MindPoint GROUP℠

We Specialize in One Thing:
Cybersecurity. Period.

FedRAMP Tailored

Accelerating the FedRAMP Process for Low Impact SaaS Solutions

March 7, 2018

PRESENTED BY:
Jason Reetz
Senior Consultant
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

FEDRAMP RECAP

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-based products and services. Using a "do once, use many times" framework, FedRAMP desires to reduce the cost of FISMA compliance and enable government entities to secure data and detect cyber security vulnerabilities at unprecedented speeds. 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). The Security Assessment Framework (SAF) simplifies the six steps outlined in the NIST Risk Management Framework (RMF) by pairing them down 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. Additional information on FedRAMP is available in MindPoint Group's FedRAMP Accelerated white paper.

MindPoint Group's singular focus in cybersecurity provides CSPs with a FedRAMP Third Party Assessment Organization (3PAO) team that has a deep understanding of cloud security, penetration testing and the FedRAMP Security Assessment Framework (SAF). MindPoint Group's 3PAO technical subject matter expertise goes beyond just independent third-party assessments to offering several services that assist companies at all stages of the FedRAMP authorization process. Prior to seeking authorzation MindPoint Group can assist with our FedRAMP Consulting which will help you get your system ready for a full FedRAMP assessment. As part of this consulting we can perform a FedRAMP Gap Assessment to determine the level of effor necessary to achive FedRAMP compliance.

If you are ready to be assesed and going the JAB authorization path; the FedRAMP Readiness Assessment will assess your system to verify that your system meets the minimum requirements outlined by FedRAMP to be recognized as FedRAMP Ready. Whether you choose to go through the JAB Authorization Path or the Agency Authorization Path Mindpoint Group can provide a full 3PAO Assessment of your system as well and help you navigate those assessmets. Once you are FedRAMP compliant, we will help you meet your annual and ongoing Continuous Monitoring requirements.

WHAT IS FEDRAMP TAILORED?

Due to the nature of securing data in the cloud, the FedRAMP process has a higher level of effort and therefore the typical process takes longer to complete. While in the end there are advantages to this (specifically the "do once, use many times" approach which allows for reuse of authorization packages), it also has its disadvantages such as certain systems taking longer to get through the process then what may be necessary. To address these concerns, FedRAMP has developed the FedRAMP Tailored path which is designed for certain low impact Software as a Service (SaaS) systems that are already in FedRAMP authorized clouds [i.e. reside on authorized Infrastructure as a Service (IaaS) and/or Platform as a Service (PaaS) clouds]. The goal is to be able to get these low impact systems that are not storing any sensitive data through the process faster.

FedRAMP's discussions with government digital service teams, Chief Technology Officer's (CTOs) and Chief Information Officers (CIOs) revealed a need to use and authorize common very low-risk applications. FedRAMP Tailored was developed as a new security baseline for qualifying low impact Software-as-a-Service (SaaS) cloud products. Examples of these types of low-cost and low-risk SaaS products that government agencies use include collaboration, project management, open source development, and system performance monitoring tools.

Low risk SaaS does not mean the system's security is low. The security is still high, but the type of data collected in these systems is not sensitive data, and therefore a potential breach would have a minimal impact on citizens and the US Government. An example of a qualifying FedRAMP Tailored system could be a publicly accessible website, library, or archive where the primary concern is not the breach of the information contained within the system but the downtime of availability.

To qualify for FedRAMP Tailored, the low-impact SaaS cloud solution must meet six criteria:

1. Must be an established cloud service
2. Must be fully operational, not under development
3. Must be a Software application (SaaS), not Infrastructure (IaaS) nor Platform (PaaS)
4. Must not process or collect any personally identifiable information (PII)
5. Must meet the definition of low-security-impact per the FIPS 199 definition
6. Must be hosted within a current FedRAMP authorized infrastructure where pre-existing controls and validations can be inherited

An additional criterion that ought to be included on the list is the low-impact SaaS cloud solution must not be part of a mission critical function of an agency.

TAILORED TO FIT JUST RIGHT

FedRAMP Tailored provides a minimum set of security control requirements specifically for very low-impact SaaS cloud products. These requirements are meant to serve as a ground floor to construct a suitable security structure while not over-mandating obligations. This allows you to build a security structure that best balances protection vs cost and the agility to leverage valuable services while maintaining the appropriate level of security.

FedRAMP Tailored follows NIST and the Office of Management and Budget (OMB) guidelines for determining the associated risks inherent in specific, unique low-impact cloud applications. Authorizing Officials could identify additional security controls to be considered as necessary.

FEDRAMP TAILORED BASELINE VS FEDRAMP L-L-L (LOW) BASELINE

The FedRAMP L-L-L (Low) baseline requires some CSPs to implement more security controls than needed based on the type of use and the type of information being placed on Low-Impact SaaS solutions by agencies. FedRAMP Tailored allows agencies to select a smaller set of controls, based on information types and use, for both appropriate and easier authorizations by agencies for these types of services. This tailoring process is explicitly allowed within NIST SP 800-53 revision 4.

Comparing the FedRAMP Tailored Baseline vs the FedRAMP L-L-L (Low) Baseline, you'll find each baseline contains roughly the same amount and type of controls, with the exception being FedRAMP Tailored added the security control IR-9. FedRAMP requires all 125 controls in the L-L-L (Low) baseline to be tested and verified prior to Authority to Operate (ATO).

Of FedRAMP Tailored's 126 controls, only 51 are required or conditionally required to undergo full testing (see table below). The remaining controls are covered and overlapped with 4 controls under federal responsibility

(FED), 13 controls not specifically related to cloud security (NSO), and 61 controls attested to being in place for Low Impact Cloud SaaS by the Cloud Service Provider (CSP).

FedRAMP Tailored Controls		
	Required Controls	**Conditional Controls**
AC	AC-2, AC-3, AC-17, AC-22	-
AU	AU-3, AU-5, AU-6	-
CA	CA-2, CA-6, CA-7	CA-3, CA-9
CM	CM-4, CM-6, CM-8	-
CP	CP-9	-
IA	IA-2 (1), IA-6,	IA-2 (12), IA-5 (11), IA-8 (1), IA-8 (2)
IR	IR-4, IR-6	-
MA	-	MA-2, MA-5
MP	-	MP-2, MP-6, MP-7
PE	-	PE-2, PE-3, PE-6, PE-8, PE-12, PE-13, PE-14, PE-15, PE-16
PL	PL-2	-
PS	PS-3	-
RA	RA-2, RA-3, RA-5	-
SA	SA-9	-
SC	SC-7, SC-12,	SC-5, SC-13
SI	SI-2, SI-3, SI-4	-
	29 Required Controls	*22 Conditional Controls*

The Cloud Service Provider (CSP) is required to provide a self-attestation for those controls or control enhancements that are expected to be routinely satisfied by the CSP without further specification for implementation and meet the intent of the security requirements. The CSP is also required to include those controls or control enhancements that are fully implemented by the infrastructure CSP and considered as FedRAMP "inherited" controls as part of the CSP self-attestation.

STREAMLINE THE PROCESS

Another goal of FedRAMP Tailored is to significantly improve process efficiency by compacting paperwork and decreasing the time expenditure, while maintaining a commensurate level of security. Core documentation such as the System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR), and Remediation Plans are combined into a single document (defined control-by-control). Separate attachments for the Risk Summary Table and Plan of Action & Milestones (POA&M) are used for the initial ATO and Continuous Monitoring. The simplified ATO documentation means Agencies and SaaS cloud service providers (CSPs) save time, effort, and costs.

Currently, a FedRAMP Joint Authorization Board (JAB) Provisional Authorization (P-ATO) takes approximately 3 to 9 months or more, and an Agency ATO takes approximately 1 to 4 months or more. FedRAMP Tailored aims to achieve ATO in under 1 month for low-impact SaaS solutions.

MOVING FORWARD

FedRAMP Tailored was introduced in February 2017 with two open public comment periods through the spring and summer. FedRAMP Tailored is now officially available for use as of September 28, 2017. Template and requirement documents for the FedRAMP Tailored baseline are posted on the FedRAMP website.

CSPs pursing to meet FedRAMP requirements for their cloud service offering (CSO) through the JAB P-ATO authorization route or Agency ATO authorization route must be assessed by an accredited assessor. MindPoint Group is an American Association for Laboratory Accreditation (A2LA) accredited FedRAMP Third Party Assessment Organization (3PAO) assessor providing independent and objective assessments. We can assist cloud providers by providing quality assessment services that meet these short deadlines or by providing our expert consulting services to help get your cloud environment fully prepared for the FedRAMP assessment. For more information, please visit MindPointGroup.com.

RESOURCES

WHITE PAPERS

- MindPoint Group: FedRAMP Accelerated
  - https://www.mindpointgroup.com/wp-content/uploads/2015/11/MindPoint-Group-Part-II-FedRAMP-Accelerated-1.pdf

BLOG POSTS

- MindPoint Group: Choosing a 3PAO: FedRAMP, Cybersecurity & Cloud Expertise are Vital
  - https://www.mindpointgroup.com/blog/choosing-a-3pao/

- MindPoint Group: The AWS Shared Responsibility Model - Part 1: Security in the Cloud
  - https://www.mindpointgroup.com/blog/the-aws-shared-responsibility-model-part-1-security-in-the-cloud/

- MindPoint Group: The AWS Share Security Model – Part II: A Step Towards FedRAMP Compliance
  - https://www.mindpointgroup.com/blog/cloud/then-aws-shared-security-model-a-step-towards-fedramp-compliance/

OTHER RESOURCES

- FedRAMP Tailored
  - https://tailored.fedramp.gov/

- FedRAMP Templates
  - https://www.fedramp.gov/templates/

ACRONYMS

- 3PAO -— Third Party Assessment Organization
- A2LA – American Association for Laboratory Accreditation
- ATO – Authority to Operate
- CIO – Chief Information Officer
- CSO – Cloud Service Offering
    - Cloud based application
- CSP – Cloud Service Provider
- CTO – Chief Technology Officer
- FED – Federal Responsibility
    - The control is typically the responsibility of the Federal Government, not the CSP.
- IaaS – Infrastructure as a Service
- JAB – Joint Authorization Board
- LI -SaaS – Low Impact Software as a Service cloud solution
- NIST – National Institute of Standards and Technology
- NSO – No impact to the Security of cloud Operations
    - FedRAMP has determined the control does not impact the security of the Cloud SaaS.
- OMB – Office of Management and Budget
- P-ATO – Provisional Authority to Operate
- PaaS – Platform as a Service
- PII – Personally Identifiable Information
- POA&M – Plan of Action & Milestones
- RMF – Risk Management Framework
- SaaS – Software as a Service
- SAF – Security Assessment Framework
- SAP – Security Assessment Plan
- SAR – Security Assessment Report
- SSP – System Security Plan

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

Jason Reetz is a Cybersecurity Senior Consultant with MindPoint Group specializing in cloud governance, risk and compliance for commercial sector clients. Jason has worked in IT since 1999 and cybersecurity since 2008. Jason is a Certified Information Systems Security Professional (CISSP) and an AWS Certified Solutions Architect Associate with a Bachelor of Science degree in Management Information Systems from George Mason University.

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 Jason and the rest of the FedRAMP team at fedramp@mindpointgroup.com