DRATA

The Cloud Service Provider's Guide to FedRAMP

Everything you need to prepare for (and pass) the FedRAMP authorization process.

Presented by Drata

drata.com

DRATA

Contents

What You Need To Know About FedRAMP **3**

What is FedRAMP? 3

Who Can Perform a FedRAMP Assessment? 4

How Long is FedRAMP Authorization Valid? 4

Benefits of FedRAMP Compliance 5

FedRAMP Compliance Challenges 5

Who Needs FedRAMP? **6**

ATOs: The 2 Paths for CSPs 6

Which ATO is Right For You? 7

FedRAMP Impact Levels 8

FedRAMP Authorization Process **9**

How To Attain JAB P-ATO Authorization 9

FedRAMP Connect 9

JAB P-ATO Authorization Process 10

How To Attain Agency A-ATO Authorization 13

A-ATO Authorization Process 13

Different Processes, Same Controls 16

FedRAMP Controls **17**

Get FedRAMP Authorized FAST by Automating Compliance **18**

DRATA

What You Need To Know About FedRAMP

If your organization provides cloud services and aims to supply any part of the U.S. Federal Government, FedRAMP is already on your radar.

Whether you're a global organization or a recent startup, attaining FedRAMP Authorization for your cloud services is far from straightforward. This guide will help you understand what FedRAMP is, where it came from, the purpose it serves, and—most importantly—how you can get FedRAMP authorized and begin supplying federal agencies.

What is FedRAMP?

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services. It provides a framework for Cloud Service Providers (CSPs) to ensure and prove services meet federal security requirements.

FedRAMP was created in 2011 by the Office of Management and Budget (OMB) and officially launched in 2012 by the General Services Administration (GSA). This followed the federal "Cloud First" initiative, which encouraged agencies to move data and workflows away from traditional on-premise systems and into the cloud. The stated purpose was:

> **To provide a cost-effective, risk-based approach for the adoption and use of cloud services to Executive departments and agencies."**

Before FedRAMP, federal agencies assessed the security of all technology partners, including CSPs, using the Federal Information Security Management Act (FISMA) of 2002. However, the combination of FISMA not being designed for cloud services and the inefficiency of agencies individually assessing vendors prompted the need for a cloud-specific framework.

> **Note:** FedRAMP has been referred to as "FISMA for the cloud," a description which is reasonably accurate as—like FISMA—it relies mainly on security controls laid out by NIST SP 800-53.

Who Can Perform a FedRAMP Assessment?

In the past, federal contractors were often allowed to self-assess cybersecurity readiness against the appropriate NIST framework. However, over time it became increasingly clear that many contractors were not holding themselves to the necessary standards.

FedRAMP was among the federal initiatives to require a verified third-party assessment for all contractors. In the years since FedRAMP launched, this approach has been expanded to other initiatives, including the DoD's Cybersecurity Maturity Model Certification (CMMC).

FedRAMP assessments can only be performed by accredited Third-Party Assessment Organizations (3PAOs). These organizations are assessed and authorized by the federal government to perform security assessments of cloud products and services.

How Long is FedRAMP Authorization Valid?

Originally, FedRAMP authorizations were valid for three years—after which, a CSP had to go through the full authorization process once again. This is no longer the case. Today, FedRAMP authorizations instead require annual assessment by an authorized 3PAO along with expanded self-reported continuous monitoring.

These are occasional exceptions, but in most cases, CSPs only have to go through the full authorization process once.

DRATA

Benefits of FedRAMP Compliance

There are several benefits to achieving FedRAMP compliance, including:

- **Work with federal agencies.** Since FedRAMP is mandatory for all Cloud Service Offerings (CSOs) used by federal agencies, CSPs can only do business with federal customers if they have the necessary FedRAMP authorizations.
- **Grow your federal customer base.** The FedRAMP Marketplace lists all CSOs that currently possess FedRAMP authorizations or are in the process of obtaining authorization. While a CSP may need to obtain further authorization to work with additional agencies, it's much easier to sell to federal agencies if you can demonstrate your CSO already meets the requirements.
- **Sell to other CSPs that have federal customers.** Many FedRAMP authorized CSPs have no direct federal customers. Instead, they need FedRAMP in order to work with other CSPs that do deal directly with federal agencies. Since these CSPs are required to choose cloud service suppliers that are FedRAMP authorized, having FedRAMP opens them up as a potential market for any FedRAMP authorized organization.
- **Establish confidence in your CSO.** FedRAMP is among the most prestigious cybersecurity credentials—not just because it enables CSPs to work with federal agencies, but because it signifies to other potential customers that a CSP can be trusted to protect sensitive information. This includes opportunities to work with state, local and education (SLED) government organizations, who often prioritize working with FedRAMP authorized CSPs.

FedRAMP Compliance Challenges

While achieving FedRAMP compliance is essential for CSPs aiming to supply the federal government, it can be challenging. Some of the most common challenges include:

Cost. FedRAMP compliance can be expensive, especially for small CSPs.

Complexity. The FedRAMP compliance process is complex and requires a significant investment of time and resources—even for organizations that already meet the necessary security requirements.

Time. The FedRAMP authorization process takes time—roughly four to six months for agency-specific (ATO) authorizations and up to two years for cross-government (JAB P-ATO) authorization.

DRATA

Who Needs FedRAMP?

FedRAMP compliance is mandatory for any CSP that wants to do business with the federal government OR another CSP that does business with the federal government. These organizations mainly fall into two categories:

- **Pure-play CSPs.** If you're a CSP that wants to do business with the federal government, FedRAMP compliance is a must. It demonstrates to government agencies that your product meets the minimum security requirements required to protect federal information.
- **Global organizations with a cloud component.** If you're a global organization that handles sensitive government data, FedRAMP compliance demonstrates that any cloud components you provide are properly secured.

FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring that can help you meet federal requirements.

ATOs: The 2 Paths for CSPs

In order to be eligible for federal agency contracts, a CSP must obtain an Authorization to Operate (ATO) from the agency it wishes to serve. There are two routes to secure this, depending on whether the CSP aims to work with an individual agency or across many agencies.

Agency ATO (ATO) status is granted by individual agencies and is typically used for Cloud Service Offers (CSOs) that are used by a small number of agencies. This route requires the CSP to acquire a separate ATO for each agency it wishes to serve—e.g., to serve three federal agencies, the CSP would need three ATOs.

JAB P-ATO (Joint Authorization Board Provisional Authority to Operate) status is granted by the Joint Authorization Board (JAB) and is typically used for cloud services that are used by multiple agencies—or even government-wide. The process to acquire P-ATO status is more in-depth than ATO, and generally more costly to obtain. There is also a limit to the number of new CSPs that can receive P-ATO status—a maximum of three CSPs are eligible for evaluation each quarter.

DRATA

Which ATO is Right For You?

If your organization aims to work with a small number of agencies, it's most likely that seeking a separate ATO for each agency will be the best approach. Keep in mind that the requirements for an ATO are always the same, so documentation, audit results, and other evidence used to achieve certification with one agency can be reused with other agencies.

Example: A smaller CSP beginning its journey serving federal agencies will almost certainly want to seek individual ATOs to get up and running as quickly as possible.

However, if your organization aims to work with many government agencies—or, more likely, already has several ATOs and aims to expand its federal agency customer base—P-ATO status may be the best course of action. P-ATO status can be more desirable for CSPs because it allows them to sell to multiple agencies without having to go through the authorization process multiple times.

Example: AWS has a range of P-ATO certified offerings for federal agencies housed in its two government-focused services: GovCloud and East/West.

> **Note:** ATO status is granted for individual CSOs not company-wide. For example, while AWS has many P-ATO certified offerings that federal agencies are free to use, it also has many offerings that don't currently have an ATO status.
>
> If your CSP offers multiple CSOs aimed at a federal audience, you will need to seek ATO status for them individually.

Both types of authorization indicate a CSP meets the security requirements set forth by FedRAMP.

DRATA

FedRAMP Impact Levels

Impact Levels refer to the sensitivity of federal data a CSO is authorized to process, store, and transmit. Fedramp categorizes data into three levels of sensitivity as laid out in FIPS Publication 199,, *"Standards for Security Categorization of Federal Information and Information Systems."*

- **Low Impact.** CSPs authorized at this level can handle data that is non-sensitive and intended for public use. According to FIPS PUB 199, the potential impact of a loss of confidentiality, integrity, or availability of Low Impact data: "could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals."
- **Moderate Impact.** Authorized CSPs can handle data that is sensitive and not available to the public BUT isn't classified, e.g., Personally Identifiable Information (PII). FIPS PUB 199 states loss of Moderate Impact data: "could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals."
- **High Impact.** Authorized CSPs can handle sensitive federal information, e.g., relating to national security, law enforcement, or healthcare. FIPS PUB 199 states loss of High Impact data: "could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals."

Every ATO specifies a data Impact Level that the associated CSO is authorized for. For example, a CSO with a Moderate Impact P-ATO can contract with any federal agency, so long as the data it holds is of Low or Moderate Impact. Meanwhile, a CSO with a High Impact P-ATO can contract with any Federal Agency and process data of any Impact Level.

The Impact Level of a CSO determines which FedRAMP Controls it must comply with. Note that ultimately, the impact level applicable to a CSO will be determined by the customer—either an individual agency or the JAB.

> According to the FedRAMP PMO: "Moderate Impact systems account for nearly 80% of CSP applications that receive FedRAMP authorization."

DRATA

FedRAMP Authorization Process

The FedRAMP authorization process varies depending on the type of authorization sought. This section will break down the authorization processes for JAB P-ATO and ATO authorization.

Note that while this section lays out the official processes for authorization, the reality can be quite different. It's important to have expert support throughout the authorization process to ensure you prepare and evidence your application effectively.

How To Attain JAB P-ATO Authorization

Joint Authorization Board (JAB) Provisional Authorization To Operate (P-ATO) is intended for CSPs that wish to serve multiple federal agencies. Often, these are CSPs that are already doing business with several agencies, or which multiple agencies are interested in doing business with.

The JAB is made up of members of the Department of Defense (DoD), Department of Homeland Security (DHS), and General Services Administration (GSA). This group is responsible for assessing prioritized CSPs for P-ATO authorization. The first step in receiving authorization is to be prioritized by the FedRAMP Project Management Office (PMO).

FedRAMP Connect

The JAB only has resources to evaluate roughly 12 CSPs per year. To ensure the most appropriate CSPs are evaluated, the FedRAMP PMO prioritizes CSPs for evaluation using the FedRAMP Connect process. According to the JAB Prioritization Criteria and FedRAMP Connect Guidance document, prioritization is based on the following criteria:

1. Demonstrable government-wide demand for the CSO.
2. FedRAMP Ready CSOs are preferred.*
3. Preferred characteristics:
    - CSO is designed for the federal government (e.g., provides a government-only product).
    - CSP demonstrates a proven record of risk management and secure implementations (e.g., holds other recognized certifications or government authorizations).

- CSP provides heightened security, presenting less risk for federal information (e.g., prepared for High Impact applications).
- CSO meets federal government needs (e.g., provides risk reduction, cost savings, or functionality important for political purposes).

*FedRAMP Ready is the FedRAMP Marketplace designation for CSPs that have completed a readiness assessment. See JAB P-ATO authorization process for more details.

To be considered for prioritization, a CSP must complete and submit:

1. A FedRAMP Business Case for JAB Prioritization form.
1. A Proof of Demand spreadsheet.

Once a CSP has been prioritized, it has 60 days to achieve FedRAMP Ready status for its CSO. In practice, many CSPs become FedRAMP Ready before seeking JAB Prioritization, as it gives them more chance of being prioritized and accelerates their journey to P-ATO authorization.

JAB P-ATO Authorization Process

Stage 1: Preparation

FedRAMP Connect	*See above.*
Readiness Assessment	• CSP & 3PAO determine Impact Level and necessary FedRAMP controls. • 3PAO assesses CSO and produces a Readiness Assessment Report (RAR). • CSP remediates issues. • 3PAO updates RAR and submits to FedRAMP PMO. • FedRAMP PMO authorizes the RAR.

FedRAMP Marketplace designation updated to: **FedRAMP Ready**

At this point, a CSP is considered to have "a high likelihood of achieving a FedRAMP Authorization." Full details of the process to become FedRAMP Ready can be found in the FedRAMP Marketplace Designations for Cloud Service Providers document.

Note: Achieving FedRAMP Ready status is **only** a requirement for CSOs seeking a JAB P-ATO. However, many CSOs opt to go through a similar process (minus FedRAMP Connect) to prepare for ATO authorization to improve their chances of achieving authorization on the first attempt.

Full Security Assessment	• CSP finalizes a System Security Plan (SSP). • 3PAO develops a Security Assessment Plan (SAP). • 3PAO conducts a full security assessment of the CSO. • 3PAO produces a Security Assessment Report (SAR). • CSP develops a Plan of Action and Milestones (POA&M) to track and manage security risks identified in the SAR. • CSP submits SSP, SAP, SAR, POA&M and one month of continuous monitoring deliverables (the "security package") to FedRAMP PMO using templates.

Stage 2: JAB Authorization Process

JAB Kickoff *~1 week*	• CSP, 3PAO, and FedRAMP PMO review CSO's system architecture, security capabilities, and risk posture. • JAB issues a "go" or "no-go" decision to proceed with authorization.

FedRAMP Marketplace designation updated to: **In Process**

Review *~3-4 weeks*	• JAB conducts an in-depth review of CSP's security package. • CSP and 3PAO support JAB by answering questions and attending meetings.

Remediation *~3 weeks*	• CSP and 3PAO remediate outstanding issues. • CSP and 3PAO update the security package as necessary.
Final Review *~4 weeks*	• JAB completes a final review of CSP's updated security package.
Formal Authorization	• JAB issues a formal authorization decision. • If favorable, JAB issues a Provisional Authority to Operate (P-ATO).

FedRAMP Marketplace designation updated to: **Authorized**

Note: JAB P-ATO status signifies all three JAB Agencies have reviewed a CSP's security package and determined the CSO suitable for federal agencies. JAB P-ATOs are "provisional" because the federal government doesn't assume responsibility for a CSP's security.

Agencies wanting to use a P-ATO authorized CSO must issue their own authorization. However, they don't need to conduct tests—they simply review the JAB P-ATO and clear the CSO for use.

Stage 3: Continuous Monitoring

Monthly Deliverables	• CSP provides continuous monitoring deliverables (including incident reporting) to JAB and any agencies using their CSO.
Annual Security Assessment	• 3PAO completes annual security assessments of the CSO. • 3PAO submits annual SAR via FedRAMP secure repository.
JAB Review	• JAB reviews continuous monitoring and annual SAR. • JAB monitors, suspends, and revokes P-ATO status as appropriate. • JAB authorizes or denies significant changes to the CSO.

	• JAB ensures continuous monitoring deliverables are provided to agencies using the CSO in a timely manner. • CSP completes improvements and remediations as necessary.

The continuous monitoring process is based on NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations.

How To Attain Agency ATO Authorization

ATO is intended for CSPs wanting to serve one or a small number of federal agencies and is easier to obtain compared to JAB P-ATO. To attain ATO status, a CSP works directly with the agencies it wants to serve. The ATO is issued directly by those agencies and validated by the FedRAMP PMO.

ATO doesn't require a JAB Readiness Assessment. However, many CSPs still choose to go through this process to ensure they are fully prepared before starting the authorization process. CSPs do, however, still have to work with a 3PAO.

ATO Authorization Process

Stage 1: Preparation

Readiness Assessment	• Optional: *see JAB P-ATO process.*

FedRAMP Marketplace designation updated to: **FedRAMP Ready**

Impact Level	• CSP and 3PAO determine Impact Level and necessary FedRAMP Controls.
Partnership Establishment	• CSP obtains written email confirmation of one or more agencies' intention to authorize (known as an "In Process Request").

Authorization Planning	• CSP produces a Work Breakdown Structure in partnership with the agency and their chosen 3PAO which includes:
	  • The ATO Impact Level.
	  • Agency and CSP points of contact for the FedRAMP PMO.
	  • Confirmation a 3PAO assessment will begin within six months.
	  • Attestation that agencies are actively working with the CSP to grant an ATO within 12 months.

Kickoff Meeting	• CSP and agencies discuss:
	  • CSO functionality and background.
	  • Technical security details, e.g., system architecture, data flows, authorization boundaries, and core security capabilities.
	  • Security controls that fall under customer agencies' responsibility.
	  • Any gaps in compliance and plans for remediation.

FedRAMP Marketplace designation updated to: **In Process**

Stage 2: Authorization

Full Security Assessment	• CSP finalizes a System Security Plan (SSP). • Agency reviews and approves the SSP. • 3PAO develops a Security Assessment Plan (SAP). • Agency reviews SAP and may request changes. • 3PAO conducts a full security assessment of the CSO. • 3PAO produces a Security Assessment Report (SAR). • CSP develops a Plan of Action and Milestones (POA&M) to track and manage security risks identified in the SAR.

Note: While a separate ATO is required per agency, a separate 3PAO assessment is **not** needed for each authorization. So long as authorizations are completed simultaneously for the same CSO, a single 3PAO assessment can be used to support multiple ATO authorizations.

Agency Authorization Process	• CSP submits SSP, SAP, SAR and POA&M (the "security package") to agency. • Agency reviews security package and highlights necessary remediations. • (If necessary) CSP completes remediations. • Agency implements, tests and documents any customer-responsible controls. • Agency performs risk analysis and accepts identified risks. • Agency issues ATO letter. • CSP uploads completed Authorization Package Checklist and security package to FedRAMP secure repository. • 3PAO uploads security assessment materials (SAP, SAR, and attachments) to FedRAMP security repository. • FedRAMP PMO reviews all security assessment materials.

FedRAMP Marketplace designation updated to: **Authorized**

Stage 3: Continuous Monitoring

Monthly Deliverables	• CSP provides continuous monitoring deliverables (scan results, incident reports, etc.) to agency customers via FedRAMP secure repository.
Annual Security Assessment	• 3PAO completes annual security assessments of the CSO. • 3PAO submits annual SAR via FedRAMP secure repository.
Agency Review	• Agency reviews monthly and annual deliverables. • Agency requests improvements and remediations. • CSP completes improvements and remediations as necessary.

The continuous monitoring process is based on NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations.

FedRAMP Authorization Documentation
The documentation required for FedRAMP authorization can vary depending on your circumstances. A full list of documents and templates is available here.

DRATA

Different Processes, Same Controls

While the processes required for JAB P-ATO and ATO authorizations are notably different, the FedRAMP controls required for CSOs remain identical. Which controls apply to a CSO are dependent on the Impact Level assigned, **not** the type of authorization.

The next section will cover the FedRAMP controls, how they differ from NIST SP 800-53, and how to determine which controls apply to a specific CSO.

DRATA

FedRAMP Controls

FedRAMP security controls are based on NIST Special Publication 800-53 revision 5, which provides standards and security requirements for information systems used by the federal government.

However, FedRAMP controls are **not** identical to NIST 800-53. In many cases, they have been refined to apply specifically to CSOs. If your security program is modeled on NIST 800-53, you'll still need to review the appropriate FedRAMP controls to ensure your CSO is ready for authorization.

The controls a CSP must implement depend on which Impact Level their CSO requires. There are 156 controls for Low Impact CSOs, 323 controls for Moderate Impact, and 410 controls for High Impact. These controls are categorized into 18 control families:

1. Access control (AC)
2. Awareness training (AT)
3. Audit and accountability (AU)
4. Security assessment and authorization (CA)
5. Configuration management (CM)
6. Contingency planning (CP)
7. Identification and authentication (IA)
8. Incident response (IR)
9. Maintenance (MA)
10. Media protection (MP)
11. Physical and environmental protection (PE)
12. Planning (PL)
13. Personnel security (PS)
14. Risk assessment (RA)
15. System and service acquisition (SA)
16. System and communications protection (SC)
17. System and information integrity (SI)
18. Supply chain risk management (SR)

For a full breakdown of FedRAMP controls by Impact Level, see the FedRAMP Security Controls Baseline document.

To reiterate, a CSO is only authorized up to the Impact Level specified in its ATO and FedRAMP Marketplace listing. While it may be tempting to pursue a Low Impact ATO to minimize the necessary investment of time and resources, this will severely limit the number of federal agencies and applications a CSO can be used for. Again, roughly 80% of all ATOs issued are of Moderate Impact.

DRATA

Book a Demo

Ready to see how Drata can help lessen the burden and automate tedious compliance tasks?

Use Drata to:

- Hit the ground running with editable, auditor-approved security and risk policies.
- Automate evidence collection and reporting.
- Easily reach and maintain compliance with regulations and compliance frameworks.
- Create, score, and manage your risk register.
- Accelerate sales by sharing a real-time view of your security and compliance posture.

Schedule a demo today to see how Drata can support your continuous compliance program. And for more resources like this delivered straight to your inbox, sign up for Trusted, the Drata Newsletter.