Federal Risk and Authorization Management Program

Update for NIST Cloud Forum III

Katie Lewin
Director, Cloud Computing Initiative
U.S. General Services Administration

April 8, 2011
The Case for FedRAMP

Problem

• Current security framework has duplicative efforts across Federal Agencies. Each agency completes a security authorization for each IT system – regardless if that system has been authorized by another agency.
• There are discrepancies and inconsistencies on how agencies conduct authorizations.

Solution

• Federal Risk and Authorization Management Program (FedRAMP) establishes a unified risk management framework for cloud computing systems based on a standard set of controls and defined processes.
• FedRAMP is compatible with FISMA security requirements and has been vetted across government and with industry.
• FedRAMP provides effective and consistent assessment of cloud services resulting in cost savings.
• Continuous monitoring focus will be on near-real time data feeds from cloud service providers.
• Uses the “Approve Once, Use Many” concept.
FedRAMP: Essential Components

- Maintains Security Baseline including Controls & CM Requirements
- Maintains Assessment Criteria
- Maintains Library of Approved Systems

Joint Authorization Board
Provides Risk Governance & Prioritization Across the Assessment, Authorization and Maintenance Phases

1. Assessment Phase
   - **Independent Assessment**
     • Cloud Service Provider system must be assessed by an Independent 3rd Party Assessor before a risk based decision to issue an ATO can be made.

2. ATO Phase
   - **Accepting the Risk**
     • ATO Issuing Body, which can be either Agency or Joint Authorization Board (JAB), reviews assessment package and accepts risk.

3. Continuous Monitoring
   - **Continuous Review of Risk**
     • Oversight of the Cloud Service Provider’s Continuous Monitoring Service through either Live Data Feeds or Measures of Measures.

- Over time, FedRAMP operational models can permutate based on who performs each phase, and the option chosen for that phase.
FedRAMP: Public Comment Period

FedRAMP Documentation Public Comment Period
• November 2, 2010 – January 17, 2011
• Spawned 1000+ Comments
  • ~1/3 were on Policy Issues
  • ~1/3 were on Technical Issues
  • ~1/3 were on the Security Requirements

Review of Comment Period
• Initial review of comments to provide trend analysis and consolidate similar comments and identify themes – PMO
• 5 Tiger Teams of volunteers from across government to review the comments by themes
• Currently finalizing the comments and Tiger Teams recommendations for presentation to the Federal CIO – PMO
Security Controls

- All controls that were challenged or questioned were reviewed by a TIGER team.
- Recommendations from the Tiger Team were presented to the JAB.
- After review by the JAB, a number of controls were eliminated for both the Moderate and Low Baseline.

Continuous Monitoring

- Currently working with NSA and ISIMC CM WG to prioritize and categorize the FedRAMP Security Controls for more effective continuous monitoring.
- NSA and ISIMC CM WG are focusing on automated monitoring of a subset of controls and inferring compliance with the larger set of controls.
- **Proposing to separate FedRAMP Controls into to 3 groups**
  1. Controls that are going to be monitored in near real time
  2. Controls that require reporting at defined intervals
  3. Controls that have inferred compliance because of 1 or 2
Policy Issues: Recommendations

**Policy Issues**

- Examples of Areas of Focus:
  - Ensuring 3rd Party Assessors’ independence
  - What entity (Security Operations Center) will do FedRAMP Continuous Monitoring?
  - How will FedRAMP work to minimize duplicative FISMA reporting?
  - How will TIC work within FedRAMP?
  - What kind of ATO can FedRAMP give?

**Technical Issues**

- Examples of Areas of Focus:
  - Privacy Concerns
  - FedRAMP Sponsorship / Eligibility Requirements
  - Change Management Issues
  - Consistent Reporting Mechanisms
  - Security Controls Roles and Responsibilities