eBook

The Importance of FedRAMP for Federal HR Software

EconSys

econsys.com

Contents

What Does FedRAMP Do? 4

How to Obtain a FedRAMP Authorization 5

Joint Authorization Board P-ATO Process 6

The Benefits of Standardized Security Assessment 8

Governance of FedRAMP 9

Utilizing a FedRAMP Authorized Cloud Service Provider 10

Choosing a FedRAMP Authorized Provider 11

Contact Us 12

The Importance of FedRAMP for Federal HR Software

Many federal agencies still operate on-premise data centers, manned by large IT staffs. Despite private enterprise and some agencies largely shifting to cloud-based solutions for HR operations, many government entities remain wary of such a major transition in how data is handled and secured. For this reason, FedRAMP has been established as a government-wide program that standardizes security assessment, authorization and monitoring for all cloud services and products.

This approach allows a “do once, use many times” framework that will save cost, time and staff required to conduct agency security assessments that for a long time have been redundant.

FedRAMP was first announced in 2010 and formalized in a 2011 Office of Management and Budget (OMB) memo from White House Chief Information Officer, Vivek Kundra. The first Authority to Operate (ATO) was issued two years later by HHS. Since then, FedRAMP has become a required step for all cloud service providers offering solutions covered by the original memo.

What Does FedRAMP Do?

FedRAMP requires that all cloud service providers are compliant for new services acquired starting in 2012 and then for all existing services as of 2014. The joint authorization board includes CIOs from DOD, DHS and GSA and issues FedRAMP requirements to meet Federal Information Security Management Act (FISMA) following the National Institute of Standards and Technology (NIST) standards.

To be FedRAMP compliant requires several steps. An ATO certification requires a several weeks process and there are multiple tiers depending on the services being provided. Steps for authorization include:

- Service provider must address all requirements aligned to the NIST 800-53, Rev. 4 for moderate impact levels.
- All system security packages must use FedRAMP templates.
- Service provider must receive assessment by an independent auditor.
- Must be posted to the FedRAMP secure repository.
- Service provider needs to have been granted a Provisional Authority to Operate (P-ATO)

This process offers many benefits when implementing new HR software, especially as you address key technology gaps related to performance management or workforce analytics. Not only does it ensure software meets the standards established by the government for protection of personal identifying information (PII), it enables faster adoption of these technologies when offered by previously authorized cloud service providers.

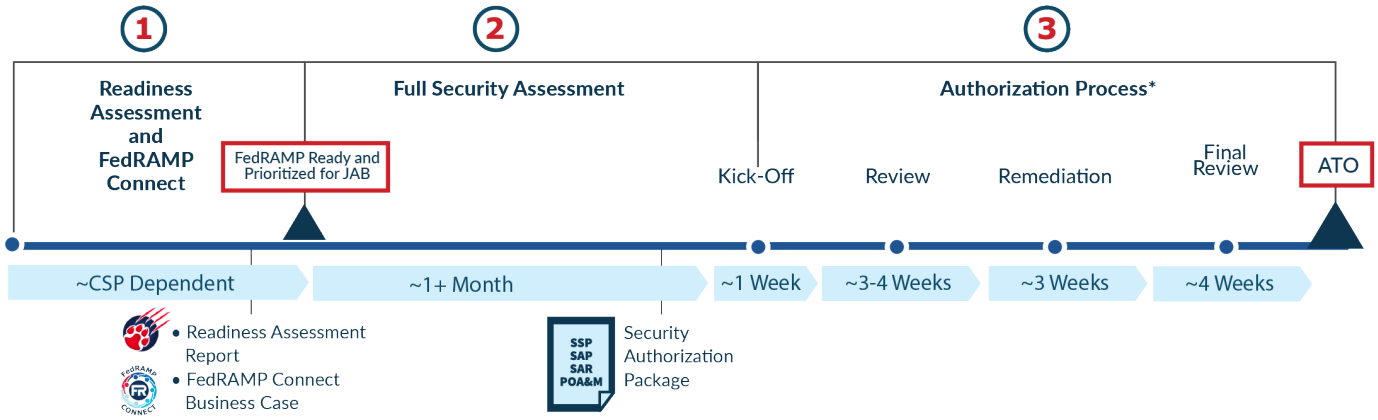
How to Obtain a FedRAMP Authorization

To become FedRAMP compliant, EconSys went through several steps laid out by the Joint Authorization Board to receive a Provisional Authority to Operate (P-ATO) and additional steps for each individual agency worked with in the form of an Agency Authority to Operate (ATO).

The authorization needed is dependent on the Cloud Service Offering (CSO) being provided and the system's impact level, deployment model, stack, and market demand. While each Agency ATO is going to be catered to that individual agency's security protocols, here is a brief overview of the JAB Authorization Process.

Joint Authorization Board P-ATO Process

Becoming authorized by the Joint Authorization Board is a three-stage process, consisting of readiness assessment, full security assessment, and the authorization process. JAB provides the following illustration of the process and the expected average timeframe for each stage:



**A CSP must be prioritized by the JAB before entering the JAB P-ATO process. The CSP can obtain FedRAMP Ready status either before or after the JAB's prioritization*

Phase 1 – Readiness Assessment and FedRAMP Connect

Because JAB has a limited number of resources to assess and authorize new CSOs each year, the FedRAMP process is used to evaluate and prioritize new offerings. JAB's P-ATO prioritization criteria consist of several different factors, but only one of them is mandatory – a demonstrable demand for the service in several different agencies. Six vendors are prioritized to work toward a JAB authorization twice a year. Once prioritized, the vendors have 60 days to finalize FedRAMP ready status to move into the next phase.

To reach this next stage of FedRAMP Readiness, the CSP partners with an accredited 3PAO to complete a readiness assessment, resulting in a Readiness Assessment Report (RAR). JAB reviews this report within one week and once deemed satisfactory, the CSP for which the report was issued will be moved to the FedRAMP Marketplace.

Phase 2 – Full Security Assessment

After being prioritized, the CSP will work to finalize a System Security Plan (SSP), working with an accredited 3PAO to develop it. The 3PAO partner will prepare a security assessment of the service offering and the CSP will develop an accompanying Plan of Actions and Milestones (POA&M) to track and manage each of the system security risks that were identified. All of these reports are completed using FedRAMP templates and must be submitted together to the FedRAMP PMO prior to coordination of a JAB kick-off meeting.

Phase 3 – Authorization

Once all necessary security documentation has been completed, a kick-off meeting is scheduled with the JAB, FedRAMP PMO, the 3PAO, and the CSP authorization team. This meeting evaluates all aspects of the CSO, including architecture, security capabilities, and risk posture, allowing a decision on whether to proceed to authorization.

For those CSPs selected to proceed, JAB will perform an in-depth review of the security authorization package. During this process, there will questions, comments and meeting requests that the CSP and 3PAO must respond to in a timely manner. Monthly continuous monitoring deliverables are also required from the CSP.

Upon completion of review, the CSP and 3PAO will review and document all issues addressed by JAB Reviewer feedback. Upon completion of all of these comments, the CSP will receive their P-ATO and formal authorization from the PMO.

Additional Security Requirements Required by Agencies

All government agencies, in addition to the P-ATO issued through FedRAMP must issue an ATO for cloud products being adopted. Since initial authorization in 2014, EconSys has received agency-level ATO from Defense Information Systems Agency, Department of Defense, Department of Energy, Department of Homeland Security, Department of the Interior, Department of Transportation, Environmental Protection Agency, and Pension Benefit Guaranty Corporation.

The Benefits of Standardized Security Assessment

There are several benefits to a standardized security assessment at the federal level. When you work with a cloud service provider who has received their FedRAMP P-ATO, some of these benefits include:

- Reduced cost, time, and resources as providers have already been assessed at a government-wide level
- An improvement to real-time security visibility
- Greater transparency between the government and the service providers they work with
- Risk based management in a more uniform approach
- Multi-Factor Authentication with CAC/PIV option in most cases.

FedRAMP now enables agencies to quickly adapt from the old system, moving away from insecure legacy IT systems to cost-effective cloud-based IT that is more secure and supportive of future goals. The system now offers:

- Coverage of more than 5 million assets of the world's largest cloud providers
- Four security baselines so government can match security to risk including high, moderate, low, and LI SAAS, with a total of more than 900 controls.
- More than 100 agencies use services from more than 150 FedRAMP ATO issued CSPs, with an average reuse of authorizations of six times, equaling more than $130 million in cost avoidance.

Governance of FedRAMP

FedRAMP is governed by several different executive branch entities that work together to develop, manage and operate the system. Based on the FedRAMP policy memo defining the key requirements of the program issued by the Office of Management and Budget (OMB), Governance is broken down by the following agencies:

- **Joint Authorization Board (JAB) –** The JAB consists of the Chief Information Officers (CIOs) of the Department of Homeland Security (DHS), General Services Administration (GSA) and the Department of Defense (DOD). DHS manages the continuous monitoring strategy including data feed criteria, reporting structure and threat notification coordination.

- **Program Management Office (PMO) –** The FedRAMP PMO is within GSA and is responsible for day to day operations and management of the program.

- **National Institute of Standards and Technology (NIST) –** The NIST advises FedRAMP on FISMA compliance requirements and provides technical advice and specifications for accreditation of independent 3PAOs.

- **CIO Council –** The CIO council shares FedRAMP information with agency CIOs and helps coordinate between agencies.

Because of the nature of the FedRAMP program, it is constantly evolving and implementing new programs and authorizations. The JAB and supporting structure of the Governance over the program ensure these changes can be made efficiently and communicated to both agency CIOs and CSPs.

Utilizing a FedRAMP Authorized Cloud Service Provider

There are many benefits for a government agency to utilize an Authorized Cloud Service. Apart from the above stated benefits which includes cost savings and adopting of a highly secure and visible security process, agencies can be confident that they're leveraging an offering that have been highly vetted, and that it will be continuously scrutinized to maintain good security posture.

Below are some best practices for a government agency when adopting a Cloud Service Provider offering:

1. The agency must do research on the CSP and its security program. Agencies can request access to security artifacts pertaining to a CSO they're interested in from the FedRAMP by completing a request form for that service. The form is available from the FedRAMP website under the specific CSP. All pertinent information needed for the CSO should be available on the appropriate FedRAMP page.

2. After reviewing the organization security artifacts, the agency should be in a better place to move forward with adoption by contacting the CSP on how to make purchase and setup their account. Agencies can request addition information from the CSP if necessary.

3. Once an agency has decided to move forward to buy the CSP's service, they are required under the FISMA and FedRAMP programs to review the packages and issue an Authority to Operate (ATO) letter to the service offering. This process involves the agency conducting the assessment of the list of controls they're responsible for, on top of the work that has been done by the CSP. Often an agency may have an additional set of internet controls to add to the list they're required to assess from the CSP. An example of such a set of controls is the Privacy and Program Management controls which are currently not required under the FedRAMP set of controls.

4. Finally, just like the CSP is expected to do, the agency should continue to perform continuous monitoring of the service offering and conduct an annual assessment of the CSO and update the ATO letter as required by FISMA and the agency internal security requirement. This way due diligence is being performed by all stakeholders to ensure the security of the product.

Choosing a FedRAMP Authorized Provider

Implementation of cloud-based technology for performance management, workforce analytics, retirement calculations, employee and labor relations, and recruitment can significantly improve performance for your agency. It reduces the time spent completing paperwork, streamlines communication, and automates tedious, detail-oriented tasks. But efficiency must be paired with security, which is what FedRAMP authorization ensures.

For HR specialists, FedRAMP offers access to a range of cloud solutions that can improve efficiency in key areas while meeting federal security requirements. This is more important than ever – enabling modernization at scale for a large workforce.

Learn more about how EconSys adheres to FedRAMP requirements

Contact Us

3120 Fairview Park Drive
Suite 500
Falls Church, Virginia 22042

703.642.5225
info@econsys.com

econsys.com