Federal Risk and Authorization Management Program

FedRAMP

Update for the

Information Security and Privacy Advisory Board

October 28, 2011

Why FedRAMP?
Problem, Solution and Key Benefits

PROBLEM:

•Duplicative, inconsistent, costly and inefficient cloud security risk management approach

•Little incentive to leverage existing ATOs among agencies – no standard controls, inconsistent application of C&A processes, no repository of relevant information

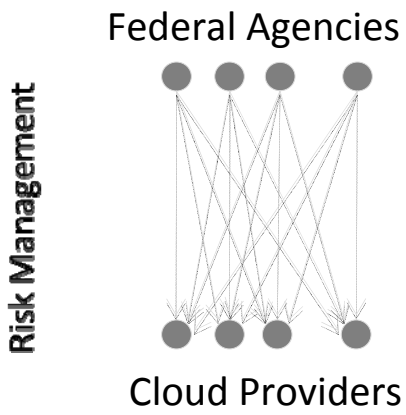
SOLUTION: FedRAMP

- Unified risk management allows for joint security authorization, continuous monitoring and independent third party assessment
- Uniform set of approved, minimum security controls and consistent assessment process for cloud computing solutions
- Based on "do once, use many" concept - agencies need only focus on assessment requirement deltas

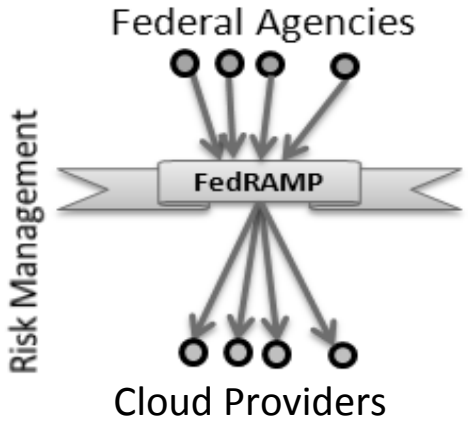
KEY BENEFITS:

- Efficient leveraging of ATOs across agencies
- Lowers overall costs for securing systems
- Fosters government-wide cloud adoption
- Improves assessment transparency and risk management
- Leverages monitoring automation technologies
- Establishes a **trusted** relationship with cloud service providers

As-is Environment



New Environment



FedRAMP Service Scope

High-Level Summary of FedRAMP Scope of Services

- **Cloud Security Requirements:** Standardizes a minimum, baseline set of government-wide security controls based on *NIST Special Publication 800-37 Revision 1 Risk Management Framework* for low or moderate risk cloud systems.
- **Assessor Accreditation:** Manages process for accrediting independent, third-party assessors to ensure competency, consistency, and compliance.
- **Assessment & Authorization:** Validates cloud services provider's security authorization packages to ensure consistent application of standard controls. Empowers a Joint Authorization Board (JAB) comprised of CIOs from DoD, DHS, and GSA, to issue provisional authorization for cloud systems. Agencies can leverage this baseline in granting their own ATOs and focus on their specific requirements "delta" for any additional C&A work.
- **Continuous Monitoring:** Based on an *initial* set of controls, performs continuous monitoring, automates oversight of government-wide authorized systems, and notifies participating agencies of any system changes to the authorized risk posture.
- **Incident Response Coordination:** Coordinates control and management of incident response for FedRAMP authorized cloud systems.
- **Data Repository:** Maintains up-to-date list of all FedRAMP authorized systems; facilitates secure access to security authorization packages; maintains contracting templates, SLAs, etc.

FedRAMP: Addressing Three Cloud Barriers

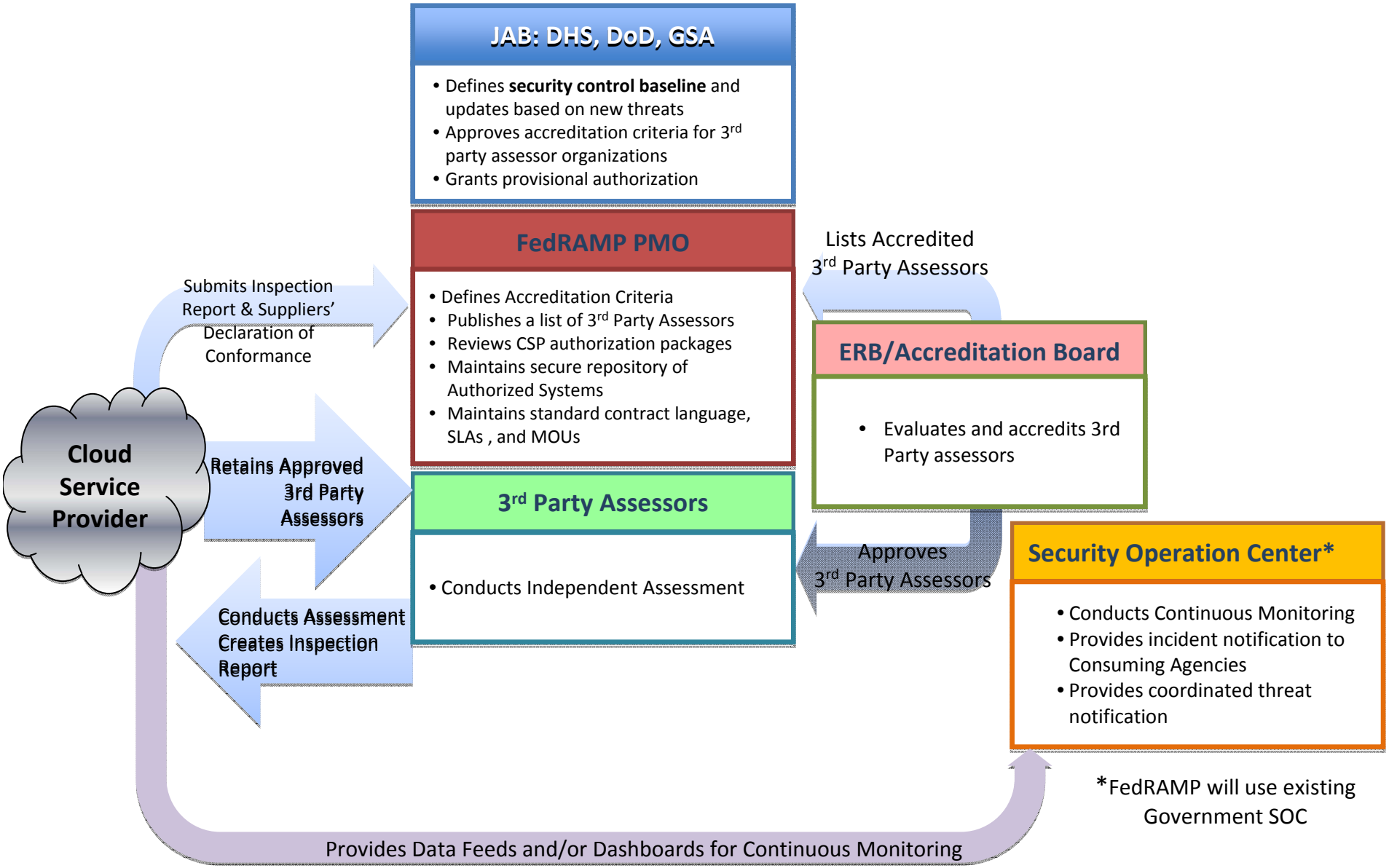
FedRAMP

Joint Authorization Board + Lightweight PMO

- **Maintains Security Baseline including Controls & Continuous Monitoring Requirements**
- **Maintains Assessment Criteria**
- **Maintains Active Inventory of Approved Systems**

Consistency and Quality	***Trustworthy & Re-useable***	***Near Real -Time Assurance***
1 Assessment	2 Provisional Authorization	3 Continuous Monitoring
Independent Assessment	***Grant Provisional Authorization***	***Continuous Review of Risk***
•Before granting a provisional authorizations, Cloud Service Provider systems must be assessed by an approved, Independent 3rd party assessor.	•Joint Authorization Board reviews assessments/grants provisional authorizations •Agencies issue ATOs using risk tolerance.	•Oversight of the Cloud Service Provider's continuous monitoring service through live data feeds or dashboards.
Independent Assessors are retained from FedRAMP approved list of 3rd party assessor organizations	**Authorizations Granted By:** ❑Joint Authorization Board – Provisional ❑Buying Agency – ATO	**CM Can Be Conducted Through:** ❑Leveraging an Existing SOC (DHS) ❑Using a Buyer Agency's SOC

FedRAMP Process



FedRAMP: Next Steps

- ✓ **Policy Memo:** OMB finalizing policy memo, release to agencies
- ✓ **Security Baseline Controls:** Publish controls, including continuous monitoring requirements
- ✓ **Conformity Assessment Model:** Publish requirements for 3rd Party Independent Assessors (FedBizOps) and begin accepting applications
- ✓ **Continuous Monitoring controls:** Working with NIST and DHS to incorporate initial set into CyberScope/US CERT
- ✓ **Communications and Outreach:** Conduct community briefings with industry associations, agencies, press, relevant Hill committees, and audit community to ensure understanding of program
- ✓ **Launch Initial Operations**
- ✓ **Continuous Improvement as Expanded**