FedRAMP compliance is necessary if a Cloud Service Provider expects to operate in the Federal market. This document details the new FedRAMP Accelerated Process and the FedRAMP Security Assessment Process.

FedRAMP Accelerated

MindPoint GROUP℠

Contents

FedRAMP Compliance

Introduction

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 (6) steps outlined in the NIST Risk Management Framework by taking the combining them into four (4) 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 compliance comes from the December 8, 2011 OMB memo[1] that states that all Low and Moderate impact level cloud services leveraged by one or more office or agency must comply with FedRAMP requirements by June 5, 2014.

With the inclusion of High impact-level systems and the FedRAMP certification process projected to surge starting in FY2017, the Federal cloud market is projected to grow to $6.4B by 2019.

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 compliant 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.

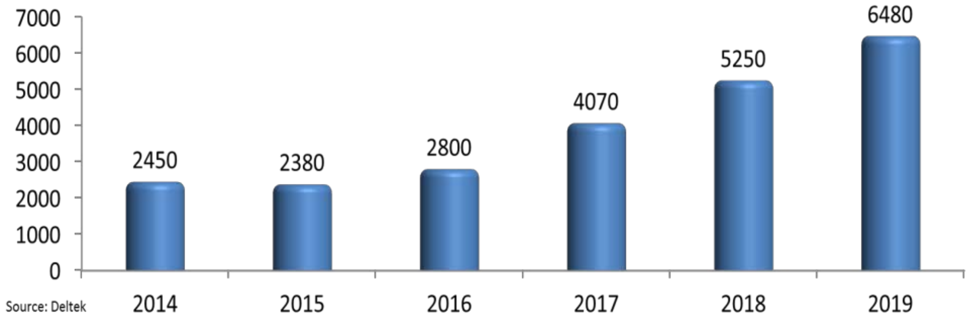
[1] OMB Memorandum for Chief Information Officers, December 8, 2011 (https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf)

Background

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. From this, FedRAMP was established.

The Cloud First Policy[2] 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; scalability; etc. This creates a large federal market for cloud computing products and services to fulfill the individual requirements of department and agencies as they continue the move towards the cloud. With the inclusion of High impact-level systems in the near future and the FedRAMP certification process projected to surge starting in FY2017, the Federal cloud market is projected to grow to $6.4B by 2019[3].

Figure 1 - Cloud Computing Market (in $ Billions), FY 2014 - 2019[4]



Source: Deltek

[2] *Federal Cloud Computing Strategy,* Vivek Kundra, U. S. Chief Information Officer, February 8, 2011, (https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf)
[3] *Federal Update – Cloud, Data Center, Big Data and Mobility, 2014- 2019,* GovWinIQ from Deltek, October 2014, p.22
[4] Ibid.

In order to meet the ever increasing demand for FedRAMP compliance the FedRAMP PMO reimagined the FedRAMP compliance process on March 28, 2016[5]. The new process, FedRAMP Accelerated, is designed to streamline Joint Authorization Board (JAB) process.

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 only real difference is that the six (6) steps outlined by NIST have been combined into four (4) 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. Additionally, FedRAMP makes use of the *Control Tailoring Workbook* and *Control Implementation Summary*[6] which are helpful to delineate and summarize security responsibilities for CSPs and agencies.

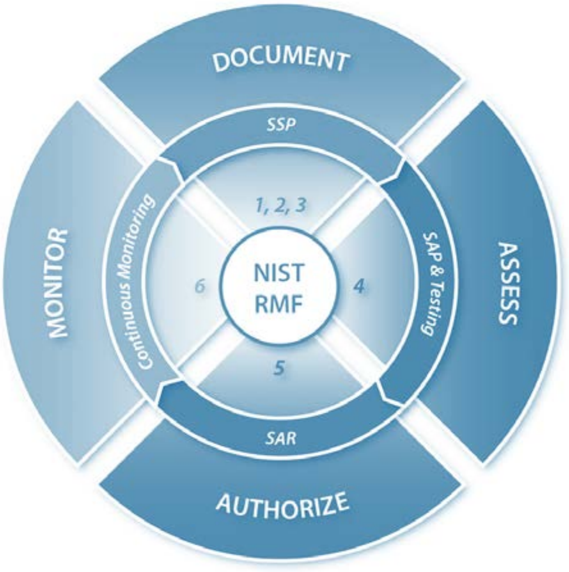


Figure 2: FedRAMP Security Assessment Framework[7]

[5] *FedRAMP Accelerated Process Overview*, (https://www.fedramp.gov/participate/fedramp-accelerated-process/)
[6] These workbooks can be found on the FedRAMP website (https://www.fedramp.gov/resources/templates-3/)
[7] *FedRAMP Security Assessment Framework*, Version 2.0, June 6, 2014 (https://www.fedramp.gov/files/2015/03/FedRAMP-Security-Assessment-Framework-v1.0-2.docx)

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. At this point the System Security Plan (SSP) can be documented. 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 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 and the final report is provided to the FedRAMP PMO for review and approval. The 3PAO then uses the SSP to generate a Security Assessment Plan (SAP), which documents the methodology and processes for testing the control implementation outlined in the SSP. The SAP identifies all of the assets within the scope of the assessment, including components such as hardware, software, and physical facilities. The SAP 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. At this point the CSP is ready to be assessed by the 3PAO.
Authorize	After the 3PAO completes testing of the required security controls, 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 encompasses operational visibility where a subset of the security controls are reassessed annually by a 3PAO and change control which requires the CSP to provide the authorizing authority with detailed change plans and updated SSP. Impacted controls 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.

Paths to FedRAMP Compliance

There are two paths for CSPs to achieve FedRAMP compliance for their cloud-based products and services, in addition to the FedRAMP Readiness Assessment process. This gives a CSP the flexibility to choose a solution that is best for their needs and goals. The paths are:

(A) **Joint Authorization Board (JAB) Reviewed:** This package is submitted to FedRAMP by either a CSP or an Agency and is intended to go to the Joint Authorization Board (JAB) for Provisional Authorization to Operate (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. The CSP must follow the FedRAMP Security Assessment Framework. After a P-ATO is granted the package is placed in the secure repository for agencies to leverage. This essentially provides the CSP with free marketing to Federal Agencies.

This is by far the most difficult path to FedRAMP compliance. The reimagined FedRAMP Accelerated Process now incorporates a FedRAMP Readiness Assessment; and there are no clear reports yet on how long the new process takes to complete. 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 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 determined if additional controls need to be assessed and whether or not to accept the risk(s) associated with operating the product or service.

(B) **FedRAMP Agency ATO:** In this scenario the agency works directly with the CSP and the Federal Agency is responsible for providing the risk review of all documentation provided 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 and the CSP must follow the FedRAMP SAF. Once an Agency ATO is granted the Agency must inform the FedRAMP PMO and the package must still be submitted for the PMO to review. After the package is reviewed to ensure it meets all of the FedRAMP requirements it is 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 comprises the CIOs from the DHS, DoD, and GSA and requires that all three (3) of them have to 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 (4) months.

(C) **FedRAMP Ready:** The FedRAMP Readiness Assessment that is part of the new FedRAMP Accelerated process is actually a standalone process that CSPs can use as a way 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 as a way to gauge a CSPs ability to successfully get through a FedRAMP Assessment. As such this process should not be overlooked when considering options to gaining FedRAMP compliance.

The question remains which option is the best path for your organization. Choosing the correct path depends on your organization's goals and timeframe. The table 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	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.	Data inconclusive	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	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	Competitive advantage over 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.

No matter which path is chosen, an independent assessor is needed to conduct the security assessment. Often, 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.   With an ever growing Federal market for cloud services and products, it is a wise decision for CSPs to take action towards becoming FedRAMP compliant.

About MindPoint Group

As a direct result of the Cloud First policy, the Federal Government is spending more time, money, and effort on cloud procurement services than ever before. Currently, there are only 38 FedRAMP compliant Cloud Service Providers (CSPs) in a market that is projected to grow to $6.4 billion by 2019. For the time being, this means that the federal green field for cloud offerings is being cornered by only a handful of compliant CSPs. However, GovWin has projected there will be a surge in applications starting in 2017. If you are a CSP without a FedRAMP compliant offering and are planning on seeking authorization in the near future, your window of opportunity for establishing a competitive advantage in the Federal cloud market is now, before saturation occurs.

As you are likely aware, CSPs in the Federal space are required to be compliant with FedRAMP, which set forth a standardized approach to risk management by assessing and monitoring the security posture of new and existing cloud products and services. When you consider the fact that data breaches are hitting the news on what seems to be a daily basis, you can clearly see that complying with FedRAMP baseline controls is an essential first step to clearing the way for Federal organizations to safely and securely implement CSP offerings in an ever-changing landscape.

To best guide you through your journey to FedRAMP compliance, your organization needs a trusted 3PAO partner to provide thought leadership and meticulous insight into the security posture of your cloud service. Without proper guidance, the path to FedRAMP compliance is a potentially long and costly journey. Whether assisting you with packet preparation or assessing your package, your 3PAO needs an intimate understanding of the FedRAMP process, cybersecurity subject matter expertise as well as deep knowledge of all things cloud. These services should not be viewed as commodities and your 3PAO shouldn’t simply ensure compliance by checking boxes. The journey to authorization requires a 3PAO to help you navigate the process, but also presents an opportunity to validate and improve your security posture. As of this blog post, there are:

- *There are over 40 3PAOs on the FedRAMP marketplace list [1];*
- *Seven (7) of these companies are listed on the Cybersecurity 500 list of the world’s top 500 cybersecurity companies [2] . Of those seven;*
- *Three (3) are pure play firms that focus exclusively on cybersecurity; and of those three [3] ;*
- ***One (1)** is actively pioneering federal cloud security services for the government’s largest cloud adoption program – **MindPoint Group**.*

MindPoint Group's singular focus and expertise in cybersecurity provide CSPs with a FedRAMP 3PAO team that has:

FedRAMP | Cloud Security | Pentest | ISO Audit Expertise
• Deep understanding of cloud security and the FedRAMP Security Assessment Framework (SAF) that resulted in the completion of MindPoint Group's external 3PAO assessment with zero findings, a singular achievement by MindPoint Group among all 3PAOs;
• Subject Matter Expertise in cloud security, FedRAMP compliance, penetration testing and ISO auditing;
• Cloud security expertise supporting clients like NASA where we have been helping one of the first and largest cloud brokers in the Federal Government deploy a secure hosting solution to migrate the largest web presence in the Federal Government to the cloud. Very few businesses, large or small have designed and operated a cloud solution at this level for large organizations. Our success and hard work resulted in a two NASA awards; and
• Security assessment expertise for a myriad of Federal Government Agencies to include: Department of Justice, Department of Agriculture, Department of Transportation, Department of Treasury, NASA, Department of Interior, as well as many commercial clients to include large financial institutions.
• Accredited Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessment Organization (3PAO)
• 2016 - 2015 Most Innovative Cybersecurity Company, Cybersecurity 500
• 2016 - 2014 Top Security Company, Inc. 5000
• 2015 NASA Honor Award for Securing EVA into GovCloud
• 2014 NASA Honor Award for Securely "Taking NASA into the Cloud"

Allow MindPoint Group to help you navigate the various paths to FedRAMP compliance. Our dedicated team can help you determine which path makes the best business sense for your organization. In addition, we can help you get your system FedRAMP audit ready or we can perform the FedRAMP assessment, depending on where your offering is in the process. No matter what your organization' s goals are and which path to FedRAMP compliance fits you best, we are here to help.

For more information on our solutions, please visit our web site at www.mindpointgroup.com, check out our blog at blog.mindpointgroup.com, or email us at fedramp@mindpointgroup.com.