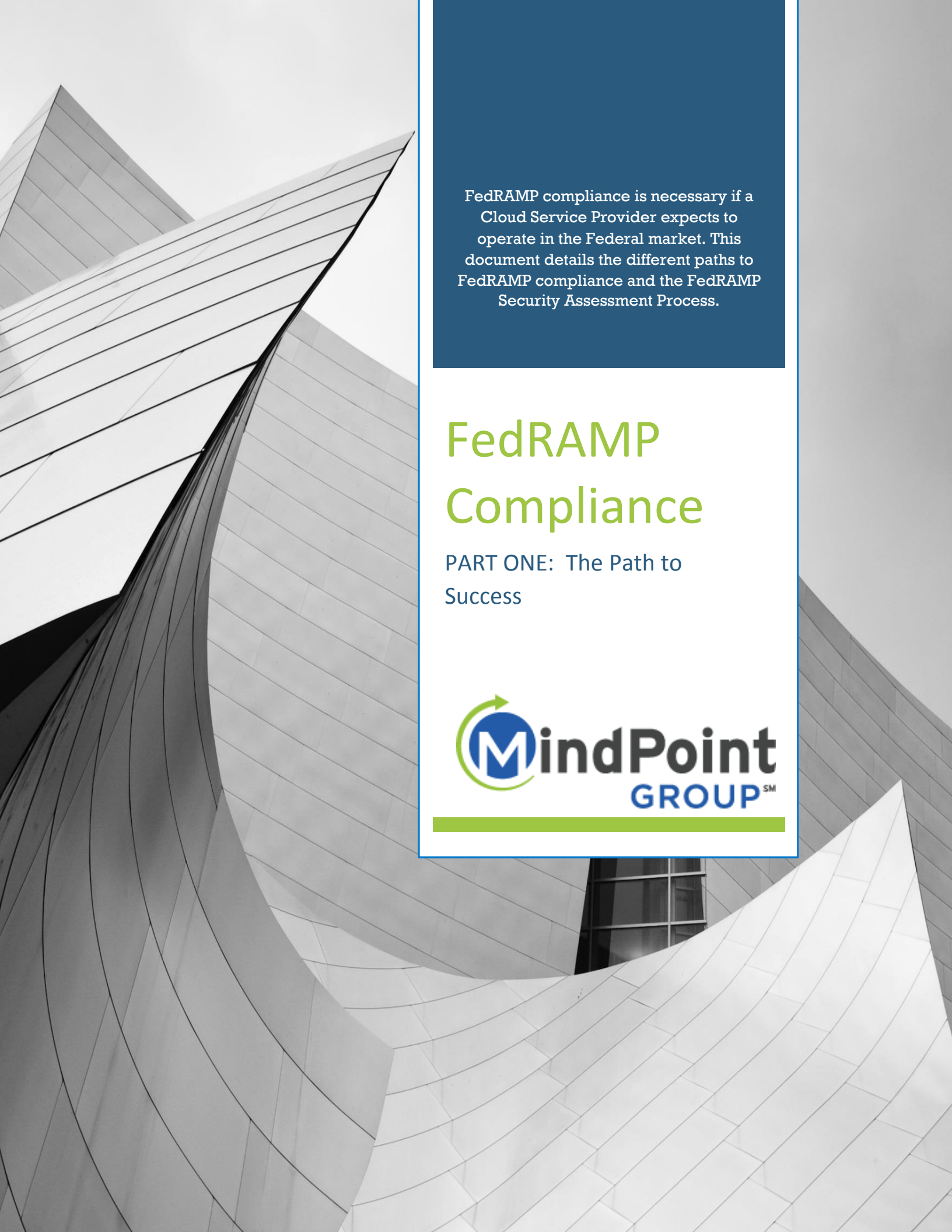


FedRAMP compliance is necessary if a Cloud Service Provider expects to operate in the Federal market. This document details the different paths to FedRAMP compliance and the FedRAMP Security Assessment Process.

FedRAMP Compliance

PART ONE: The Path to Success

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 combining them into four (4) process areas. The FedRAMP baseline controls identify the minimum controls that a Cloud Service Provider (CSP) must meet to be FedRAMP compliant. Currently, FedRAMP has baseline controls for Low and Moderate impact level systems, although they have started development on the baseline for High impact level systems and expect to begin to offer FedRAMP certification for those systems within the next year.

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 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.

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 CSP-supplied security package have the best opportunity to obtain and maintain Federal Government contracts.

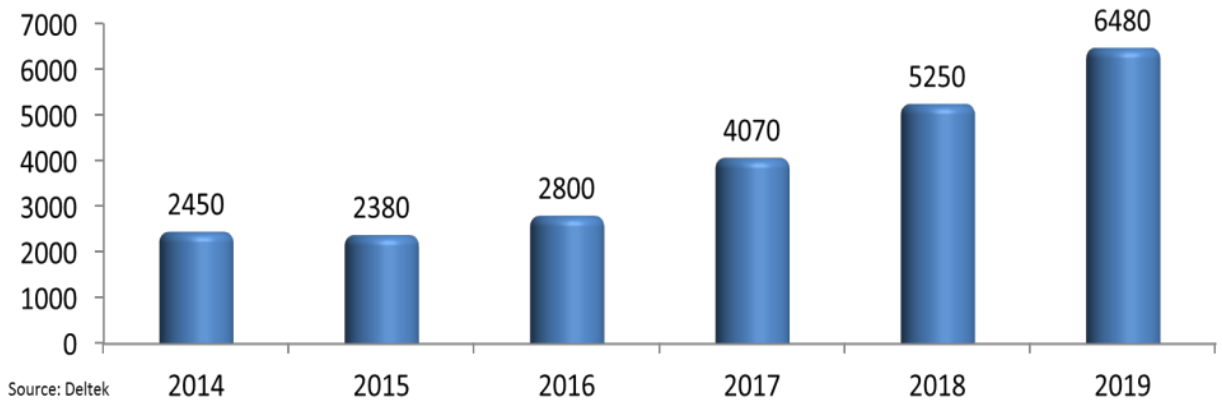
[1] OMB Memorandum for Chief Information Officers, December 8, 2011 (https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf)

The Federal Cloud Market

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]



[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.

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*[5] which are helpful to delineate and summarize security responsibilities for CSPs and agencies.

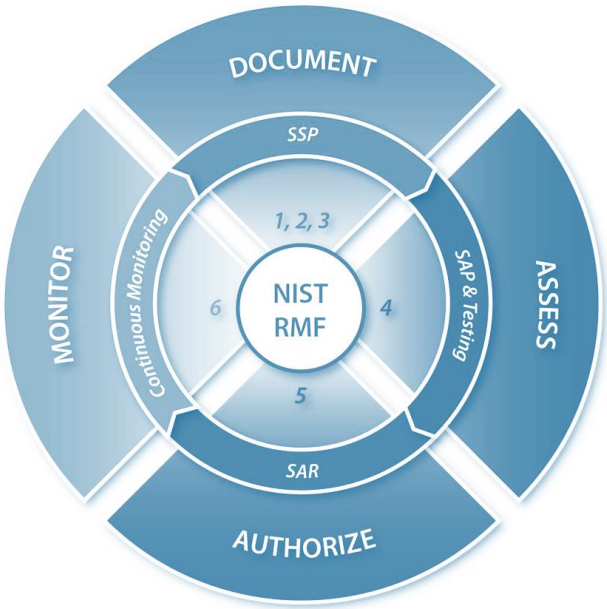


Figure 2: FedRAMP Security Assessment Framework[6]

[5] These workbooks can be found on the FedRAMP website (https://www.fedramp.gov/resources/templates-3/)
[6] *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*. Currently, FedRAMP only supports certifications for Low or Moderate impact level systems, although a High impact level system baseline is being developed. 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). The 3PAO 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 three (3) paths for CSPs to achieve FedRAMP compliance for their cloud-based products and services. This gives a CSP the flexibility to choose a solution that is best for their needs and goals. The three (3) 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, taking on average nine (9) months or more[7] to obtain, but it also provides 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.

[7] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-10/oct22_fedramp_mgoodrich.pdf

(C) CSP Supplied: FedRAMP also accepts security authorization packages directly from CSPs and will place them in the secure repository for prospective Agency use. The CSP completes the FedRAMP SAF on their own which includes having a security assessment completed by a 3PAO. Once the security authorization package is completed the CSP submits it to the FedRAMP PMO where a review of the package for completeness is performed. Once the review has been completed the security authorization package is placed in the secure repository.

Unlike the other processes no P-ATO or ATO is granted after the package is placed in the secure repository. As such, a CSP will still need to find an Agency to work with for final review, approval, and an ATO. This process can be used to by a CSP to penetrate the Federal market and/or an organization easier. First, the repository acts as free marketing to all Federal Agencies looking for a cloud product or service. Additionally, an agency searching for these services are likely to be more willing to work with a CSP that has already gone through the effort of having a security assessment completed and has already documented all of their results in the security authorization package. The agency needs to only review the content of the package, confirm that the risk is acceptable, and then provide the CSP with an ATO. Additionally, this process takes the least amount of time (six weeks or less depending on the complexity of the system), and therefore the smallest investment. This is a great solution for those cloud providers looking to break into the Federal market.

No matter which solution 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 for: determining 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.

With three choices and a 9 month JAB ATO process, selecting the best avenue to FedRAMP certification can be a challenge. PART TWO of our series, "Fast Track to FedRAMP", will discuss the FedRAMP compliance options and how to select the best path for your company.

About MindPoint Group

MindPoint Group is an SBA certified 8(a), woman-owned, economically disadvantaged, and minority-owned small business with its headquarters in Springfield, VA. At MindPoint Group, we specialist in one thing: IT Security. Period. Our singular focus and reputation as cyber security experts have earned us roles as trusted advisors to key government and industry decision makers where we provide broad perspective on today's security challenges, early insight into tomorrow's threats, and engineer innovative security solutions. Our dedication to innovation and service delivery has most recently earned us recognition as a NASA Honor Award recipient for securely bringing NASA into the cloud. For more information on our solutions, please visit our web site and blog at www.mindpointgroup.com, or email us at fedramp@mindpointgroup.com.