FedRAMP on Salesforce – What You Need To Know
Understanding the regulatory roadmap for FedRAMP on Salesforce

David Clevenger
December 2015

Summary
The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This cloud security program and approach provides a "do once, use many times" framework that saves the U.S. government redundant assessment costs, internal time and money, and in many cases, can provide an equal and/or better security posture than current in-house IT infrastructure options.

FedRAMP is a government-wide program involving numerous departments, agencies, and government groups. The program’s primary decision-making body is the Joint Authorization Board (JAB), comprised of the CIOs from DOD, DHS, and GSA. In addition to the JAB, OMB, the Federal CIO Council, NIST, DHS, and GSA’s FedRAMP Program Management Office (PMO) all play key roles in effectively running FedRAMP.

This document provides general FedRAMP related information as it relates to Salesforce SaaS and PaaS (Native and Composite) ecosystem partners.

What You Need To Know for FedRAMP Accreditations

Question – Is FedRAMP mandatory for public sector cloud services?

Answer – Yes, FedRAMP is mandatory for federal agency cloud deployments and service models at the low and moderate risk impact levels (https://www.fedramp.gov/files/2015/03/fedrampmemo.pdf). OMB mandates FedRAMP compliance for all cloud service providers (CSPs) selling cloud services to the federal government with the following criteria;

- All new services acquired after June 2012
- All existing services by June 2014
Question – What are the paths for FedRAMP compliance?

Answer - There are three routes that a CSP may take to obtain a FedRAMP certified environment. The three existing FedRAMP submission paths are the following;

<table>
<thead>
<tr>
<th>Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FedRAMP JAB Approved</td>
<td>Certification through the FedRAMP Joint Authorization Board</td>
</tr>
<tr>
<td>FedRAMP Agency ATO</td>
<td>Certification through an Agency</td>
</tr>
<tr>
<td>FedRAMP Compliant (CSP Supplied)</td>
<td>CSP Supplied Certification through Third Party Assessment Organization (3PAO) validation testing</td>
</tr>
</tbody>
</table>

Since May 23, 2014, the Salesforce Government Cloud Force.com Platform, Sales Cloud, Service Cloud, and Chatter have been accredited through the Department of Health and Human Services (HHS), and have maintained their FedRAMP accreditation through continuous monitoring and annual assessment validations. In September of 2015, Analytics Cloud was added to the Salesforce FedRAMP Agency level accreditation. See the following link for more detail:  

It is important to note that because the Salesforce Government Cloud is currently accredited under a FedRAMP Agency ATO (HHS) moderate-level, the only FedRAMP paths that can be pursued by current Salesforce ecosystem partners are FedRAMP Agency ATOs and FedRAMP CSP supplied (until one obtains an agency sponsor).
Question - What are some of the actions we need to prepare for a FedRAMP accreditation?

Answer - You will need to create the required FedRAMP documentation and follow the necessary steps listed on the FedRAMP website. The following documents must be prepared in support of FedRAMP readiness:

- FIPS 199 Security Categorization
- Control Implementation Summary (CIS)
- System Security Plan (SSP)
- System-Specific Policy/Procedures
- User Guide
- Rules of Behavior
- IT Contingency Plan (CP)
- Configuration Management Plan (CMP)
- Incident Response Plan (IRP)
- e-Authentication Workbook
- Privacy Threshold Analysis / Privacy Impact Assessment (PTA/PIA)

It's also useful to review the "Guide to Understanding FedRAMP" (https://www.fedramp.gov/resources/documents/) for a programmatic high-level understanding of the FedRAMP security control and documentation process.

At the outset, you should understand what resources can be leveraged internally and start with a FedRAMP preliminary gap analysis. It is also worth mentioning that understanding your strategic roadmap for cloud-based services is very important. This facilitates the use of a consolidated preparation/audit approach, which can leverage reuse of other Governance, Risk and Compliance (GRC) compliance frameworks (e.g., ISO 27001, HITRUST/HIPAA, SOC II/III, etc.) to make the most efficient use of the assessment time.

Question - Who can I talk with for the FedRAMP information and assistance?

Answer - FedRAMP provides a list of independent 3PAOs that are accredited by FedRAMP to perform FedRAMP assistance and guidance. The list of 3PAOs can be found here. Due to the comprehensive nature of the FedRAMP assessment process, most CSPs require the assistance of independent audit or assessment firms, typically by a 3PAO (not required, but recommended) that has been through the FedRAMP process for all submission paths and has a proven track record of success (http://www.meritalk.com/fedramp-experience-frequency.php). Salesforce leverages...
Veris Group’s expertise to perform the FedRAMP assessments for the Salesforce Government Cloud environment.

Question – Who are the main stakeholders in the FedRAMP process?

Answer – FedRAMP stakeholders consist of the CSP, Agencies (buyers), 3PAOs, FedRAMP PMO and FedRAMP JAB.

- CSP – provides the cloud solutions to the government
- Federal Agency – buyer of the cloud solutions
- 3PAO – government accredited and independent testing/audit organization used for FedRAMP assessment and advisory services
- PMO – established within the GSA and responsible for the development of FedRAMP (inclusive of day-to-day operations)
- JAB – consists of federal CIO representatives from DHS, GSA and DOD

All parties serve a key role in ensuring cloud solutions are provided, tested and validated in accordance with FedRAMP requirements for government-wide usage.

Question – How many specific FedRAMP requirements are there?

Answer – As it relates to all cloud providers, security is a shared responsibility. FedRAMP controls are based off of NIST SP 800-53 Revision 4 requirements with additional controls specific to cloud offerings. The FedRAMP baseline contains 125 controls for Low impact systems, 325 controls for moderate impact systems and 408 requirements for High impact systems (pilot phase). There are controls that apply exclusively to Salesforce, some shared between Salesforce and CSP (PaaS/SaaS) and still others between Salesforce and the end customer. As of now, FedRAMP only applies to Low and Moderate impact systems, a High baseline is being piloted but is not widely available to mainstream cloud providers quite yet.

Question - How long does it take to prepare for FedRAMP readiness?

Answer – FedRAMP preparation effort timelines are contingent on several variables within the organization. GRC in the cloud achievement requires a very methodical, strategic roadmap to ensure regulatory compliance is achieved as efficiently as possible within your services offerings. Management buy-in, dedicated time and internal resource commitment are key to estimating time to prepare for a significant effort like this. Most CSPs require outside help, typically by a 3PAO (not required, but
recommended) that has been through the FedRAMP process for all submission paths and has proven success (http://www.meritalk.com/fedramp-experience-frequency.php) in order to yield the best results. There are many elements (internal/external) that need to be in sync for timelines to be executed within the estimate below. We are providing timelines below with many caveats but are generally accepted timeframes to work from;

- **FedRAMP Agency**: 4-8 months
- **CSP Supplied**: 4-8 months
- **FedRAMP JAB**: N/A

You will hear other and varying timeframes from industry CSPs. There are many variables that can have significant impact on the timeframes (e.g., architecture was deficient, or additional security elements, employee separation, clearances, multifactor-authentication had to be added). You will also find that most CSPs are juggling other regulatory drivers (PCI, ISO 27001, SOC, HIPAA, etc.) that can affect timeframes as well.

Your GRC strategy in the cloud should be set prior to engaging the FedRAMP process and consolidation of regulatory requirements and resources should be well thought out for your system development lifecycle. **Knowing when you can re-use/leverage existing resources and documentation is critical.**

**Question - How long does it take to undergo a FedRAMP audit?**

**Answer** – We have supported many Salesforce partners through the FedRAMP process. Many factors can influence the timeframe and well-used preparation time is key for planning purposes. We recommend CSPs expect the following timeframes:

- **FedRAMP Agency**: 4-8 months
- **CSP Supplied**: 4-8 months
- **FedRAMP JAB**: N/A

Plan on at least 12 months of preparation/assessment timeframe (minimum) when building your business case with stakeholders.
Question – Can a 3PAO support the full FedRAMP cycle, preparation and assessment work?

Answer – A 3PAO can support a CSP in preparing a specific cloud solution for FedRAMP readiness (and interface throughout audit on behalf of customer) OR be the 3PAO auditor for the specific cloud assessment. They cannot under any circumstance support both preparation and assessment work for that specific system (IaaS, PaaS and/or SaaS).

Question - How much does it cost to undergo the FedRAMP process?

Answer – In our opinion, there is a lot of mis-information being disseminated about FedRAMP costs in general.

First, for a reality check, CSPs need to look at the process in the following phases to get a good understanding of total cost of ownership associated with getting a FedRAMP approved ATO;

- **Pre-Planning Phase (CSP architecture)** – architecture deficiencies identified as the security requirements are cross-walked. All the CSP infrastructure /application changes needed to meet the FedRAMP requirements. Also, number of internal staff needed to support the effort.
- **Planning Phase** – all preparation activities required to document the implementation of the solution (inside/outside assistance).
- **Audit Phase** – 3PAO audit cost, should be a reputable 3PAO firm.
- **Continuous Monitoring Phase** – all costs required to maintain the accreditation through weekly, monthly, quarterly and annual support (internal and external – 3PAO support).

Secondly, FedRAMP assessment and approval costs also widely depend on the complexity of your solution (IaaS, PaaS, SaaS, or some combination of services). It’s recommended to have a customized/tailored quote to get a better cost estimate for the services requested above (preparation or assessment support).

Third, it is best to work with a reputable 3PAO that can provide you a customized quote for advisory or assessment services, but also ongoing costs for maintaining the accreditation. The key is understanding the full ROI before going any further in the FedRAMP process; it’s certainly not for every organization.
Question - If my cloud offering (PaaS/SaaS) leverages the Salesforce Government Cloud offering, am I FedRAMP certified?

Answer – The definitive answer is no. The Salesforce Government Cloud environment where the application will reside is FedRAMP accredited, but as either a native or composite application, you/CSP will need to ensure your application and custom configurations meet FedRAMP requirements as well. There are specific FedRAMP controls that apply to cloud SaaS and PaaS.

Question – Are all Salesforce services FedRAMP approved?

Answer – Salesforce has created a specific cloud for the Government called Salesforce Government Cloud that has been FedRAMP approved at the agency-level by the HHS. Within the Salesforce Government Cloud, the following services are approved: Force.com Platform, Sales Cloud, Service Cloud, Analytics Cloud, and Chatter. Rather than starting from scratch, agencies interested in contracting for these services can expedite the required Authority to Operate (ATO) security designation by leveraging the assessment work already conducted by the HHS on these Salesforce cloud services. As a reminder, things change quickly in the cloud space, so be sure to keep in contact with your Salesforce account representative for compliance updates.

Question – Can CSPs on Salesforce pursue a FedRAMP JAB P-ATO?

Answer – At this time, ecosystem partners on the FedRAMP approved Salesforce Government Cloud environment cannot pursue a FedRAMP JAB P-ATO. The approved FedRAMP paths for Salesforce CSPs are FedRAMP Agency ATO and FedRAMP CSP Supplied paths. This is due to the Salesforce ATO being agency specific and not fully vetted through the JAB.

Question - As an ISV (Native or Composite) residing on Salesforce Government Cloud, what are we responsible for?

Answer - Most FedRAMP approved (IaaS/PaaS) providers will provide control inheritance for any CSP residing on their ecosystem. In the case of Salesforce Government Cloud, you should take into account what Salesforce is providing, whether it be for native or composite applications. FedRAMP controls will be specifically inherited from Salesforce Government Cloud assessment (e.g., physical/media protection). However, many of the controls are shared inheritance with Salesforce (the
CSP native/composite as defined by NIST) and the end customer responsibility. As an example for Amazon Web Services Partner Network (APN) providers, you can expect a range of 55-75% +/- control inheritance for your specific cloud offering.

Salesforce account representatives or Veris Group (under NDA) can also assist in providing control inheritance guidance and insight into their offering and what controls apply and/or can be inherited in a formal assessment process.

Spending the time to get this right upfront will pay dividends in the long run. Remember, you must put a boundary around the cloud offering. If you don’t, everything else that you do will be at risk of being inaccurate.

**Question - How do we validate that Salesforce is implementing the controls we are inheriting?**

**Answer -** This is based on the FedRAMP accreditation that has already been awarded to and maintained in conjunction with Salesforce (Government Cloud) by the HHS.

Navigating the complexities of cloud ecosystems can be a daunting task. Understanding the boundaries of Salesforce and its ecosystem partners, what security controls and regulatory bodies are applicable, and what preparation is needed for success are all key elements of a successful FedRAMP implementation.

If you have any questions and wish to speak further, feel free to send an inquiry to David Clevenger at dclevenger@verisgroup.com to discuss how strategic GRC roadmaps, FedRAMP and Salesforce ecosystems come together.

**David Clevenger**
Director, Commercial Account Management
E-mail: dclevenger@verisgroup.com

**Veris Group, LLC**
www.verisgroup.com

[Social media icons]