Grant Thornton

Cloud Security in the Federal Sector:

FedRAMP (Federal Risk and Authorization Management Program)

Rex Booth, CISSP, PMP

Senior Manager, Grant Thornton LLP

Agenda

- Federal Adoption and Regulation of Cloud Services
  - Introduction
  - Cloud computing: the push for adoption in the Federal sector
  - FedRAMP – elements, governance, and process
  - FedRAMP – efficiencies and shortcomings
- Questions

Many thanks to Kurt Garbars, Senior Agency Information Security Officer, GSA, and Chair, Cloud Computing Security Working Group, for the content of some of these slides…

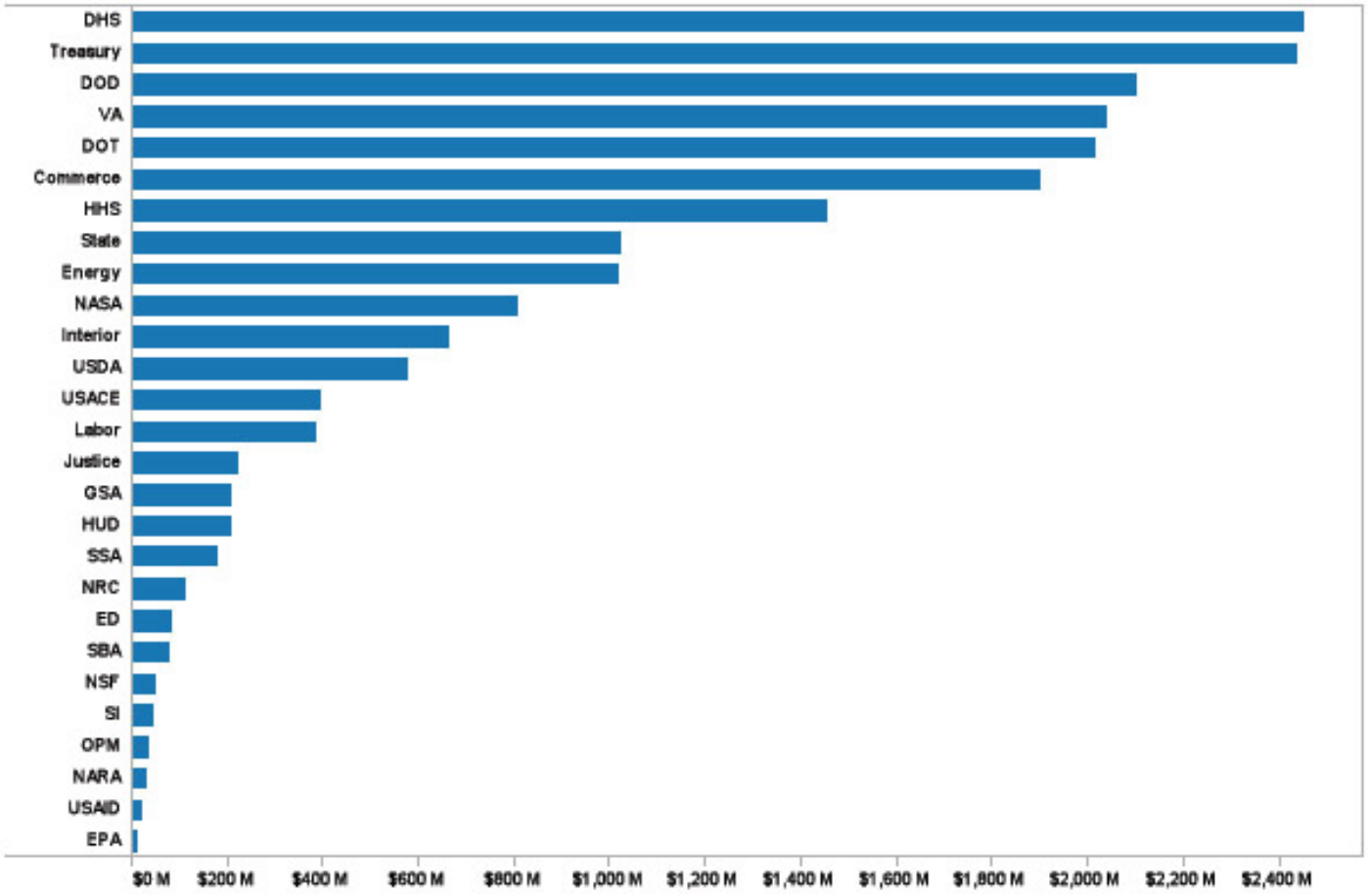
Cloud Within the Federal Sector

- The push for cloud adoption
  - Part of a larger drive for efficiency (data center consolidation, etc)
- Cloud computing strategy released February 8, 2011
  - Estimates $20B of the $80B Federal IT budget could be spent on cloud computing
  - Builds on "Cloud First" policy (part of the administration's 25 point IT plan)
- Embraces all cloud service models
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
- The Feds have invaded the cloud already
  - NASA Nebula (community cloud focused on research)
  - USDA E-Mail migration

Cloud Within the Federal Sector

EFFICIENCY	
Cloud Benefits	**Current Environment**
• Improved asset utilization (server utilization > 60-70%) • Aggregated demand and accelerated system consolidation (e.g., Federal Data Center Consolidation Initiative) • Improved productivity in application development, application management, network, and end-user	• Low asset utilization (server utilization < 30% typical) • Fragmented demand and duplicative systems • Difficult-to-manage systems
AGILITY	
Cloud Benefits	**Current Environment**
• Purchase "as-a-service" from trusted cloud providers • Near-instantaneous increases and reductions in capacity • More responsive to urgent agency needs	• Years required to build data centers for new services • Months required to increase capacity of existing services
INNOVATION	
Cloud Benefits	**Current Environment**
• Shift focus from asset ownership to service management • Tap into private sector innovation • Encourages entrepreneurial culture • Better linked to emerging technologies (e.g., devices)	• Burdened by asset management • De-coupled from private sector innovation engines • Risk-adverse culture

Cloud Within the Federal Sector



Source: Agency estimates reported to the Office of Management and Budget (OMB).

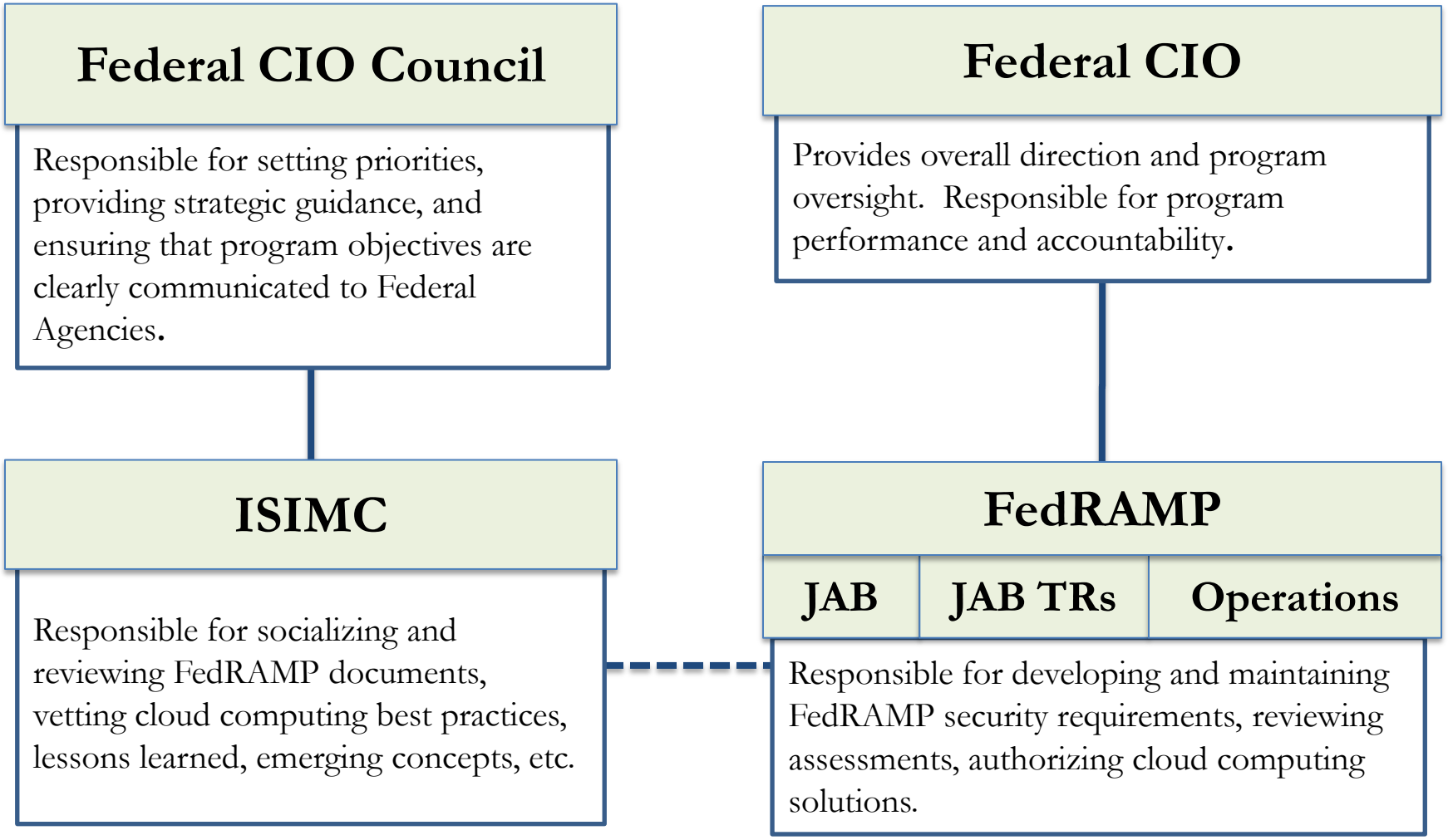
FedRAMP: Overview

- A government-wide initiative to provide joint authorization services
  - FedRAMP PMO in GSA
  - Unified government-wide risk management
  - Agencies would leverage FedRAMP authorizations (when applicable)
- Agencies retain their responsibility and authority to ensure use of systems that meet their security needs
- FedRAMP would provide an optional service to agencies
- Federal agencies will interact with FedRAMP in two ways:
  - Sponsoring a multi-agency cloud provider
  - Leveraging a FedRAMP authorized system

FedRAMP: Participants

- Joint Authorization Board (JAB)
  - DoD, DHS, GSA, Sponsoring Agency CIOs
  - Authorizes service provider to operate
- JAB Technical Representatives
  - Review of the authorization package
  - Recommendations to the Authorizing Officials
- FedRAMP Operations Office
  - Day-to-day support of the authorization process
  - Interacts with federal agencies and service providers
- Information Security and Identity Management Committee (ISIMC)
  - Creates guidelines for secure use of cloud computing by federal agencies including Federal CIO "Top 20" security issues
  - Socializes and reviews FedRAMP documents, vetting cloud best practices, lessons learned, emerging concepts, etc
- NIST
  - Provides technical support to FedRAMP for the application of security standards and guidelines to cloud computing

FedRAMP: Governance Model



FedRAMP: Governance Model

Roles and Responsibilities of the JAB

- Permanent members include DoD CIO, DHS CIO, GSA CIO
  - Sponsoring agency of specific cloud service provider (CSP)
- Responsibilities
  - Authorize CSPs to operate
  - Manage overall risk (both initially and ongoing)
  - Approve security requirements and A&A process used by FedRAMP
- Supported by JAB Technical Representatives (JABTR)
  - Technical staff under CIOs to provide recommendations and assistance to CIOs

FedRAMP: Process

There are 3 ways a Cloud Service can be proposed for FedRAMP Authorization:

1

Cloud BPA

Cloud Services through FCCI BPAs

2

Government Cloud Systems

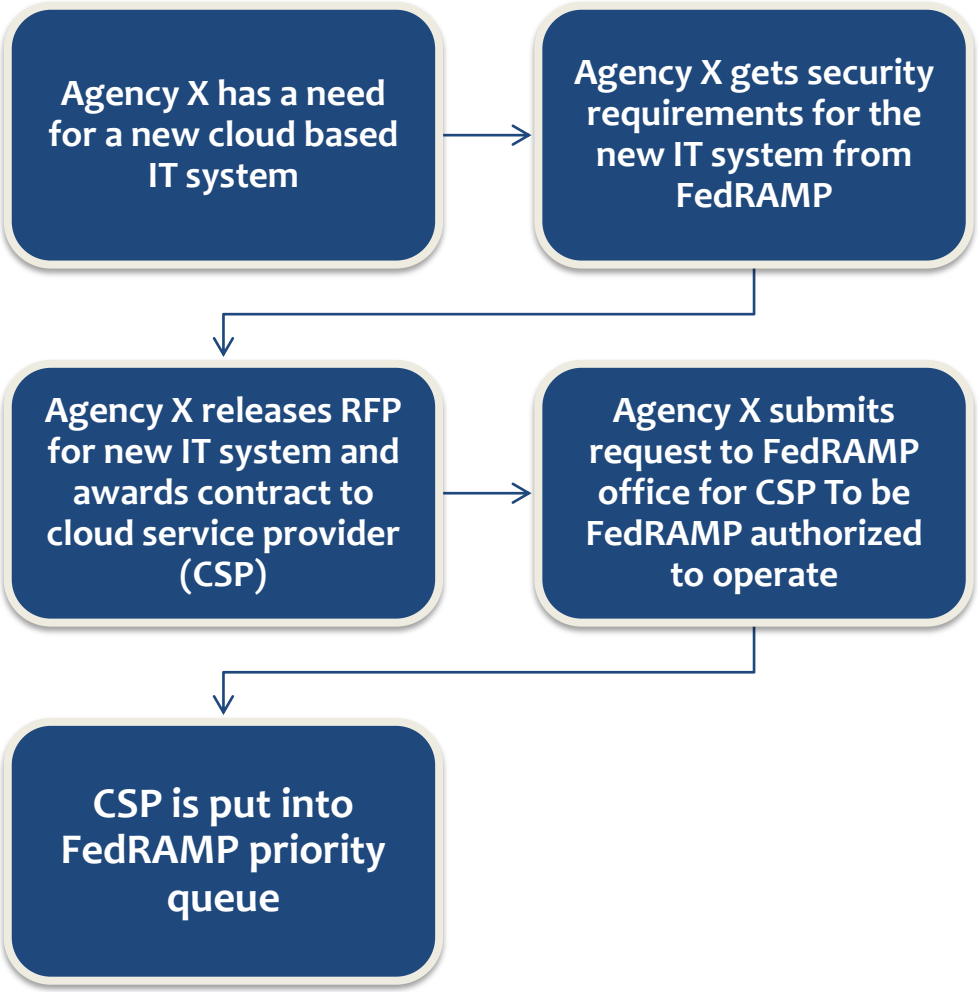
Services must be intended for use by multiple agencies

3

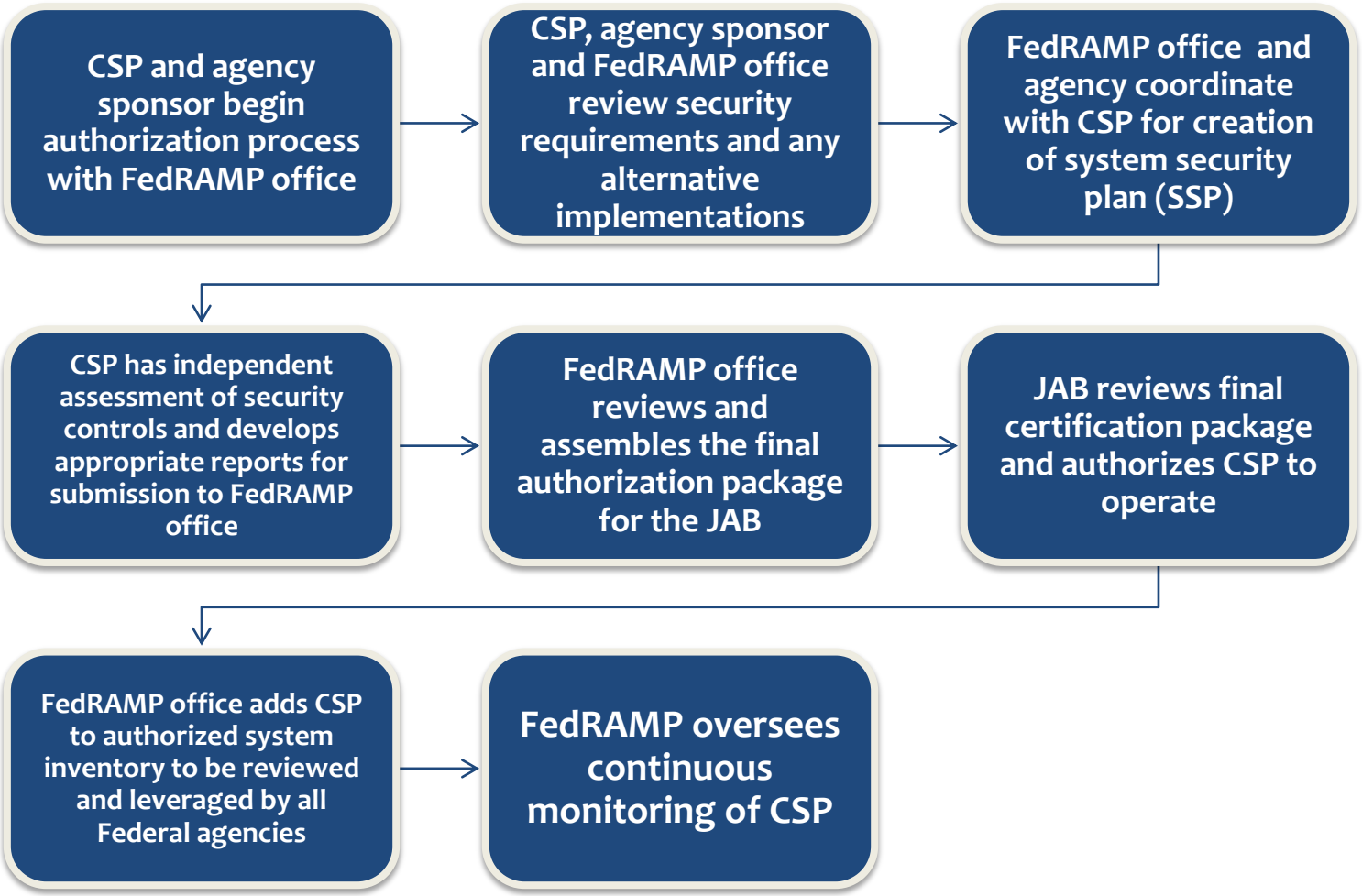
Agency Sponsorship

- Primary Agency Sponsorship
- Primary Agency Contract
- Secondary Agency Sponsorship

FedRAMP: Process



FedRAMP: Process



FedRAMP: Control Requirements

- Authorization process is based on current NIST guidance
- Controls based on NIST SP 800-53R3
- Cloud Computing Security Working Group (CCSWG) worked with the JAB over the past 10 months in creating controls
  - Members from agencies across government
- 13 additional controls/enhancements for low impact systems
- Approximately 60 additional controls/enhancements for moderate impact systems
- FIPS 199 and 800-37 R1 apply

FedRAMP: Control Requirements

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AC-18	Wireless Access	AC-18	AC-18 AC-18 (1) **AC-18 (2)** **AC-18 (3)** **AC-18 (4)** **AC-18 (5)**	**AC-18 (2)** [*Assignment: organization-defined frequency*] Parameter: [at least quarterly]	None.
AC-19	Access Control for Mobile Devices	AC-19	AC-19 AC-19 (1) AC-19 (2) AC-19 (3)	AC-19g. [*Assignment: organization-defined inspection and preventative measures*] Parameter: See additional requirements and guidance.	AC-19g. Requirement: The service provider defines inspection and preventative measures. The measures are approved and accepted by JAB.
AC-20	Use of External Information Systems	AC-20	AC-20 AC-20 (1) AC-20 (2)	None.	None.
AC-21	**User-Based Collaboration and Information Sharing**	Not Selected	**AC-21**	**AC-21a.** [*Assignment: organization-defined information sharing circumstances where user discretion is required*] Parameter: See additional requirements and guidance. **AC-21b.** [*Assignment: list of organization-defined information sharing circumstances and automated mechanisms or manual processes required*] Parameter: See additional requirements and guidance.	**AC-21a.** Requirement: The service consumer defines information sharing circumstances where user discretion is required. **AC-21b.** Requirement: The service provider defines the mechanisms or manual processes for the information sharing circumstances defined by the service consumer.
AC-22	Publicly Accessible Content	AC-22	AC-22	AC-22d. [*Assignment: organization-defined frequency*] Parameter: [at least quarterly]	None.

FedRAMP: Control Responsibilities

- Agencies remain responsible for a variety of controls (e.g SaaS):
  - Security categorization
  - Privacy impact assessment
  - Account management (i.e. provisioning of users)
  - Identification and authentication (e.g. 2-factor, password policy)
  - Auditing and monitoring (e.g. audit log reviews)
- As an agency goes from SaaS to PaaS to IaaS, agency control requirement responsibilities increase

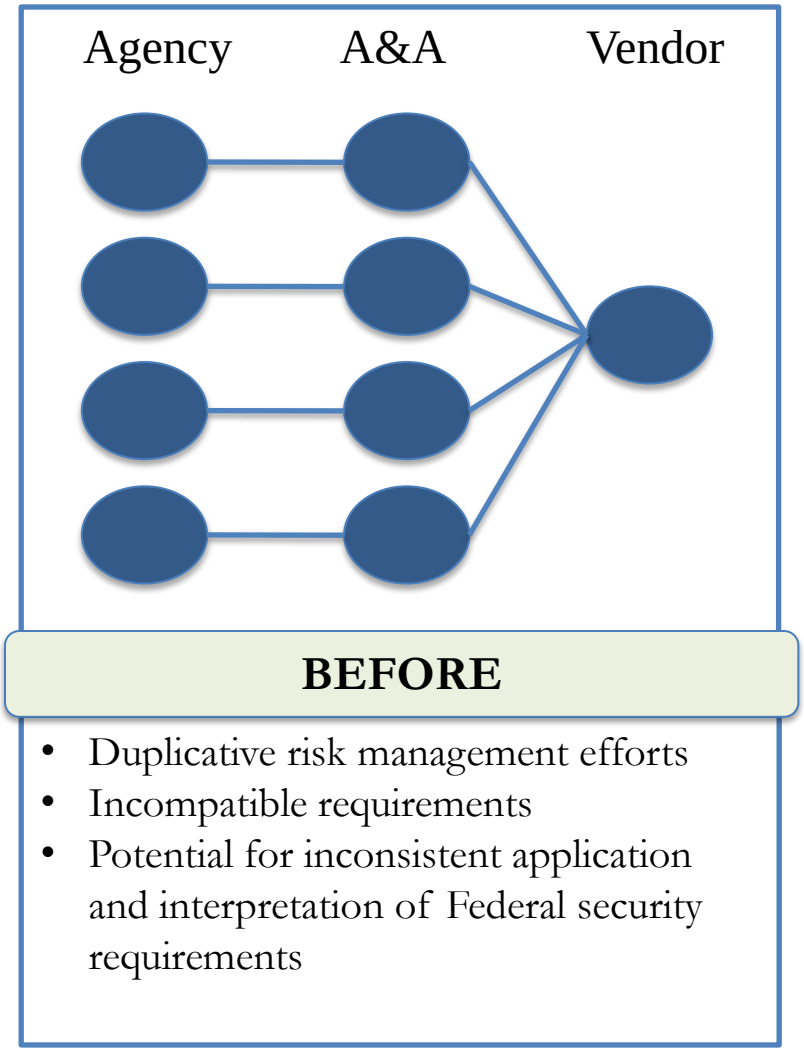
FedRAMP: Continuous Monitoring

- FedRAMP will perform continuous monitoring oversight of cloud service providers
- Monitoring of controls that fall within the system boundary defined in the service provider's SSP will be done by Independent 3rd party assessors hired by the CSP and also by the CSP depending on the control
  - *Please refer to the FedRAMP continuous monitoring section continuous monitoring deliverables and reporting requirements*
- Continuous monitoring of any controls that fall outside of the system boundary defined in service provider's SSP and identified as customer responsibility should be done by the customer Agency

FedRAMP: Continuous Monitoring

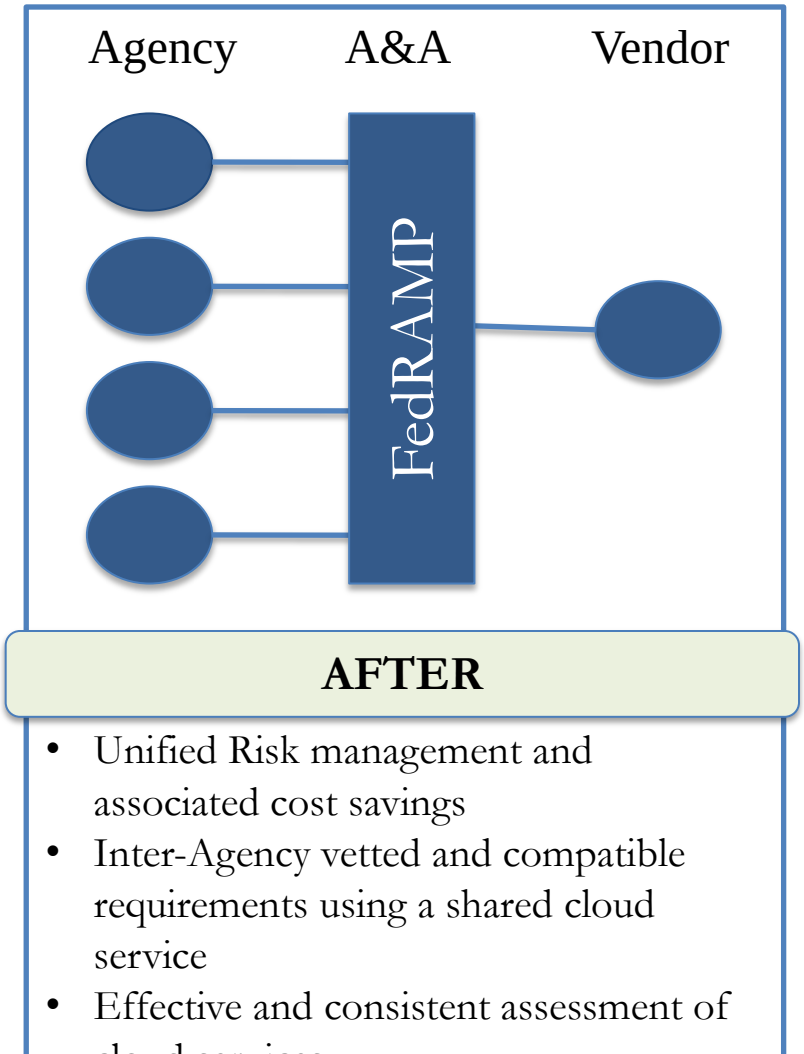
- Continuous monitoring includes:
  - Maintenance of the system security plan
  - Vulnerability scans on a regular and continuous basis
  - Automated mechanism for verifying configuration settings
  - Monitoring of operational and management controls
  - Situational awareness and incident response
  - Ability to add or remove controls throughout the lifecycle of the system
    - FedRAMP will ask for implementation plans
    - Ability to respond to new threats
  - FISMA reporting
  - Watch the watcher……. Assess the assessor

FedRAMP: Efficiencies



BEFORE

- Duplicative risk management efforts
- Incompatible requirements
- Potential for inconsistent application and interpretation of Federal security requirements



AFTER

- Unified Risk management and associated cost savings
- Inter-Agency vetted and compatible requirements using a shared cloud service
- Effective and consistent assessment of cloud services

FedRAMP: Efficiencies

Multi-Agency Use Saves Money

- Example – 3 Agencies, 3 Cloud Providers
  - Currently if each agency used all 3 providers
    - 9 full Assessment and Authorizations (A&A) would need to be performed
  - Under FedRAMP
    - 3 A&As could be leveraged
    - Cost savings of up to 67% for just 3 agencies and 3 providers
    - Transparent and consistent A&A help alleviate duplicative efforts

Continuous Monitoring Leveraging

- Continuous monitoring leveraged across agencies
  - FedRAMP oversees process, cloud service providers and independent assessors perform continuous monitoring activities
  - Agencies would only have to provide continuous monitoring on agency specific controls

FedRAMP: Shortcomings

- Too dependent on NIST 800-53
  - Lack of application-specific controls
  - Inherits focus on non-technical controls
- Infrequent "continuous monitoring"
  - Monthly or quarterly
  - Top threats to be assessed by DHS every 6 months
- Centralized structure removes some autonomy from agencies
- Federal CIO desire for sensitive information from vendors