Federal Risk and Authorization Management Program (FedRAMP)

ISPAB Update
October 22, 2014
FedRAMP Current State

FedRAMP to Date
• Operational for over 2 years
• Mandatory compliance date has passed (June 2014)
• ~40% of agency reported use of cloud through PortfolioStat is FedRAMP compliant cloud
  – PMO estimates actual number around 25%

Agency use of FedRAMP
• 22 of 24 CFO Act Agencies actively reviewing FedRAMP security authorization packages
  – Over 500 active reviewers of FedRAMP security authorization packages
  – 50+ requests from other Federal entities (small and micro agencies, congress, courts)
• 30 ATO letters provided by Agencies

Estimated Cost Savings
• 160 identified instances of agency cloud FISMA implementations using authorized CSPs
• $250K average per authorization x 160 cloud implementations = $40M savings
  – Based on 2012 FISMA metrics and agency provided estimates
Cloud System Providers Progress

Authorizations

- **JAB P-ATOs** - 12 cloud services
  - Includes services from IBM, Microsoft, Akamai, HP, Lockheed Martin
- **Agency ATOs** - 6 cloud services
  - Includes Amazon, AINs, USDA, Micropact, Salesforce

FedRAMP Authorizations cover 500+ contracts and 160 known FISMA implementations

In Process CSPs

- **JAB P-ATO** - 18 cloud services
  - Includes services from Dell, SecureKey, Oracle, Amazon, Microsoft, IT-CNP, IBM.
- **Agency ATOs** – 17 cloud services
  - Includes Microsoft, Google, Adobe, IBM, Oracle, Verizon
FedRAMP Ready Systems

• Released on October 16, 2014
• Goal is to assist agencies and CSPs achieve a FedRAMP authorization faster.

Qualifications

• Documentation reviewed by FedRAMP PMO
• Minimum of FedRAMP PMO readiness review process
• CSPs will have varying degrees of readiness
  – Initial documentation
  – Testing completed by 3PAO
  – All required documentation
• Will also include open source code builds
3PAO Accreditation Program Privatization

Cloud Auditor Accreditation (3PAO Program)
- First program (Federal or private) to accredit cloud auditors
- 31 organizations accredited to date
  - Including KPMG, Ernst & Young, Veris, Booz Allen Hamilton
  - ~60% are small businesses
  - One government agency (USDA ESC)
- Privatized in Nov 2013 with A2LA

FedRAMP PMO 3PAO Program Oversight
- Define and update 3PAO requirements – ISO 17020 and FISMA
- Use a conformity assessment approach
- Can revoke accreditation at any time
- Requires 3PAO to agree to adhere to requirements for rigor and independence
- Access to evidence and reports created by A2LA
Security Controls Baseline Update June 2014
- Public comment period and PMO and JAB reviews
- Includes Privacy Appendix J

Rev. 4 Documentation Update Effort
- Updates affected 13 core FedRAMP templates and documents
- Approximately 2000 hours to complete analysis and updates
- Approximately 1250 pages of edits

Major Overhauls and New Documentation
- CONOPS updated to FedRAMP Security Assessment Framework
- Guide to Understanding FedRAMP including new lessons learned
- Creation of 80 test cases due to NIST not updating 800-53a
Major Update: FedRAMP Baseline

FedRAMP Baseline 800-53 Security Control Update

• Revision 3: 298 controls
• Revision 4: 325 controls

<table>
<thead>
<tr>
<th>Category of Changes</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Withdrawn by NIST</td>
<td>45</td>
</tr>
<tr>
<td>Removed by Analysis</td>
<td>8</td>
</tr>
<tr>
<td>Unchanged or Minimal Changes</td>
<td>245</td>
</tr>
<tr>
<td>Added by NIST</td>
<td>39</td>
</tr>
<tr>
<td>Added by Analysis</td>
<td>41</td>
</tr>
</tbody>
</table>

JAB Members Approve Baseline

• Required by FedRAMP Policy Memo
• PMO has received recommended approval from JAB TRs
FedRAMP Security Assessment Framework
Replaces Concept of Operations (CONOPS)
Timeline for Security Assessment Framework

Documentation
- SSP
  - NIST RMF 1, 2, 3

Assess
- SAP
- Testing
  - NIST RMF 4

Authorize
- SAR
- POAM
  - NIST RMF 5

Monitor
- ConMon Reports
  - NIST RMF 6

JAB P-ATOs
- 9+ mos

Agency ATOs
- 4+ mos

CSP Supplied
- ~6 wks
FedRAMP 2 Year Roadmap

Goals
1. Increase adoption and compliance
   • Greater agency involvement in ATOs
   • Provide enhanced training, education, and outreach
2. Improve efficiencies
   • Automation capabilities
   • Faster authorizations and more efficient ConMon reviews
   • Align CSPs with most appropriate authorizer: JAB or Agency
3. Continue to adapt
   • Refinement of ConMon with continuous authorization
   • Better integration with CDM and TIC
   • Establish high baseline

Transparency
• Roadmap will be public document (November release)
• Remain accountable to all stakeholders for the continued evolution and success of the program
Impact of FedRAMP

Enables Cloud Security
• Successfully proven the USG can securely use all types of cloud computing
• Created a standards based approach to security through risk management
• Implements continuous diagnostics and mitigation (CDM) for cloud
• FedRAMP is establishing a new marketplace for cloud vendors
  – Consistent positive press in Forbes, Wall Street Journal, Politico, InfoWeek, and others.

Accelerates USG adoption of Cloud Computing
• Enables agencies achieve cost savings and efficiency through cloud computing
• Accelerates time to market for cloud services when authorizations re-used
  – DOI leveraged 6 authorizations with 1 week review time and conservatively estimates a cost savings of 50% per authorization

Ahead of the Curve
• Commercial industry is looking to FedRAMP as a model for building standards based security for cloud services
• Other countries are also looking to FedRAMP for their security frameworks