA)?

FISMA is a federal law that requires US federal agencies and their partners to procure information systems and services only from organizations that adhere to FISMA requirements. Most agencies and their vendors that indicate FISMA compliance are referring to how they meet the controls identified by the NIST in Special Publication 800-53 rev 4. The FISMA process (but not the underlying standards themselves) was replaced by FedRAMP in 2011.

To whom does FedRAMP apply?

“FedRAMP is mandatory for federal agency cloud deployments and service models at the low and moderate risk impact levels.” Any federal agency that wants to engage a CSP may be required to meet FedRAMP specifications. In addition, companies that employ cloud technologies in products or services used by the federal government may be required to obtain an ATO.

Can I use Microsoft compliance in my agency’s authorization process?

Yes. You may use the certifications of Microsoft cloud services as the foundation for any program or initiative that requires an ATO from a federal government agency. However, you will need to achieve your own authorizations for components outside these services.

Additional resources

- FedRAMP Security Assessment Framework
- Get Authorized: Agency Authorization
- Microsoft Government Cloud