DuploCloud

2026

CHECKLIST

The Essential FedRAMP Compliance Requirements Checklist

Prepare your cloud service offering for FedRAMP Authorization with this complete guide from DuploCloud.

Table of Contents

Introduction

FedRAMP Authorization is an essential undertaking for cloud service providers (CSPs) with a cloud service offering (CSO) they wish to make available for use by federal agencies. This ebook will serve as a guide for cloud-native application developers seeking to offer their products to federal agencies, whether they're already working with an agency or wish to find new potential customers in the federal space.

We at DuploCloud are happy to help engineers embark on this journey by presenting these materials, as well as offering a No-code/Low-code cloud infrastructure automation platform. Building your app with DuploCloud will give you a head start on compliance documentation, thanks to our ready-made automation layers that have controls built in. Get in touch with us to learn more.

FEDRAMP'S Origins and Purpose

Before we delve into the specifics, here is a quick primer on FedRAMP before you begin working with the program.

A Brief History of FedRAMP

FedRAMP is an abbreviation for the Federal Risk and Authorization Management Program. It was first established in 2011 "to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government." As cloud-based services have grown in prominence, number, and utility, FedRAMP has filled an increasingly essential role in bridging the gap between private sector innovations and their applications in the federal government.

FedRAMP is primarily overseen by its Joint Authorization Board (JAB). The JAB is composed of Chief Information Officers from the Department of Defense, the Department of Homeland Security, and the General Services Administration. On top of defining and updating the FedRAMP security authorization requirements, as well as approving accreditation criteria for third-party assessors, the JAB grants provisional authorization for cloud services to be used across federal agencies.

Other governing bodies of FedRAMP include:

- The Office of Management and Budget
- The Chief Information Council
- The National Institute for Standards and Technology

FedRAMP's Guiding Principle Is "Do Once, Then Use Many Times"

FedRAMP cuts down on redundant work by offering a marketplace of approved cloud services in which federal agencies can "shop" for solutions that meet FedRAMP standards. To ensure the program meets the strict security and compliance needs of the federal government, FedRAMP collaborates with government agencies such as the Cybersecurity and Infrastructure Security Agency, or CISA, to continually update and integrate new policies.

Beyond working directly with federal agencies, FedRAMP also assists CSPs who wish to reach FedRAMP Authorized status by maintaining a database of online training courses and videos. The FedRAMP Marketplace additionally serves as a one-stop clearinghouse for finding certified third-party assessors, as required in the authorization process.

FEDRAMP Requirements Checklist

As you work through the FedRAMP requirements checklist, consult the next section for more detailed information at each step of the process.

- Complete CSP Intake Form
- Conduct Intake Call
- Finalize Authorization Strategy
- If JAB Authorization:
  - Establish sufficient demand through FedRAMP Connect
  - Partner with an accredited third-party assessor to obtain FedRAMP Ready status and receive a Full Security Assessment
  - Schedule a Kickoff meeting with 3PAO and JAB to begin review process
- If Agency Authorization:
  - Establish partnership with a federal agency
  - Partner with a third-party assessor to create a Security Assessment Report
  - Schedule a Kickoff Meeting with agency and 3PAO to begin review process
- Provide Periodic Security Deliverables for Continuous Monitoring

Full FEDRAMP Requirements for CSPS

The following pages contain more detailed information for each step of the FedRAMP Authorization process to help as you work through the checklist on the previous page,

1: Finalize Your FedRAMP Authorization Strategy

Cloud service providers can take their offering down one of two paths to FedRAMP Authorization.

The first path is to pursue Joint Authorization Board authorization, which will grant your CSO provisional approval to be used across federal agencies (meaning each agency will be able to individually review and accept your offering based on their own needs and risk tolerance). While this is ideal for providers who wish to get their service in front of as many clients as possible, only CSOs that can demonstrate broad demand across government agencies will be considered by the JAB. Additionally, the JAB only evaluates about 12 CSPs per year to be granted Provisional Authority to Operate (P-ATO).

The second path is agency authorization, which requires working with a specific agency to move your product through the FedRAMP authorization process. This option presents a more certain path to approval, especially if you already have an agency partner that wishes to use your product. However, opting for agency authorization means your product will only be approved for that specific agency, and you must follow the same process for any other agencies that may wish to use it in the future.

FedRAMP recommends filling out its CSP intake form and signing up for an intake call before finalizing your choice of authorization strategy.

2A: For JAB Authorization

If you decide to pursue JAB Authorization for your CSO, you must first undergo the FedRAMP Connect process. This will evaluate your offering against the JAB Prioritization Criteria, helping to determine if and when the JAB will officially take up your application. FedRAMP uses its official blog to announce due dates for FedRAMP Connect Business Cases and to announce which cloud service providers have been selected for consideration during each period.

You must also obtain a FedRAMP Ready designation from a certified third-party assessment organization before you can be authorized. Once you have received a full security assessment from the assessor and responded to its feedback, you are ready to begin the authorization phase by scheduling a Kickoff Meeting between your organization, your assessor, and the JAB.

The Kickoff Meeting will determine whether your offering is fit to proceed with the full authorization process, and if so, will begin a three-to-six month process of in-depth security reviews and remediation. If accepted at the end of the process, your offering will be granted Provisional Authority to Operate.

2B: For Agency Authorization

Seeking agency authorization from FedRAMP is somewhat simpler than working directly with the JAB; the FedRAMP Connect process does not apply, and seeking a FedRAMP Ready designation from a third-party assessor is not required, though it is recommended. The most important way to prepare ahead of the authorization phase is to formalize your partnership with a federal agency, then schedule and conduct a Kickoff Meeting with that agency and a certified third-party assessment organization.

After the Kickoff Meeting, your third-party assessor will perform an independent audit of your offering and test your systems, and you must also submit your own System Security Plan for approval by the agency. At the conclusion of testing, the assessor will submit a full Security Assessment Report detailing its findings and recommendation for FedRAMP Authorization. Finally, the agency will review all the supplied security materials to perform a risk analysis, and if found acceptable, the agency will grant you an Authority to Operate letter.

3: Continuous Monitoring Phase

Whether you were authorized by the JAB or an individual agency, your cloud service offering's authorization remains contingent upon continuous monitoring. You must provide periodic security deliverables to all agency customers, as well as the JAB itself if provisionally authorized. These deliverables may include vulnerability scans, annual security assessments, and incident reports.

Expedite Your Authorization With Proven Solutions

Each layer of a cloud service offering must be evaluated before a product can become FedRAMP authorized. However, software built on FedRAMP Authorized infrastructure inherits controls from that authorized system, which will give you a significant head start in both your documentation and for proving compliance during assessments.

DuploCloud's No-code/Low-code cloud infrastructure automation platform is built to make effective and compliant cloud service creation accessible for your business. Reach out today to find out how DuploCloud can help bring your product vision to life for federal customers

Building Your Cloud Application to be FEDRAMP-Compliant

The choices you make as you build your cloud service offering will directly impact its chances of being authorized. Here are three important steps to consider early on in the process.

Find the Classification for Your Offering

The federal government uses a scale published in FIPS Publication 199 to classify the types of information systems it uses. Applications are rated as having potentially Low, Moderate, or High Impact in the Confidentiality, Integrity, and Availability categories. For instance, an information system with high confidentiality impact "could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals" in the event of unauthorized disclosure of information.

These ratings will be used in the lead-up to and throughout your assessment, so you'll have an advantage if you understand them ahead of time.

Prepare for Security Assessments

Your CSO must undergo extensive security assessments conducted by a third-party assessment organization before it can be authorized. FedRAMP's Security Assessment Plan Template offers some helpful examples of what kind of tests will be performed on your CSO so you can start preparing for them now:

- The first round of testing will be performed using automated tools such as file integrity checking and web application scanning
- The second round will use manual methods of security testing, such as forceful browsing conducted via URL manipulation, SQL injection, and CAPTCHA trials.

This isn't an exhaustive list of tests, so be sure to prepare broad and effective security measures before submitting your application for testing.

Build With Your System Security Plan in Mind

While the third-party assessor will play a major part in establishing the security capabilities of your offering, the Security System Plan is your chance to proactively demonstrate the security of your product. Therefore, good documentation is essential. Here are some of the organizational and system attributes that must be present in your SSP.

- Data flows that run internally, externally, and across the system boundary
- Dataflows that have FIPS 140 validated encryption.
- Customer responsibilities for each security control.
- Diagrams that show how your CSO provides identification and MFA for relevant network and local access.
- All scanning capabilities for operating systems, databases, and web apps.
- An inventory for all hardware, software, and firmware.

Your system security plan should also note inheritances from other FedRAMP leveraged systems.

As you move into the authorization phase, the JAB or your agency partner will give you 30 days to remediate high risks, 90 days for moderate risks, and 180 days for low risks.

FEDRAMP Marketplace Primer

Beyond authorizing services for use with federal agencies, FedRAMP also maintains the FedRAMP Marketplace, a searchable and sortable database organized into three categories:

- CSOs that have achieved a FedRAMP designation (whether Ready, In Process, or Authorized)
- Federal agencies using FedRAMP Authorized CSOs
- Third-party auditors authorized to perform FedRAMP assessments

The FedRAMP Marketplace can also be useful as a point of comparison for CSPs who wish to research other products that have already been cleared. It's also an excellent way to find a third-party assessment organization before beginning your authorization process, since only certified assessors are listed

How Can I List My Product on the FedRAMP Marketplace?

To be listed on the FedRAMP Marketplace, your cloud service offering must be at a minimum certified as FedRAMP Ready (see the FedRAMP requirements checklist for more info on how to obtain this designation). In other words, while you will need to do a substantial amount of work before your product can be listed on the marketplace, almost all FedRAMP Ready products will be listed automatically with no need for further input or fees.

The only exception to this automatic market listing policy is in the case of private cloud deployments. This is because the Marketplace is meant to enable the reuse of security package documentation, which is not feasible for private deployments. More information about how to get your product listed is available in the FedRAMP Marketplace's Designations for Cloud Service Providers documentation.