MindPoint GROUP℠

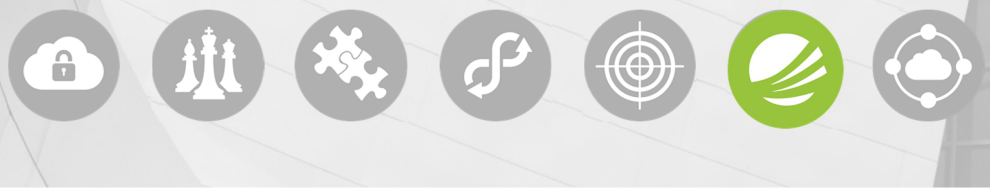
We Specialize in One Thing:
Cybersecurity. Period.

FedRAMP: Achieving Authorization

Achieving FedRAMP Authorization Through FedRAMP Security Assessment Process for Cloud Service Providers

PRESENTED BY:
Samantha Dizor-Carter
FedRAMP Team Lead

MindPoint Group, LLC
1330 Braddock Place, Suite 600, Alexandria VA 22314
(o) 703.636.2033 | (f) 866.761.7457 | **www.mindpointgroup.com**



FedRAMP Series

CONTENTS

INTRODUCTION

With the growing Federal market for cloud services on track to surpass $10 billion by 2023, becoming FedRAMP compliant is a necessity in order to better position your organization when bidding on Federal contracts[1]. Being FedRAMP compliant is the best way to market your cloud service offering to Federal agencies. You may ask, "With so many options to achieve FedRAMP authorization, which is the best path for my organization?" The answer: it depends on your organization's goals and timeframe since choosing the correct path can streamline the process for you.

Cloud services in the Federal market are on track to surpass $10 billion by 2023, compared to just $3.7 million in 2017.

BACKGROUND

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 products and services. The concept of FedRAMP is a "do once, use many times" approach that is designed to save the government time and money. The FedRAMP Security Assessment Framework (SAF) is based on the Risk Management Framework (RMF) that was developed by the National Institute of Standards and Technology (NIST). It simplifies the six steps outlined in the NIST Risk Management Framework by combining them into four steps. The FedRAMP baseline controls identify the minimum controls that a Cloud Service Provider (CSP) must meet to be FedRAMP compliant. FedRAMP has baseline controls for Low, Moderate, and High impact level systems.The requirement for FedRAMP authorization comes from the December 8, 2011 OMB memo[2] that states that all Low and Moderate impact level cloud services leveraged by one or more offices or agencies must comply with FedRAMP requirements by June 5, 2014. Since it's inception, FedRAMP has undergone significant changes to expand FedRAMP authorizations to a larger selection of CSPs by developing a baseline for High impact level systems and the FedRAMP Tailored authorization process for Low Impact Software-as-a-Service (LI-SaaS) systems.

As demand for cloud-based products and services continues to grow within the Federal Government, it is imperative that CSPs wishing to have an advantage while marketing their products to the Federal Government are FedRAMP compliant. Those that are FedRAMP Authorized with a completed Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO), Agency ATO, or a FedRAMP Ready security package have the best opportunity to obtain and maintain federal government contracts.

In December of 2010, the Office of Management and Budget (OMB) released the *25 Point Implementation Plan to Reform Federal Information Technology Management*, which established the Cloud First policy requiring federal agencies to use cloud-based solutions. This plan triggered the establishment of FedRAMP.

---

[1] *U.S. Federal Cloud Computing Market Forecast 201-2023*, Market Research Media, May 29, 2017 (https://www.marketresearchmedia.com/?p=145)

[2] OMB Memorandum for Chief Information Officers, December 8, 2011 (https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf)

The Cloud First Policy[3] is designed to accelerate the pace at which government agencies adopt the cloud. Since the Federal Government is such a large consumer of IT services, the concept of leveraging shared infrastructure and economies of scale is compelling. Further, the ability to purchase scalable and elastic cloud services enables the federal government to only purchase information technology products and services to support current operations but can be increased as demand rises in the future. Other reasons the Federal Government decided to move resources to the cloud include: efficiency improvements that will shift resources towards higher-value activities; better utilization of assets; reduction of duplication in IT infrastructure; data center consolidation; simpler and more productive IT functions; agility; and scalability. This creates a large federal market for cloud computing products and services to fulfill the individual requirements of agencies as they continue the move towards the cloud as the U.S. federal cloud computing market is set to surpass $10 billion by 2023.

In order to meet the ever-increasing demand for FedRAMP authorization, the FedRAMP PMO reinvented the FedRAMP authorization process on March 28, 2016[4]. The updated process, FedRAMP Accelerated, was designed to streamline Joint Authorization Board (JAB) process. Additionally, FedRAMP Tailored was also developed to provide a more efficient path towards FedRAMP authorization for Low Impact Software-as-a-Service (LI-SaaS) systems, as outlined in our previous white paper: FedRAMP Tailored – Accelerating the FedRAMP Process for Low Impact SaaS Solutions. These updates to the program resulted in a 75% reduction in time to achieve FedRAMP authorization; down from the original 9 to 12 months to complete the process and instead being achieved in approximately 3 to 6 months[5].

[3] *Federal Cloud Computing Strategy,* Vivek Kundra, U. S. Chief Information Officer, February 8, 2011, (https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf)

[4] *FedRAMP Accelerated Process A Case Study for Change Within Government*, (https://www.fedramp.gov/assets/resources/documents/FedRAMP_Accelerated_A_Case_Study_For_Change_Within_Government.pdf)

[5] *How FedRAMP Transformed JAB Authorizations to take 75% Less Time* (https://www.fedramp.gov/how-fedramp-transformed-jab-authorizations-to-take-less-time/)

FEDRAMP SECURITY ASSESSMENT FRAMEWORK (SAF)

Federal agencies are required to assess and authorize information systems in accordance with the Federal Information Security Management Act (FISMA) of 2002. The FedRAMP SAF is in compliance with FISMA and is based on the *NIST Special Publication 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems*. The key difference is that the six steps outlined by NIST have been combined into four process areas: Document, Assess, Authorize and Monitor (see Figure 2). The Document process area combines steps 1 through 3 of the NIST RMF and the rest of the process areas are a direct mapping to process steps outlined by NIST.

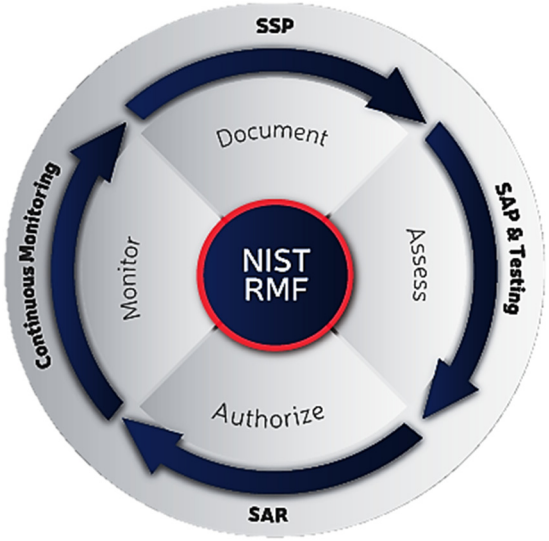


Figure 1: FedRAMP Security Assessment Framework[6]

Additionally, FedRAMP makes use of the *Control Tailoring Workbook* and *Control Implementation Summary*[7] which are helpful to delineate and summarize security responsibilities for CSPs and agencies. Below you will find a detailed step-by-step review of each of the four process areas of the FedRAMP SAF that are depicted in the figure above.

[6] *FedRAMP Security Assessment Framework,* Version 2.4, November 15, 2017 (https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf)

[7] These workbooks can be found on the FedRAMP website (https://www.fedramp.gov/templates/)

SAF Process Areas

Document	The CSP determines the information types and completes a FIPS 199 worksheet to categorize what type of data can be contained/processed within the system to determine the impact level. The categorization is based upon *NIST Special Publication 800-60 (Volumes I and II) Guide for Mapping Types of Information and Information Systems to Security Categories*. FedRAMP supports certifications for Low, Moderate and High impact level systems. Next, the appropriate FedRAMP security controls baseline is selected to match the FIPS 199 categorization level. The applicable security controls are then implemented by the CSP. The System Security Plan (SSP) can be documented at this point. This document includes information such as: the security authorization boundary, how implementations address each required control, roles and responsibilities, and expected behavior of individuals with system access. Nuances that can impact this part of the process include scenarios such as inheriting controls from a lower-level system and ensuring that any additional controls that may be required are also implemented at this time.
Assess	The CSP selects an independent assessor, typically referred to as a Third-Party Assessment Organization (3PAO). Depending upon the path to compliance the CSP has selected, the 3PAO may perform a FedRAMP Readiness Assessment first. This is designed to verify that the CSP meets certain minimum requirements prior to proceeding in the assessment process. The final report is then provided to the FedRAMP PMO for review and approval. The 3PAO generates a Security Assessment Plan (SAP), which documents the methodology and processes for testing the control implementation outlined in the SSP and provides a roadmap and methodology for execution of the tests. The FedRAMP security test case procedures and templates must be used when assessing a cloud system for FedRAMP. The actual assessment includes a kick off meeting, a data call detailing all the artifacts that need to be collected for the assessment, on-site interviews of technical personnel, and a penetration test of all attack vectors.
Authorize	After the 3PAO completes testing of the required security controls, then risks are analyzed, and the results are presented in a Security Assessment Report (SAR). This report provides information regarding the vulnerabilities, threats, and risks discovered during the testing process. It also contains guidance for the CSPs in mitigating the security weaknesses that are identified. The CSP then generates a Plan of Action & Milestones (POA&M) which addresses each of the specific vulnerabilities that are identified in the SAR. The CSP will need to demonstrate that the plan is in place, complete with staffing, resources, and a schedule for correcting each security weakness that is identified. Finally, the security package is ready to be submitted for authorization review. The authorizing official will be able to make a risk-based decision on whether or not to authorize a CSP product or service after a thorough review of the provided information.
Monitor	This process is required to ensure that a cloud product or service maintains an acceptable risk posture. The continuous monitoring results in greater transparency of the security posture of the CSP system and enables the authorizing authority to make appropriate, timely, risk-management decisions. This process promotes operational visibility where a subset of the security controls are reassessed annually by a 3PAO and as well as change control which requires the CSP to provide the authorizing official with detailed change plans and updated an SSP. Controls impacted by these changes are then reassessed by a 3PAO. The last component of the continuous monitoring phase is incident response, where a CSP must follow an implemented incident response plan for its FedRAMP compliant system. The CSP must report incidents according to the documented plan and the authorizing authority must communicate that information to the US-CERT and the FedRAMP PMO according to procedures outlined by FedRAMP. Reassessment of impacted controls may be required depending on the nature of identified incidents.

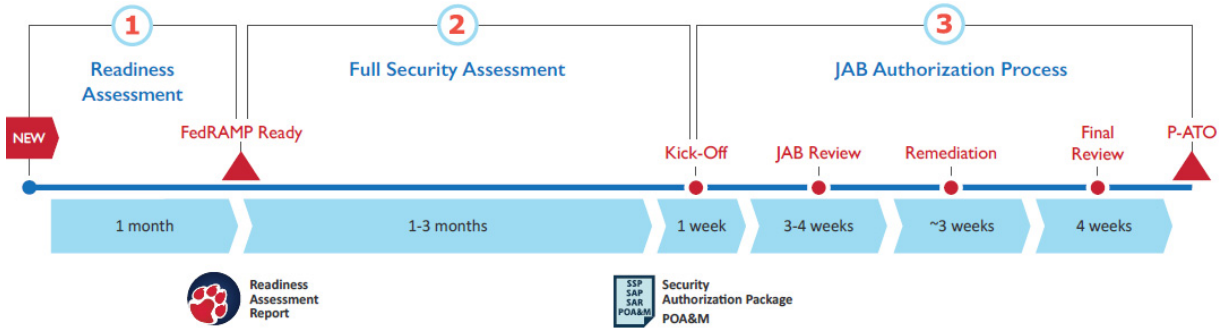
ACHIEVING FEDRAMP AUTHORIZATION

There are four paths that CSPs can take to achieve FedRAMP authorization. The two most utilized paths are the Joint Authorization Board (JAB) Provisional ATO (P-ATO) and the FedRAMP Agency ATO. Another option for CSPs is FedRAMP Tailored, which enables Low Impact Software-as-a-Service (LI-SaaS) systems to achieve FedRAMP Authorization in an expedited manner meeting a fraction of the controls that are required for Low systems. Finally, the FedRAMP Readiness Assessment path allows CSPs to undergo an abbreviated assessment and achieve the FedRAMP Ready status. This shows that they are compliant with the core requirements of FedRAMP and are ready to undergo a full FedRAMP assessment. These distinct paths towards FedRAMP compliance gives a CSP the flexibility to choose a solution that is best for their needs and goals.

JOINT AUTHORIZATION BOARD (JAB) P-ATO

While the JAB P-ATO is one of the most popular paths, it is still considered the most difficult path towards FedRAMP authorization. The initial step for CSPs in this assessment process is to undergo a FedRAMP Readiness assessment which achieves the FedRAMP Ready status. Along with achieving the FedRAMP Ready status, CSPs must also meet the new JAB prioritization guidelines[8], and submit a proposal to FedRAMP documenting how their CSP is meeting these prioritization guidelines and should therefore be considered for the JAB P-ATO process. Those CSPs that are selected for the JAB P-ATO authorization process then undergo a full FedRAMP assessment by a 3PAO. Next, the final security package is submitted to FedRAMP by either a CSP or an Agency and is intended to go to the JAB for P-ATO. The JAB members are the Chief Information Officers (CIOs) from the Department of Homeland Security (DHS), Department of Defense (DoD), and the General Services Administration (GSA). The JAB will perform the risk review of all documentation provided by the CSP in the security package prior to the JAB granting a P-ATO to the CSP. After a P-ATO is granted, the package is placed in the secure repository for agencies to leverage. Figure 2 below illustrates this process.

Figure 2: FedRAMP JAB Authorization Process[9]



[8] *FedRAMP JAB P-ATO Process*, Version 2.0; November 20, 2017 (https://www.fedramp.gov/assets/resources/documents/CSP_JAB_P-ATO_Prioritization_Criteria.pdf)

[9] *FedRAMP Accelerated Process A Case Study for Change Within Government*, (https://www.fedramp.gov/assets/resources/documents/FedRAMP_Accelerated_A_Case_Study_For_Change_Within_Government.pdf)

The JAB P-ATO path does provide agencies with the ability to contract with a CSP that has a P-ATO immediately, often with minimal additional effort regarding review and approval of the CSP. A P-ATO should not be confused with an Agency ATO, as the P-ATO is not to be considered a full Authorization to Operate. Rather, the cloud service provider still needs to secure an Agency ATO from a procuring organization. An Authorization Official (AO) from the procuring organization will need to perform a detailed review of the P-ATO security package and determine if additional controls need to be assessed and whether they will accept the risk(s) associated with operating the product or service.

FEDRAMP AGENCY ATO

Choosing the FedRamp Agency ATO path to FedRAMP Authorization enables the CSP to work directly with the federal agency that is interested in utilizing their offering. The agency holds the responsibility for providing the risk review of all documentation submitted by the CSP in the security authorization package. The security authorization package is the same as that which is provided to the JAB for review which is also done in accordance with the FedRAMP SAF. Once an Agency ATO is granted, the Agency must inform the FedRAMP PMO and submit the package to the PMO for review. After the package is reviewed to ensure it meets all of the FedRAMP requirements, it is then published in the secure repository for other agencies to leverage. One of the biggest differences and advantages associated with this approach is that there is one agency, and therefore one AO. In contrast, the JAB is comprised of the CIOs from DHS, DoD, and GSA and requires that all three of them agree on the risks associated with the system prior to granting a JAB P-ATO. The biggest hurdle with this approach is that a CSP must find a supporting Agency before beginning this process. The typical timeframe associated with an Agency ATO is about four months.

FEDRAMP READY

The FedRAMP Readiness Assessment is part of the new FedRAMP Accelerated process. It is a standalone process that CSPs can use to distinguish themselves from other CSPs competing in the same market for an Agency sponsor. While a CSP will not receive a FedRAMP JAB P-ATO or a FedRAMP Agency ATO, sponsoring agencies can use the process to gauge a CSPs ability to successfully complete a FedRAMP Assessment. As such, CSPs should not overlook this process when considering options to gaining FedRAMP authorization.

FEDRAMP TAILORED

FedRAMP Tailored was also developed to provide a more efficient path towards FedRAMP authorization for Low Impact Software-as-a-Service (LI-SaaS) systems. These systems must meet the following six main criteria to qualify for the program[10]:

1. Operate in a cloud environment;
2. Fully operational cloud service;
3. Must be a Software as a Service (SaaS) as defined by *NIST SP 800-145, The NIST Definition of Cloud Computing*;

[10] *FedRAMP Tailored LI-SaaS Requirements,* Version 3.1, August 23, 2017 (https://www.fedramp.gov/assets/resources/templates/FedRAMP-Tailored-LI-SaaS-Requirements.docx)

4. May not collect any personally identifiable information (PII); except that PII needed to provide login capability (username, password and email address);
5. Qualify as a low-security-impact service, as defined by FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems; and
6. The cloud service must either be hosted within a FedRAMP authorized Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), or the CSP must provide the underlying cloud infrastructure.

The CSPs that meet the above criteria have an easier path to FedRAMP authorization. They are required to meet a substantially smaller set of only 112 controls and are assessed to only a subset of the controls that they are required to meet; totaling 51 controls to be assessed, in comparison to the 125 controls that are part of the FedRAMP low baseline. Authorization times can be as short as a FedRAMP Ready assessment.

The question remains: which path towards FedRAMP Authorization best suits your organization? Choosing the correct path depends on your organization's goals and timeframe. Table 1 below provides a guide to determine the optimal path for your organization.

Table 1: Choosing the Right Path

Path to FedRAMP	*Items needed for completed package*	*What the CSP receives*	*How does this help CSP sell to the Fed. Gov.*	*How long does this take?*	*What is still needed to get work*
JAB	FedRAMP Readiness assessment and Prepare Assessment Package for JAB review and approval of SAP and SAR. 3PAO Readiness Assessment 3PAO Security Assessment	P-ATO for a Low, Moderate or High baseline system	Bid on work with P-ATO Become FedRAMP Compliant without an Agency backing you. Completed package listed in the secure repository for agencies to review.	Estimated 3 to 6 months[11]	Submitting the winning bid in order to obtain an Agency ATO.
Agency ATO	Agency Sponsorship Prepare Assessment Package for Agency review and approval of SSP, SAP, SAR 3PAO Security Assessment	Agency ATO for a Low, Moderate or High baseline system	An Agency ATO from the agency that sponsored you. Completed package listed in the secure repository for agencies to review and leverage.	Estimated 4 months	Additional Agency ATO's require submission of winning bid.
Readiness Assessment	Completed SSP 3PAO Readiness Assessment	FedRAMP Ready for a Low, Moderate or High baseline system	Competitive advantageover other non-FedRAMP Ready or FedRAMP compliant CSP who are bidding on the same work. Readiness assessment package listed in the secure repository for agencies to review.	Estimated 6 weeks	Submitting the winning bid in order to obtain an Agency ATO and undergo a FedRAMP Assessment to receive an Agency ATO.
FedRAMP Tailored	Agency Sponsorship Prepare Assessment Package for Agency review and approval 3PAO FedRAMP Tailored Assessment	Agency ATO for a LI-SaaS System	An Agency ATO from the agency that sponsored you. Completed package listed in the secure repository for agencies to review and leverage.	Estimated 6 weeks	Additional Agency ATO's require submission of winning bid.

No matter which path is chosen, an independent security assessment is required. It is also advisable for the CSP to work with a 3PAO to perform pre-assessment evaluations to determine gaps in security control compliance, documentation development, enhancing controls, and the development of the System Security Plan in order to ensure a successful security assessment. With an ever-growing Federal market for cloud services and products, it is a wise decision for CSPs to take action towards achieving FedRAMP authorization.

[11] Time estimated from kickoff with FedRAMP PMO.

ABOUT MINDPOINT GROUP

MindPoint Group is a cybersecurity consulting firm providing innovative solutions including:

- Cloud Security
- Security Operations
- FedRAMP 3PAO Services
- Governance, Risk & Compliance
- Proactive Security
- Managed Security Services
- Security Architecture & Engineering

MindPoint Group's singular focus and expertise in cybersecurity provides CSPs with a FedRAMP 3PAO team that has intimate understanding of the FedRAMP process, cybersecurity subject matter expertise as well as deep knowledge of all things cloud.

ABOUT THE AUTHOR

Samantha Dizor Carter is the FedRAMP Team Lead with MindPoint Group. She has over 11 years of auditing experience, and over 3 years of risk management, security assessment of Third Party Assessment Organizations (3PAOs) for GSA Federal Risk and Authorization Management Program (FedRAMP). Ms. Carter spearheaded MindPoint Group's accreditation as a FedRAMP 3PAO, including an initial assessment with no findings. As FedRAMP Team Lead she has lead multiple FedRAMP assessments including PowerTrain's initial assessment and most recently Deloitte's continuous monitoring assessment.

LEARN MORE

For additional information about our cybersecurity services, please visit our website and social media:


mindpointgroup.com


GitHub


LinkedIn


Glassdoor


Twitter


Facebook

To learn more about MindPoint Group's FedRAMP 3PAO Services, please email Sam and the rest of the FedRAMP team at fedramp@mindpointgroup.com