FedRAMP: A Practical Approach

Katy Warren
Rock Sabetto

July 2018

Approved for Public Release;
Distribution Unlimited. Case Number 18-2368
FedRAMP Agenda

- Introduction
- Process
- Considerations
- DoD FedRAMP+
- Closing Thoughts
5 Essential Cloud Computing Characteristics

- **Resource Pooling.** Compute resources can be shared by multiple users
- **On Demand.** Compute resources can be “spun up” as they are needed (and torn down, put back in the pool as they are no longer needed)
- **Broadband Access.** The cloud environment is online (typically via the Internet / ISP) and is accessible from remote locations
- **Metered Services.** Compute resource usage is measured for the purposes of billing, accounting, SLA measurement, etc.
- **Rapid Elasticity.** Cloud environment can scale up (or down) quickly to accommodate new users and/or new compute requirements from existing users

4 Cloud Deployment Models

- **Private.** Solely for an organization
- **Community.** Shared by multiple organizations from a community with shared concerns (e.g., mission, security requirements)
- **Public.** Shared by many tenants, to include businesses and the general public. Owned by a cloud service provider
- **Hybrid.** Some combination of the above, and potentially on premise IT as well

3 Cloud Service Models

- **IaaS (infrastructure)**
- **PaaS (platform)**
- **SaaS (software)**
Before the creation of the **Federal Risk and Authorization Management Program (FedRAMP)**

Gov't Agencies  Many ATOs*  Cloud Services

* ATO: Authority to Operate
After FedRAMP

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

Gov’t Agencies

Finite number of P-ATOs*

Cloud Services

* P-ATO: Provisional Authority to Operate
Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a Government-wide Cloud Program
- Provides standardized approach to security assessment and authorization
- Ensures POA&M* remediation and continuous monitoring

Memo issued by 2nd CIO of the US, Steven VanRoekel
- Published to federal agency CIOs on December 8, 2011
- Defining how federal agencies should use FedRAMP

Hosted by the Office of Management and Budget (OMB)

Current FedRAMP Director - Matt Goodrich

* POA&M: Plan of Actions and Milestones
FedRAMP Governing Bodies

- **FedRAMP PMO (GSA):** Administers FedRAMP, providing standard guidance and information.
- **Joint Authorization Board (JAB):** Primary governance and decision-making body for FedRAMP. Members from CIO offices of DHS, GSA, and DOD. Grants P-ATOs, accredits 3PAOs, defines security requirements.
- **CIO Council:** Disseminates FedRAMP information to Federal CIOs.
- **DHS:** Manages FedRAMP continuous monitoring strategy including data feed criteria, reporting structure, threat notification coordination, and incident response.
- **DOD:** Created FedRAMP+ model with Information Impact Levels for DOD programs.
- **NIST:** Advises FedRAMP on FISMA compliance, assists in developing standards for 3PAOs accreditation.
- **OMB:** Issued FedRAMP policy memo defining key FedRAMP requirements and capabilities.

Image Source: [https://www.fedramp.gov/governance/](https://www.fedramp.gov/governance/)
FedRAMP Today

We cover more than 5 MILLION ASSETS of the world’s largest cloud providers and 1/3 of the world’s internet traffic through our program.

WE NOW OFFER

4 security baselines so government can match security to risk

HIGH (421 controls)
LOW (125 controls)
MODERATE (325 controls)
LI SAAS (38 controls)

Agencies reuse authorizations an average of 6X = >$130 MILLION in cost avoidance

Image Source: https://www.fedramp.gov/about/
FedRAMP builds upon existing policy, frameworks

- **Clinger-Cohen Act of 1996**: Congress establishes that agency heads are responsible for information security.
- **OMB A-130 and NIST SP 800-37, 800-137, 800-53**: OMB A-130 provides policy, NIST Special Publications provide risk management framework.
- **eGov Act of 2002 includes Federal Information Security Management Act (FISMA)**
- **FedRAMP Security Requirements**: FedRAMP builds upon NIST SPs establishing common cloud computing baseline supporting risk-based decisions.
- **Agency ATO**: Agencies leverage FedRAMP process, heads of agencies understand, accept risk and grant ATOs.

Image Source: NIST FedRAMP overview, 7/10/2014
Note: Image adapted by MITRE to include Clinger-Cohen
FedRAMP Partners

- **Agency**
  - Owner of the operational systems and information
  - Accountable for security: owns the risk associated with moving to cloud. Grants the ATO
  - Over 100 Agencies have implemented FedRAMP-compliant cloud solutions*

- **CSP (Cloud Service Provider)**
  - Provides cloud service to the Agency
  - Responsible for obtaining P-ATO (provisional)
  - Current providers include: AWS, Microsoft (Azure), IBM, Google, Oracle, Salesforce
  - Currently there are 102 authorized CSPs*

- **3PAO (Third Party Assessment Organization)**
  - Accredited, independent CSP assessors
  - Perform initial and periodic assessments of CSPs against FedRAMP security requirements
  - Currently there are 43 authorized 3PAOs*

* [www.fedramp.gov](http://www.fedramp.gov) as of 6/4/2018
FedRAMP Learning Paths for CSPs, 3PAOs, and Agencies

1. All Stakeholders
   - 100-A: Welcome to FedRAMP

2. CSPs and 3PAOs
   - 200-B: Security Assessment Plan (SAP)
   - 200-C: Security Assessment Report (SAR)
   - 200-D: Continuous Monitoring (ConMon) Overview
   - 201-B: How to Write a Control

3. 3PAOs (all stakeholders welcome to review)
   - 300-A: 3PAO FedRAMP 17020 Requirements: Understanding and Bridging the Gap
   - 300-B: 3PAO Security Assessment Plan (SAP) Guidance
   - 300-C: 3PAO Security Assessment Report (SAR) Guidance
   - 300-D: 3PAO Documenting Evidence Procedures
   - 300-E: 3PAO Vulnerability Scanning Methodology and Documentation
   - 300-F: 3PAO Review of Security Assessment Report (SAR) Tables
   - 300-G: Readiness Assessment Report (RAR) Preparation

Image Source: https://www.fedramp.gov/training/
FedRAMP Process
Overall FedRAMP Process

**Independent Assessment:**
3PAO performs independent assessment and CSP prepares package for JAB

**JAB P-ATO:**
JAB issues P-ATO; service added to marketplace

**Agency ATO:**
Agency chooses services from marketplace and accepts risk

**Continuous Monitoring:**
CSP, Agency perform continuous monitoring

Next slides focus on JAB P-ATO and Agency ATO processes
FedRAMP Process: JAB P-ATO

- CSPs obtain Provisional ATO (P-ATO) to provide service to Federal organizations via 3PAO companies
- P-ATO is granted by FedRAMP’s Joint Authorization Board (JAB)
- Authorization Package minimally includes Security Plan (SSP), Security Assessment Plan and Report (SAP, SAR), POA&M, Continuous Monitoring Plan

Note: image, copied from FedRAMP.gov, refers to the CSP P-ATO as “ATO”.

Note: Agencies seeking services which have not obtained P-ATO may sponsor this process, and may be able to share cost with the CSP since the CSP will benefit from providing the service.

*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.

- Process used in cases where CSP service will serve one Agency or a small number of Agencies
- Agency grants ATO, using similar documentation package. Can be augmented with additional controls
- Other Agencies can leverage Agency ATO directly, but must accept risk
- Agency authorizations may include IATT, IATO, risk acceptance memorandum, etc.

Note: this process is described in detail in the FedRAMP Agency Authorization Playbook available on the FedRAMP public website
Example: Legacy Application Migration and ATOs

**Migration Process**

- **Rehost, Replatform, Refactor**
  - Functionality
  - Performance
  - Interoperability / interfaces

- **Re-Secure**
  - Implement Controls
  - Obtain IATT, ATO, etc.
  - Continuously Monitor

**Agency On Premise IT**
- Agency ATO
- Agency App and Data
- On Premise Infrastructure

**Cloud**
- Agency App and Data
- CSP IaaS / PaaS Services
- Agency ATO
- P-ATO

**CSP and FedRAMP Marketplaces**
- SaaS
- PaaS
- IaaS
Example: Migration to SaaS and ATOs

**Migration Process**

- **Replace**
  - Business Processes
  - Performance
  - Interoperability / interfaces
  - Data migration

- **Secure**
  - Implement Controls
  - Obtain IATT, ATO, etc.
  - Continuously Monitor
FedRAMP Considerations
Considerations (1 of 3)

- **FISMA compliance is mandatory.** Agencies comply with FISMA by applying NIST controls. For Federal Agency cloud deployments at low, moderate, and high risk impact levels, FedRAMP provides a proven, NIST-based path for FISMA compliance.

- **Median Cost** for CSP to Obtain FedRAMP P-ATO = $2.25M (50% engineering work, 50% process). Ongoing Cost = $1M to maintain Continuous Monitoring. Source: Continuum GRC site

- **Time to ATO**
  - 2014 – 16 months for JAB P-ATO, 13 months for Agency ATO; 2016 – 7 months for JAB P-ATO, 7 months for Agency ATO. Source: 2017 independent study by Coalfire 3PAO
  - Reduction in times have been driven by the “FedRAMP Accelerated” initiative. The processes described in this briefing are the result of this initiative. More details are available here: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Accelerated_A_Case_Study_For_Change_Within_Government.pdf
Considerations (2 of 3)

- **Data Ownership.** Government Agencies should carefully assess the data ownership portions of CSP contracts and SLAs. This is particularly important if the government wants to get the data out of the CSP (e.g., to move it on premise or to another CSP).

- **TIC Compliance.** TIC compliant architectures are required through the FedRAMP security controls baseline. TIC compliance is a hybrid responsibility with CSPs needing to have an architecture that supports TIC and Agencies enforcing TIC routing and compliance.

- **POA&M Remediation.** A CSP has 30 days for remediating high POA&M items, 90 days for remediating moderate POA&M items, and 180 days to remediate low POA&M items.

- **Change Management**
  - CSPs changing existing services (IaaS/PaaS/SaaS with JAB P-ATO) will document the change in the FedRAMP Significant Change Form and submit to FedRAMP for approval.
  - Agencies changing their cloud-hosted systems (i.e., systems they have installed on top of CSP services) will follow Agency-specific change control procedures.

© 2018 The MITRE Corporation. ALL RIGHTS RESERVED.
Considerations (3 of 3)

- **FedRAMP Security Baselines.** FedRAMP (like FISMA) uses (but is not limited to) NIST SP 800-53 r4 security controls:
  - HIGH = 421 Controls
  - MODERATE = 325 Controls
  - LOW = 125 Controls
  - LOW IMPACT (LI-SaaS) = 38 Controls (FedRAMP Tailored)
  - Controls are all downloadable via FedRAMP website
  - Notes:
    - Currently the only Approved FedRAMP HIGH CSPs are AWS, Azure, CSRA, Oracle, Workplace.Gov, Zscaler
    - FedRAMP Tailored LI-SaaS minimum requirements are described in the “FedRAMP Tailored Security Requirements for LI-SaaS” document, including restriction of PII to SaaS login information only

- **Automation.** FedRAMP is working with NIST to begin implementing OSCAL (Open Security Controls Assessment Language). OSCAL is an emerging control language for security authorization that seeks to introduce automation and reduce subjectivity in control assessments
DoD FedRAMP+
FedRAMP+

- DoD established “FedRAMP+” (FedRAMP-Plus) containing additional security controls beyond basic FedRAMP

FedRAMP+ P-ATO process
- Similar to, but separate from, the base FedRAMP process
- Leverages NIST RMF (NIST SP 800-37R1)
- Includes establishing “Impact Levels” that define specific requirements for Unclassified data that is not sensitive / somewhat sensitive / very sensitive / classified. Impact levels are 2, 4, 5, 6

- Many non-DoD agencies accept FedRAMP+
  - Agencies may leverage the added security requirements
  - Usually, DoD does not accept other agency ATOs
## FedRAMP+ Information Impact Level Comparison

**Source:** DoD Cloud Computing Security Requirements Guide, 3/6/2017

<table>
<thead>
<tr>
<th>IMPACT LEVEL</th>
<th>INFORMATION SENSITIVITY</th>
<th>SECURITY CONTROLS</th>
<th>LOCATION</th>
<th>OFF-PREMISES CONNECTIVITY</th>
<th>SEPARATION</th>
<th>PERSONNEL REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>PUBLIC or Non-critical Mission Information</td>
<td>FedRAMP v2, Moderate</td>
<td>US / US outlying areas or DoD on-premises</td>
<td>Internet</td>
<td>Virtual / Logical PUBLIC COMMUNITY</td>
<td>National Agency Check and Inquiries (NACI)</td>
</tr>
<tr>
<td>4</td>
<td>CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems</td>
<td>Level 2 + CUI-Specific Tailored Set</td>
<td>US / US outlying areas or DoD on-premises</td>
<td>NIPRNet via CAP</td>
<td>Virtual / Logical Limited “Public” Community Strong Virtual Separation Between Tenant Systems &amp; Information</td>
<td>US Persons ADP-1 Single Scope Background Investigation (SSBI)</td>
</tr>
<tr>
<td>6</td>
<td>Classified SECRET National Security Systems</td>
<td>Level 5 + Classified Overlay</td>
<td>US / US outlying areas or DoD on-premises</td>
<td>SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval</td>
<td>Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems &amp; Information</td>
<td>US Citizens w/ Favorably Adjudicated SSBI &amp; SECRET Clearance NDA</td>
</tr>
</tbody>
</table>
DoD Cloud Services: Assessment and Authorization Roles

Image Source: DoD Cloud Computing SRG, Figure 6 – DoD Continuous Monitoring for DoD Assessed CSOs

© 2018 The MITRE Corporation. ALL RIGHTS RESERVED.
Closing Thoughts
Closing Thoughts

- FedRAMP is achieving the objective to “do once, use many times”
  - Effectively reducing time and expense required for Agencies to adopt cloud services
  - Over 100 Agencies, 150 CSPs, and 40 3PAO Assessors have successfully leveraged FedRAMP

- Understanding FedRAMP is an important part of cloud adoption, but…
  - FedRAMP addresses security, but does not cover funding, acquisition, engineering, operational, governance, or agency-specific security / change control requirements

**Agencies are accountable for security**

CSOs with JAB P-ATO still require Agency ATO

This is true even if the Agency is leveraging a SaaS solution: the Agency must still ensure data is protected
Questions?
Sources

- FedRAMP.gov (accessed during May and June 2018)
- NIST FedRAMP Overview, NIST Technology Standards Coordination Office, 7/10/2014