



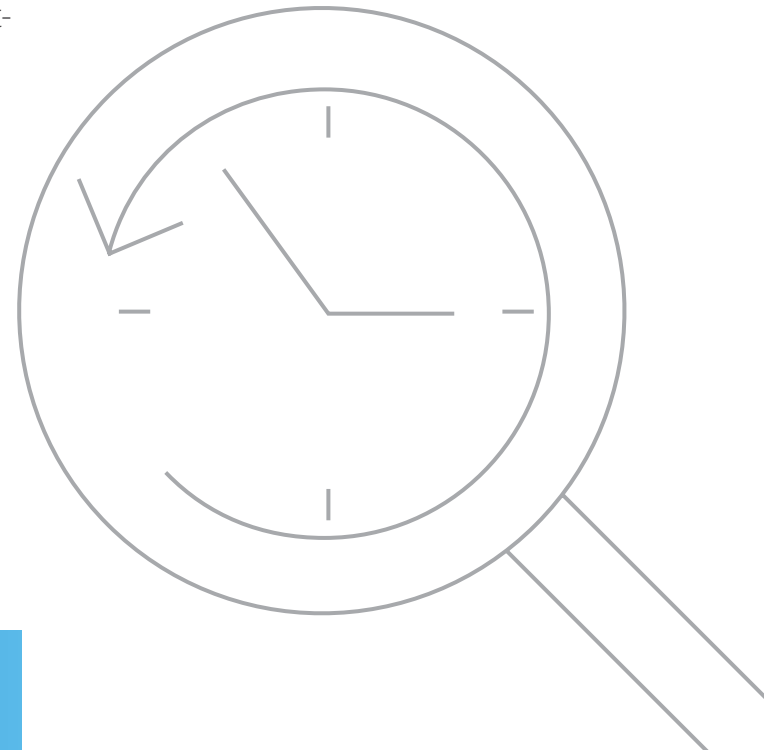
Understanding FedRAMP

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.


Overview & History

Over the past several years, as cloud solutions became more prevalent, it became increasingly important that organizations leveraging cloud technologies—and doing business with federal agencies—had robust cloud security controls in place. Initially, however, many federal agencies maintained their own standards for achieving an authority to operate (ATO), causing confusion and making the ATO approval process difficult, inconsistent, and lengthy for businesses and agencies.

As a solution to this problem, the government created the Federal Risk and Authorization Management Program (FedRAMP), a government-wide standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Several agencies collaborated to create this framework, including the General Services Administration (GSA); National Institute of Standards and Technology (NIST); Department of Homeland Security (DHS); Department of Defense (DOD); National Security Agency (NSA) and others.



Program Goals



The FedRAMP program seeks to achieve several important goals, including:

- Faster, simpler adoption of secure cloud products and services through reuse of assessments and authorizations
- Increased confidence in security of cloud products and services
- Consistent security authorizations built on baseline standards
- Increased confidence in security assessments

Program Benefits

There are several benefits for both CSPs and federal agencies looking to enter business engagements. Some of the most critical advantages include:

- Significant cost and time savings because of a “do once, use many times” framework
- Uniform approach to risk-based management
- Enhanced transparency between agencies and CSPs
- Improved consistency and quality of the Federal security authorization process



Authorized Assessors

There are currently more than 44 3PAOs, including Schellman, authorized by the PMO. Of those organizations, Schellman has conducted more assessments to date than all but one other, making it a trusted leader in the FedRAMP marketplace.



Key Stakeholders

There are four principal stakeholders that participate in the FedRAMP program. They are:

1. FedRAMP Program Management Office (PMO):

The PMO presides over the entire FedRAMP program and is governed primarily by the Joint Authorization Board (JAB), comprised of CIOs from the DOD, DHS and GSA. The JAB is responsible for granting provisional ATOs (P-ATO) to providers looking to perform services government-wide.

2. Cloud Service Providers (CSPs):

Any entity that provides a cloud service offering and wants to do business with the government. Government agencies can only use CSP services that have received an ATO.

3. Federal Agencies:

These are the agencies that engage in business with CSP services. Agencies are responsible for granting ATOs to CSP services. Once an ATO is granted, other agencies can leverage the ATO and follow the FedRAMP continuous monitoring process to ensure compliance.

4. Third Party Assessment Organizations (3PAOs):

These are organizations—such as Schellman & Company—that work with the CSPs and agencies as part of the FedRAMP assessment program. Typically, a 3PAO can either specialize in the upfront implementation of documentation and technology or in the independent assessment of documentation and security controls and subsequent reporting.

FedRAMP regulations stipulate that for any ATO, each of these responsibilities must be performed by a different 3PAO. Schellman & Company specializes in performing the independent assessment, typically after a different organization has performed the upfront implementation work.

Crucial Processes

Phase	Core CSP Activities	Schellman 3PAO Activities
FedRAMP Ready	Submit documentation and evidence key controls.	Conduct an independent readiness assessment and issue a formal Readiness Assessment Report (RAR) per the FedRAMP Ready program guidelines.
Documentation	Develop and submit core security program documentation including the System Security Plan (SSP) and related policies and procedures to the Agency or JAB.	Schellman performs readiness review of the SSP and supporting documentation. While client is finalizing its SSP, Schellman begins to collaborative draft the security assessment plan.
Testing	<p>Stage 1: Review and approve SAP prior to submission to the Agency or JAB</p> <p>Stage 2: Assist Schellman by providing any required documentation and testing evidence.</p> <p>Document any Plan of Action and Milestones (POA&M) generated from the assessment.</p>	<p>Stage 1: Draft and submit the SAP to the Agency or JAB for approval.</p> <p>Stage 2 : Conduct testing of all in-scope controls, complete detailed control finding matrices, and issue SAR.</p>
Finalization	Submit security assessment package.	Provide clarification to the Agency or JAB and/or client as required to complete the authorization process.
Maintenance	Conduct annual continuous monitoring activities as specified in the FedRAMP Annual Assessment Guidance.	<p>Conduct annual assessment of core controls as well as 1/3 of the remaining NIST control set along with review of POA&Ms and remediation.</p> <p>Conduct annual penetration testing and oversee scanning activities as required.</p>

Getting Started

Typically, the first step for CSPs interested in becoming FedRAMP compliant is completing a brief initiation request that provides summary information on their organization and cloud system. This FedRAMP Initiation Request can be found on the [FedRAMP website](#).

Contact Us Today

Schellman offers several competitive differentiators for CSPs looking to be assessed for FedRAMP Ready (RAR) or FedRAMP authorization. We are the first CPA firm that is 100% independent with no consulting agenda. We also offer organizations the opportunity to consult with our distinguished subject matter experts:



Doug Barbin

Principal

CPA, CISSP, PCI QSA, ISO Lead



Steve Halbbrook

Senior Manager


CISSP, CISA, CIA, PCI QSA



Christina McGhee

Manager

CISSP, CIA, ISO Lead



For more information or to contact us about your FedRAMP initiatives,
go to www.schellman.com/fedramp

CLICK FOR MORE INFO

www.schellman.com

4010 W Boy Scout Blvd, Suite 600 / Tampa, FL 33607 / 1.866.254.0000

Outside of the United States, please dial: +1.973.854.4684