DoD Cloud Assessment Process

Gordon Bass
Chief, Certification and Assessment Branch (RE52)

29 January 2015
PA & ATO Terminology

• A FedRAMP Provisional Authorization (PA)
  – Issued by the Joint Authorization Board (JAB)
  – To a Cloud Service Provider (CSP) for their Cloud Service Offering (CSO)

• A DoD PA – Will typically leverage a CSP’s JAB PA (or Agency ATO)
  – Issued by the DISA Authorizing Official (AO)
  – To a CSP for their CSO, based on a FedRAMP JAB PA or FedRAMP compliant Agency ATO (Level 2)
  – To a CSP for their CSO, based on additional DoD security requirements (Levels 4/5/6)

• A DoD Authority to Operate (ATO) – Will leverage a CSP’s DoD PA
  – Issued by a DoD Component AO
  – To a Mission Owner for their system that makes use of the CSP’s CSO

PA – Focuses on CSO Risk
Granted by: The FedRAMP JAB and the DISA AO
To: A CSP for their CSO

ATO – Focuses on Mission Risk
Granted by: A DoD Component’s AO
To: A DoD Mission Owner for their system
Impact Level 2 – DoD PA assessment is no longer required! *

* If the Cloud Service Offering (CSO) has a FedRAMP JAB PA or Agency ATO

NOTE: The decision to leverage the JAB PA or Agency ATO is at the discretion of the DoD Mission Owner and the responsible Authorizing Official (AO). Further assessment may be needed in order to grant an ATO.

Impact Level 4/5/6 – DoD PA assessments are required

– Based on security controls/enhancements in the FedRAMP Moderate baseline coupled with DoD specific controls and other requirements (referred to as FedRAMP+)

<table>
<thead>
<tr>
<th>Level 4</th>
<th>Level 5</th>
<th>Level 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>+35 DoD Controls/Enhancements</td>
<td>+44 DoD Controls/Enhancements</td>
<td>+44 DoD Controls/Enhancements</td>
</tr>
<tr>
<td>Plus Privacy Overlay if Required</td>
<td>Plus Privacy Overlay if Required</td>
<td>Plus 98 from Classified Overlay</td>
</tr>
</tbody>
</table>
Assessment Synergies

A parallel vs. serial assessment approach is used as much as possible to shorten timelines.
FedRAMP Process

Current duration (per CSP) is 6 months +

Initiation
- CSP submits SSP for Review
- FedRAMP Assigns ISSO & Holds CSP Kick-off

System Security Plan
10-15 weeks
- ISSO & CSP Review SSP
- JAB TR Review [2 week review]
- CSP Addresses JAB Concerns
- 3PAO Creates SAP/ISSO Reviews SAR

Security Assessment Plan
3-4 weeks
- JAB TR Review [1 week review]
- CSP Addresses JAB Concerns
- 3PAO Tests & Creates SAR

Testing
6 weeks
- ISSO/CSP Reviews SAR
- JAB TR Review [2 week review]
- CSP Addresses JAB Concerns Creates POA&M

SAR & POA&M Review
6 weeks
- Final JAB Review / P-ATO Sign Off

Authorize
- Authorization Recommendation “One Pager” submitted to DOD JAB Member

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

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

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

United In Service to Our Nation
DoD FedRAMP+ Process

Current duration (per CSP) is 3 months +

Initiation
- CSP submits SSP+ for Review
- DISA Assigns CA & Holds CSP Kick-off
- CA Review (2 week review)
- CSP Addresses CA Concerns
- 3PAO Creates SAP/CA Reviews SAP+
- CA Review [1 week review]
- CSP Addresses CA Concerns
- 3PAO Tests & Creates SAR+
- CA Review [1 week review]
- CSP Addresses CA Concerns Creates POA&M+
- Certification Recommendation submitted to DSAWG for comment then to DISA AO for authorization

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

System Security Plan+
- 2-15 weeks

Security Assessment Plan+
- 2-4 weeks

Testing
- 3 weeks

SAR+ & POA&M+ Review
- 3 weeks

Review and Authorization
- Authorize 1 week

Monitor & Manage
- Network Defense and Monitoring

United in Service to Our Nation
Transition Plan for Assessments:

- New assessments will use the requirements in SRG v1r1
- Assessments in process according to CSM v2.1 will continue on that track
  - Must transition to compliance with SRG v1r1 with their next FedRAMP annual assessment
- CSPs that have already received a DoD PA under CSM v2.1
  - Must transition to compliance with SRG v1r1 with their next FedRAMP annual assessment
Mission Owner Considerations

John J. Hickey Jr.
Authorizing Official

29 January 2015
Cloud Inheritance Model

Cloud Service Provider

3PAO

FedRAMP JAB
Provisional Authorization

FedRAMP Assessment

DoD
FedRAMP+
Assessment

DISA
AO

DoD
Specific Controls
Reporting and Evidence

Attestation Reports
Evidentiary Artifacts

DoD
Mission Owner
Assessment

ATO

AO

United in Service to Our Nation
Mission Owner Considerations

• Determination of Impact Level
• Infrastructure sharing with other systems
• Trust between systems (e.g. Active Directory trust relationships)
• Location Considerations
• Availability Requirements
  – Must be determined and included in the contract or Service Level Agreement (SLA)
• Disaster Recovery Requirements/Options
  – Methods available for data/system backup
• Contract Termination Considerations (e.g. return/wipe of data)
• Personnel Investigation Requirements
  – Appropriate investigations based on OPM and DOD requirements (e.g. Insider Threat requirements)
Mission Owner Considerations

• Mission-focused Computer Network Defense (MCND)
  – Engaging a MCND and establishing role/responsibilities between MCND and supporting systems administration team

• System Administration / Patching / Scanning

• Review of Authorization Package and supporting artifacts being leveraged (e.g. Provisional Authorization documentation or Agency ATO documentation)
  – May drive additional control requirements or specific value requirements

Opportunities
• Cost savings
• Agility
• Innovation

DoD Imperatives
• Security
• Command and Control
• Situational Awareness
Challenges on the Horizon

- Establishing a base of knowledge and training for Security Control Assessors (SCAs) and Authorizing Officials (AOs) in leveraging CSP documentation
- Integrating CSP Cloud Service Offering information into tools such as eMASS to support RMF package inheritance
- Enabling the sharing and use of CSP Continuous Monitoring information by AOs and Mission Owners

Understanding the architecture of a system is key to managing its risk and is critical in preventing risk to others systems!