Federal Risk and Authorization Management Program (FedRAMP)

ISPAB
June 14, 2013

Matt Goodrich, JD
FedRAMP, Program Manager | Federal Cloud Computing Initiative | OCSIT | GSA
FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

- This approach uses a “do once, use many times” framework that will save cost, time, and staff required to conduct redundant agency security assessments.
FedRAMP builds upon NIST SPs establishing common cloud computing baseline supporting risk based decisions.

OMB A-130 provide policy, NIST Special Publications provide risk management framework.

Congress passes FISMA as part of 2002 eGov Act.

Agencies leverage FedRAMP process, heads of agencies understand, accept risk and grant ATOs.


OMB A-130

NIST SP 800-37, 800-137, 800-53

FedRAMP Security Requirements

Agency ATO

FedRAMP Policy Framework

eGov Act of 2002 includes Federal Information Security Management Act (FISMA)
FedRAMP and NIST RMF 800-37

NIST Risk Management Framework

1. Categorize the Information System
   - Low Impact
   - Moderate Impact

2. Select the Controls
   - FedRAMP Low or Moderate Baseline

3. Implement Security Controls
   - Describe in SSP

4. Assess the Security Controls
   - FedRAMP Accredited 3PAO

5. Authorize Information System
   - Provisional Auth.
   - Agency ATO

6. Monitor Security Controls
   - Continuous Monitoring

CSP

JAB / Agency

CSP and 3PAO

Agency
FedRAMP Standardizes RMF for Cloud

<table>
<thead>
<tr>
<th>NIST SP 800-37 Step</th>
<th>FedRAMP Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Categorize System</td>
<td>Low and Moderate Impact Levels</td>
</tr>
<tr>
<td>2. Select Controls</td>
<td>Control Baselines for Low and Moderate Impact Levels</td>
</tr>
<tr>
<td>3. Implement Security Controls</td>
<td>Document control implementations using the FedRAMP templates</td>
</tr>
<tr>
<td></td>
<td>Implementation Guidance in “Guide to Understanding FedRAMP”</td>
</tr>
<tr>
<td>4. Assess the Security Controls</td>
<td>FedRAMP accredits 3PAOs 3PAOs use standard process, templates</td>
</tr>
<tr>
<td>5. Authorize the System</td>
<td>Joint Authorization Board or Agency AO authorize the system that can be leveraged</td>
</tr>
<tr>
<td></td>
<td>due to increased trust</td>
</tr>
<tr>
<td>6. Continuous Monitoring</td>
<td>CSPs conduct monitoring in accordance with Continuous Monitoring Strategy and Guide</td>
</tr>
</tbody>
</table>
FedRAMP Key Stakeholders & Responsibilities

**Federal Agencies**
- Contract with Cloud Service Provider
- Leverage ATO or use FedRAMP Process when authorizing
- Implement Consumer Controls

**Cloud Service Provider**
- Implement and Document Security
- Use Independent Assessor
- Monitor Security
- Provide Artifacts

**3PAOs Third Party Assessment Organizations**
- Cloud auditor, maintains independence from CSP
- Performs initial and periodic assessment of FedRAMP controls
- Does NOT assist in creation of control documentation

**FedRAMP PMO & JAB**
- Establish Processes and Standards for Security Authorizations
- Maintain Secure Repository of Available Security Packages
- Provisionally Authorize Systems That Have Greatest Ability to be Leveraged Government-wide
When a cloud service provider is selected, FedRAMP governs the security authorization process.

Cloud First Policy

- Agencies must default to cloud based products and services when spending any new money on IT
  - New services, recompetes, additional services
- Agencies must justify to OMB when a cloud provider is NOT selected

Cloud Definition

- FedRAMP is not arbiter of what is and what is not cloud.
- We will authorize anything that is “cloud” esque
- If any agency submits a FedRAMP package for a system they deem cloud, FedRAMP will review that system as cloud – we will not interfere with or negate an agency determination of cloud.
Many cloud vendors are new to FISMA and it takes time to meeting Federal Requirements

- Clearly Defined Boundaries
- FIPS 140-2 Encryption
- Authenticated Scans
- Remediation of Vulnerabilities
- Multi-Factor Authentication
FedRAMP is a rigorous process, with increased scrutiny on meeting security requirements

- Currently 4 JAB provisional ATO’s: CGI Federal, Autonomic Resources, Lockheed Martin, HP
- Currently 2 Agency ATOs: Amazon’s US East/West, and Amazon’s GovCloud
- FISMA process takes time
- Difference between efficient and expedient
- Transparency
- New process for many vendors
- Updated CONOPs and standardization of timelines
- AGENCY ATO’S AND JAB PROVISIONAL ATO’S
FedRAMP Provisional Authorization

Timeframe Overview

SSP Finalization
10-15 weeks

- Assign ISSO -- Kick Off
- SSP Ready Review
- ISSO / CSP review SSP
- JAB Review
- Address JAB Notes

Quality of SSP and responsiveness and ability of CSP to resolve ISSO comments can create iterations in this process

SAP Finalization
3-4 weeks

- JAB Review
- Address JAB Notes
- ISSO / 3PAO Review SAP
- JAB Review
- Address JAB Notes

Quality of SAP and responsiveness and ability of CSP to resolve ISSO comments can create iterations in this process

Testing
6 weeks

- Testing

SAR / POA&M Review
6 weeks

- ISSO / 3PAO / CSP review SAR
- JAB Review
- Address JAB Notes

Quality of SAR as well as number and types of risks can create iterations in this process

Final Review
P-ATO Signoff

- Final Review

SSP Finalization
10-15 weeks

- Assign ISSO -- Kick Off
- SSP Ready Review
- ISSO / CSP review SSP
- JAB Review
- Address JAB Notes

Quality of SSP and responsiveness and ability of CSP to resolve ISSO comments can create iterations in this process

SAP Finalization
3-4 weeks

- JAB Review
- Address JAB Notes
- ISSO / 3PAO Review SAP
- JAB Review
- Address JAB Notes

Quality of SAP and responsiveness and ability of CSP to resolve ISSO comments can create iterations in this process

Testing
6 weeks

- Testing

SAR / POA&M Review
6 weeks

- ISSO / 3PAO / CSP review SAR
- JAB Review
- Address JAB Notes

Quality of SAR as well as number and types of risks can create iterations in this process

Final Review
P-ATO Signoff

- Final Review

Key

CSP Action
FedRAMP / CSP Action
FedRAMP / 3PAO Action
FedRAMP JAB Action
FedRAMP / 3PAO / CSP Action
JAB Provisional ATO vs Agency ATO

**Timeframe**
- JAB: 25+ weeks minimum
- Agency: 14+ weeks minimum

**Level / Depth of Review**
- JAB: Four sets of eyes (PMO, DoD, DHS, GSA)
- Agency: One set of eyes (agency)

**Risk Acceptance Level**
- JAB: Low risk tolerance level, security for security
- Agency: Varying levels of risk acceptance, business needs can justify more risk as can individual agency policies

**Continuous Monitoring**
- JAB: JAB will maintain, agencies need to review
- Agency: Agency must work with CSP to complete
Baseline Controls: NIST 800-53 rev4 Updates

Impact of Revision 4 on FedRAMP Baseline

<table>
<thead>
<tr>
<th>Description</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Change</td>
<td>65</td>
</tr>
<tr>
<td>Insignificant Change</td>
<td>36</td>
</tr>
<tr>
<td>Significant Change</td>
<td>156</td>
</tr>
<tr>
<td>New</td>
<td>40</td>
</tr>
<tr>
<td>Total</td>
<td>297</td>
</tr>
</tbody>
</table>

- Controls have been combined, removed, clarified, scope expanded, additional guidance given, etc.
- Management, Operational, Technical labels removed.
- Privacy controls added in appendix J
3PAO Privatization

3PAO Privatization is designed to keep rigor of 3PAO program and free government resources

- Same process that was done for Health IT, NAVLAP, UL, etc.
- FedRAMP will maintain ownership of accreditation list and is final source of accreditation decision
- Privatization is for accreditation reviews of applicants ONLY
- Privatization will also allow for increased surveillance post accreditation
Privatization Timeframe

Tentative Timeline for 3PAO Privatization

- Currently reviewing AB applications
- We are evaluating all possibilities and approaches for transition of currently accredited 3PAOs to privatized accreditation review
- CSPs and Federal agencies will not be impacted due to privatization efforts – SARs will be accepted from anyone who is on the accredited list
For more information, please contact us or visit us the following website:

www.FedRAMP.gov
Email: info@fedramp.gov