Federal Risk and Authorization Management Program

Information Security and Privacy Advisory Board
August 5, 2010

Katie Lewin
Director, Cloud Computing Program, GSA

Kurt Garbars
Senior Agency Information Security Officer, GSA
Chair, Cloud Computing Security Working Group

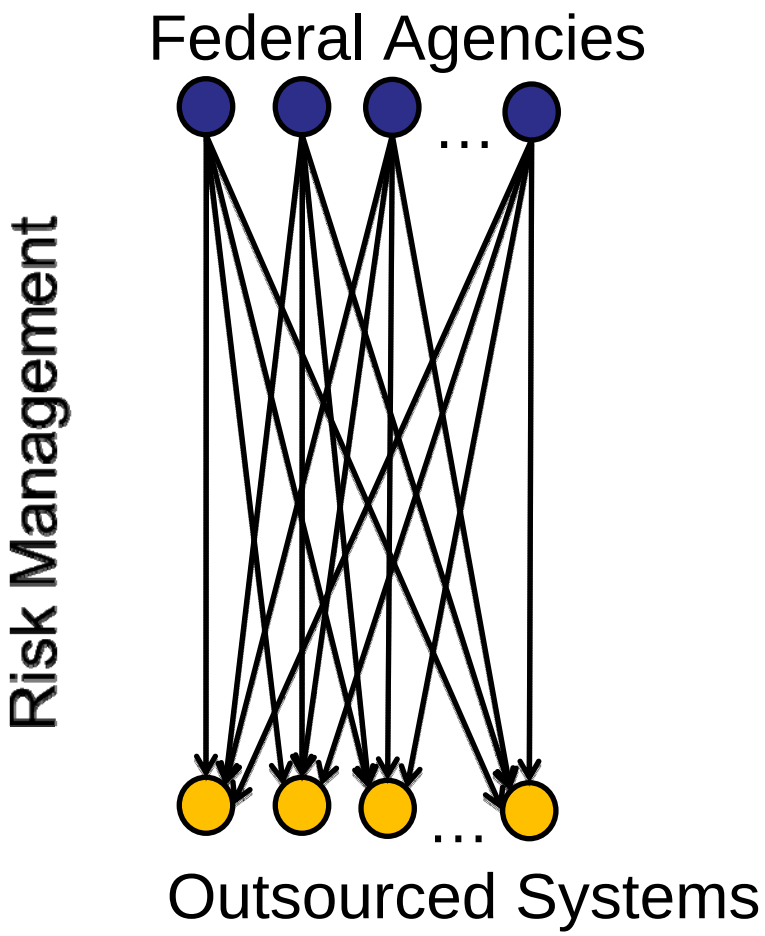
The Problem Statement

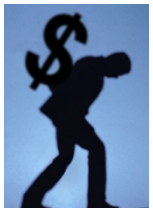
Problem: How do we best perform security authorization and continuous monitoring for large outsourced and multi-agency systems?

- Government is increasing its use of large shared and outsourced systems
  - Technical drivers: the move to cloud computing, virtualization, service orientation, and web 2.0
  - Cost savings: through datacenter and application consolidation
- Independent agency risk management of shared systems can create inefficiencies

FedRAMP

The Problem: Independent Agency Risk Management of Shared Systems





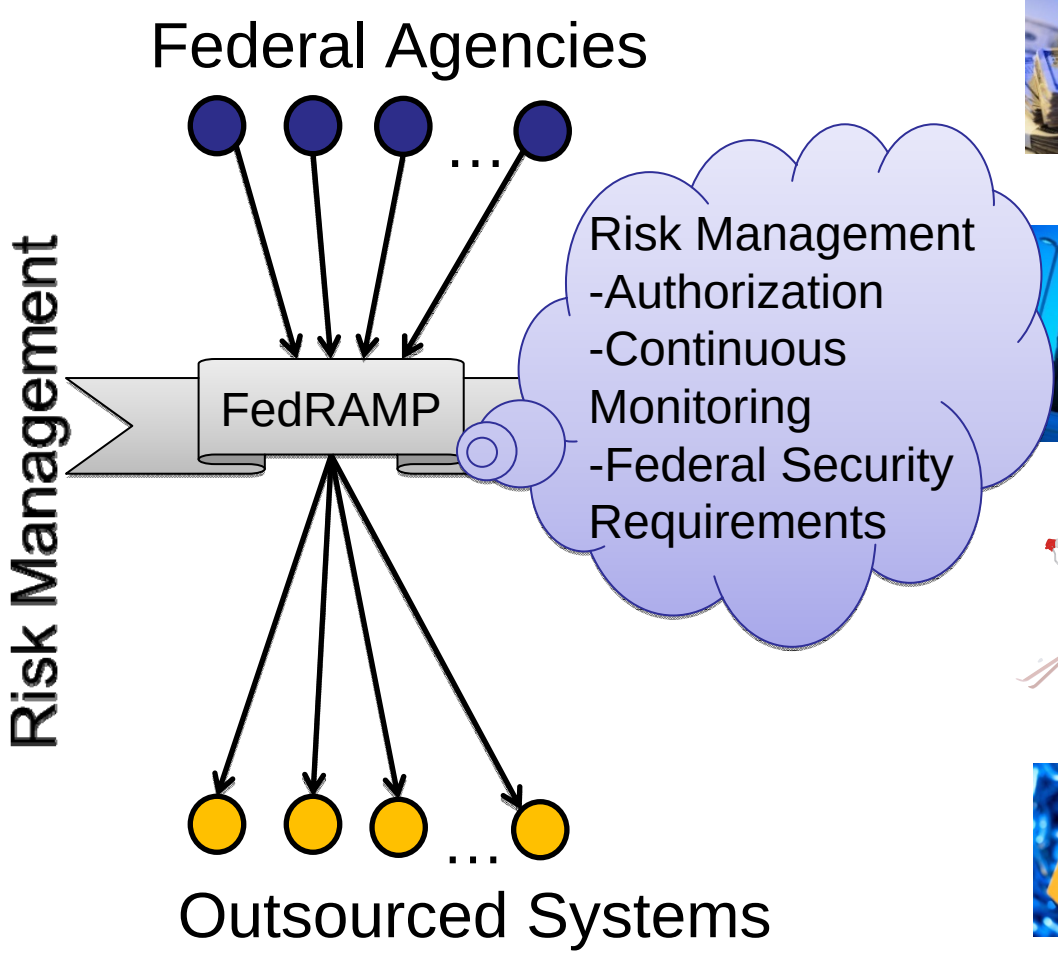
: Duplicative risk management efforts

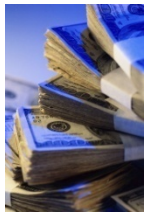
: Incompatible requirements

: Acquisition slowed by lengthy compliance processes

: Potential for inconsistent application of Federal security requirements

The Solution: Government-wide Risk Management of Shared Systems





: Risk management cost savings and increased effectiveness

: Interagency vetted approach

: Rapid acquisition through consolidated risk management

: Consistent application of Federal security requirements

FedRAMP: Federal Risk and Authorization Management Program

The Solution Concept: FedRAMP

Federal Risk and Authorization Management Program

- A government-wide initiative to provide joint authorization services
  - 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

Agency Perspective

Independent Agency Effort

Security Control Selection
Security Implementation
Security Assessment
Authorization
Plan of Action and Milestones
Monitoring

Leveraged Authorization

Review security details
Leverage the existing authorization
Secure agency usage of system

Assurance strengthened through focused effort

: Slower acquisition

: Significant effort

: Enables rapid acquisition

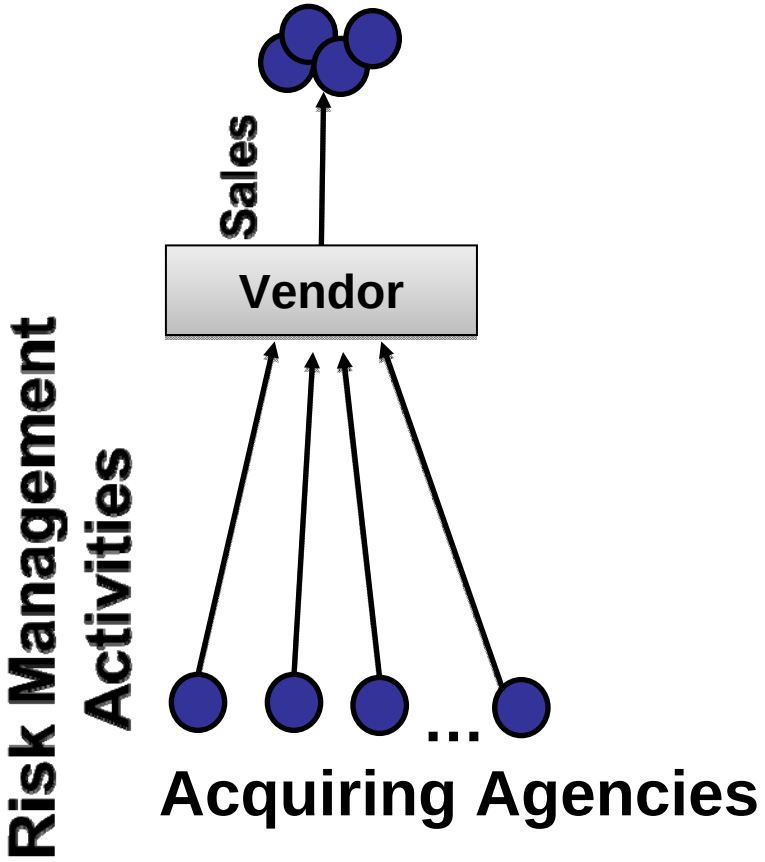
: Reduced effort

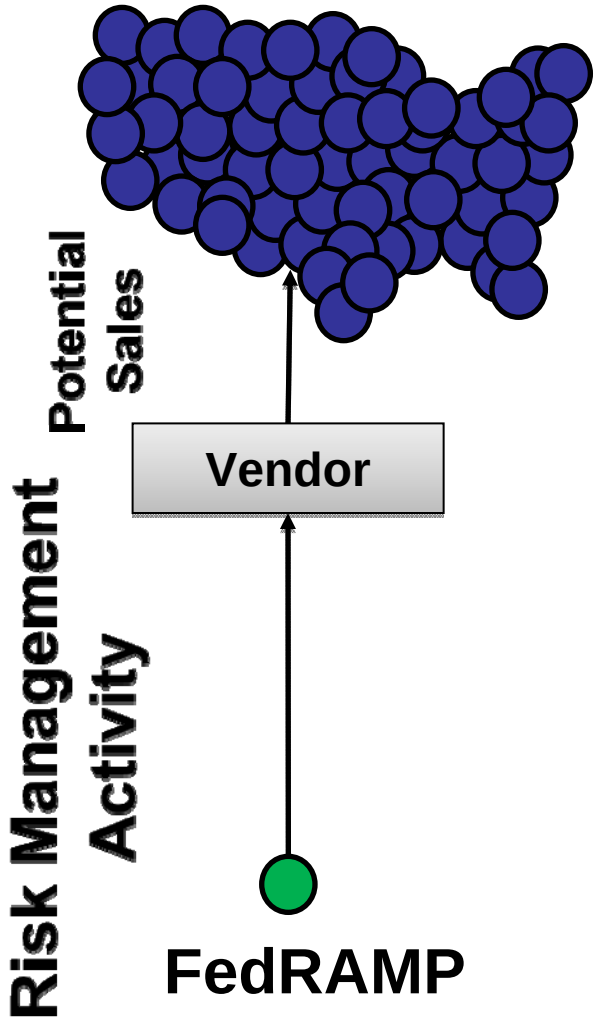
Agency Responsibilities

- Review FedRAMP authorization packages prior to making a decision to accept the risk
  - Determine suitability to agencies mission/risk posture
  - Determine if additional security work is needed
- Perform agency specific security activities
  - FedRAMP will publish a list of security controls that are the responsibility of the agency (can't be done government-wide)
  - Need for agency system security plans

Vendor Perspective

Coverage of the Federal market





- Products publicly listed as FedRAMP authorized

Scope for FedRAMP Office

- Centralized security authorizations of cloud computing systems (both commercial and government) to be used government-wide.

- Centralizing authorizations allow multiple Federal agencies to leverage a single security authorization.

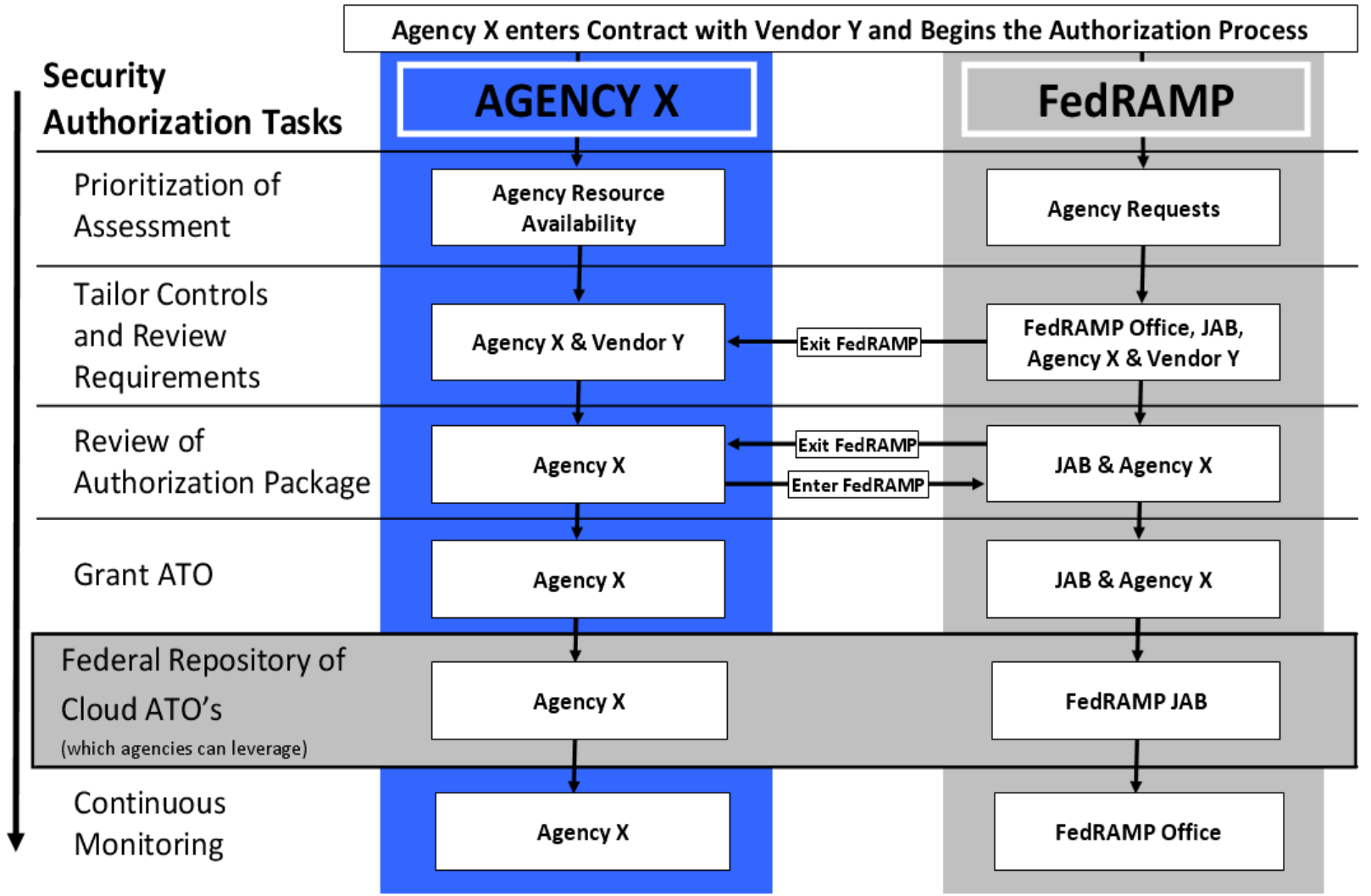
Assumptions for FedRAMP Office

- FedRAMP will NOT be a mandatory authorization process for agencies wishing to authorize cloud systems
- Size of the FedRAMP office will be controlled by available resources, cost model, funding, and demand from agencies
- FedRAMP will make public a set of common security requirements (CSR) and process documents which the FedRAMP Office and the Joint Authorization Board (JAB) will use to assess and authorize systems
- The security requirements and process documents used by the FedRAMP Office will be created and approved by the Cloud Computing Security Working Group (an interagency group within the Cloud Computing Working Group under the Federal CIO Council)
- FedRAMP will provide access to the authorization packages that document an ATO granted by a sponsoring agency or the JAB

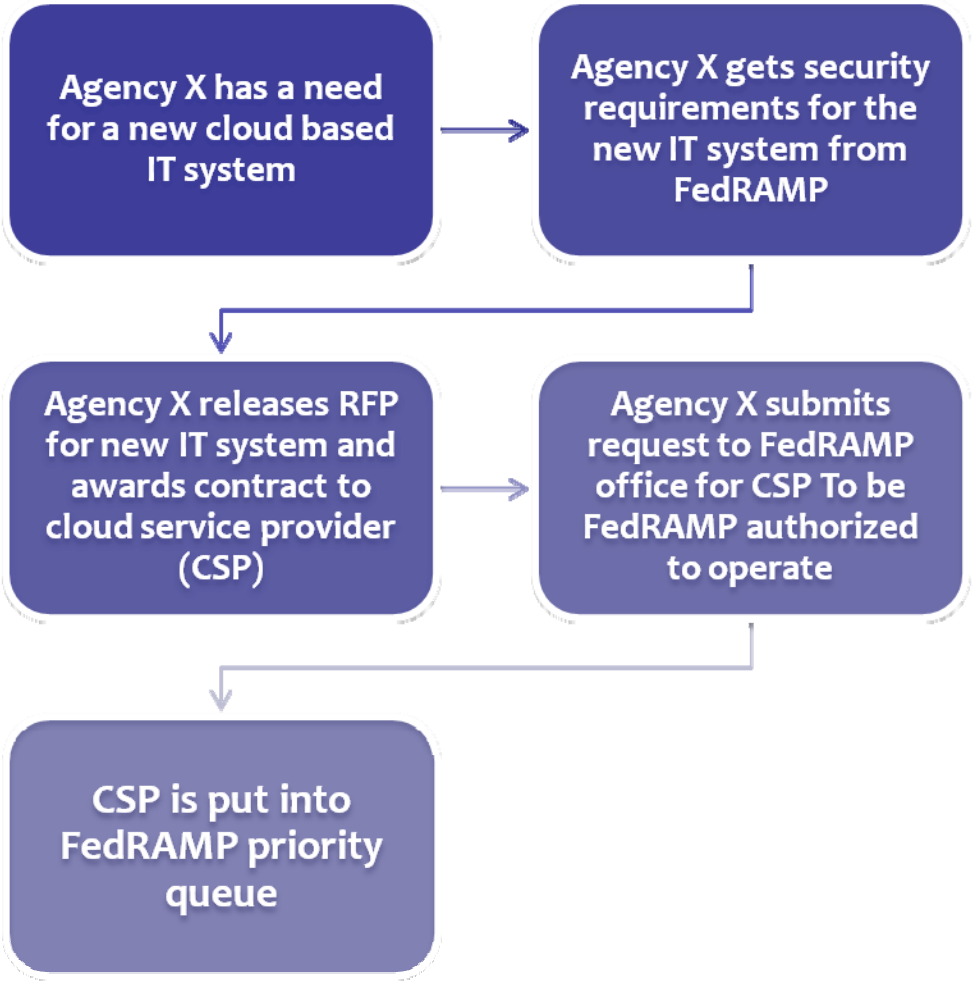
FedRAMP Authorization Process

- FedRAMP authorization process is based on current NIST guidance
  - NIST SP 800-37R1 (Risk Management Framework)
  - NIST SP 800-18 (System Security Plan)
  - NIST SP 800-53 R3 (Security Controls)
  - NIST SP 800-53A R1 (Security Assessment)
  - NIST SP 800-34 R1 (Contingency Planning)

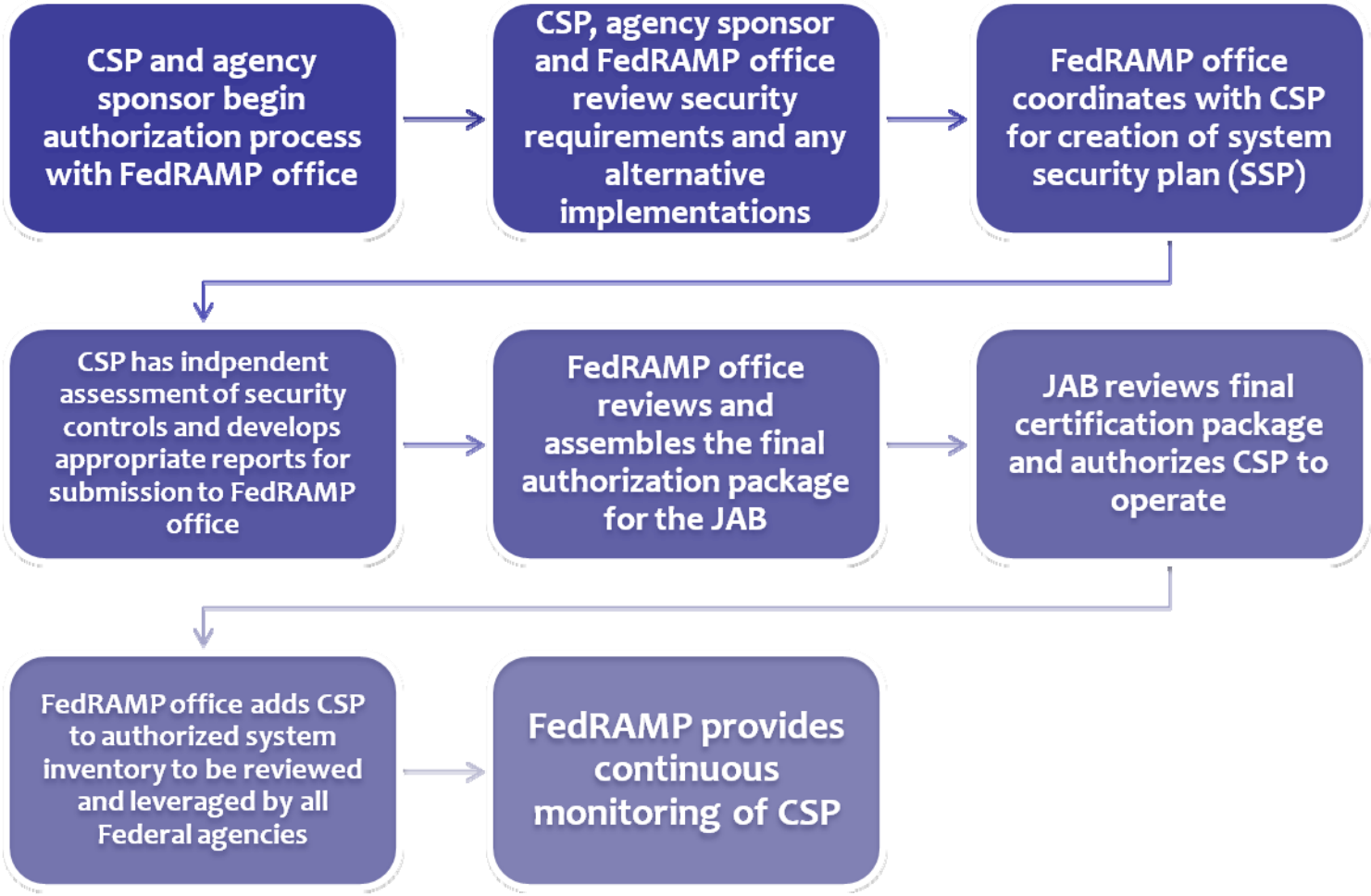
FedRAMP Authorization Models



FedRAMP Authorization Process

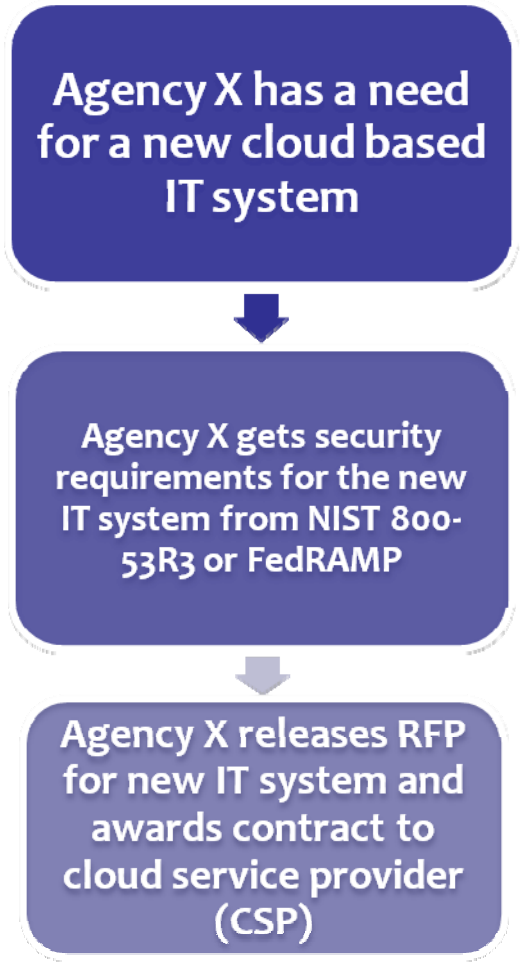


FedRAMP Authorization Process (cont)

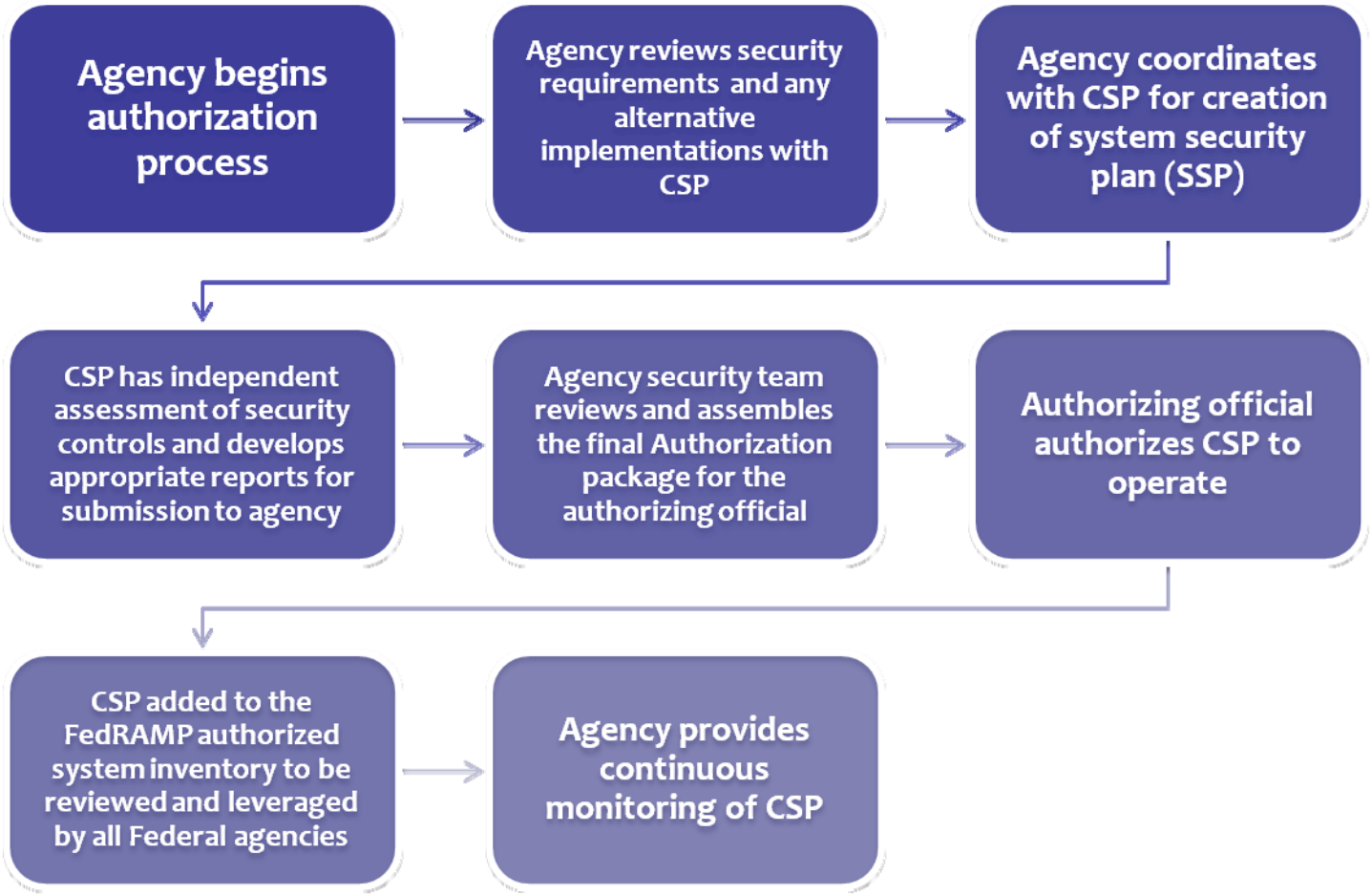


Agency-only Authorization Process

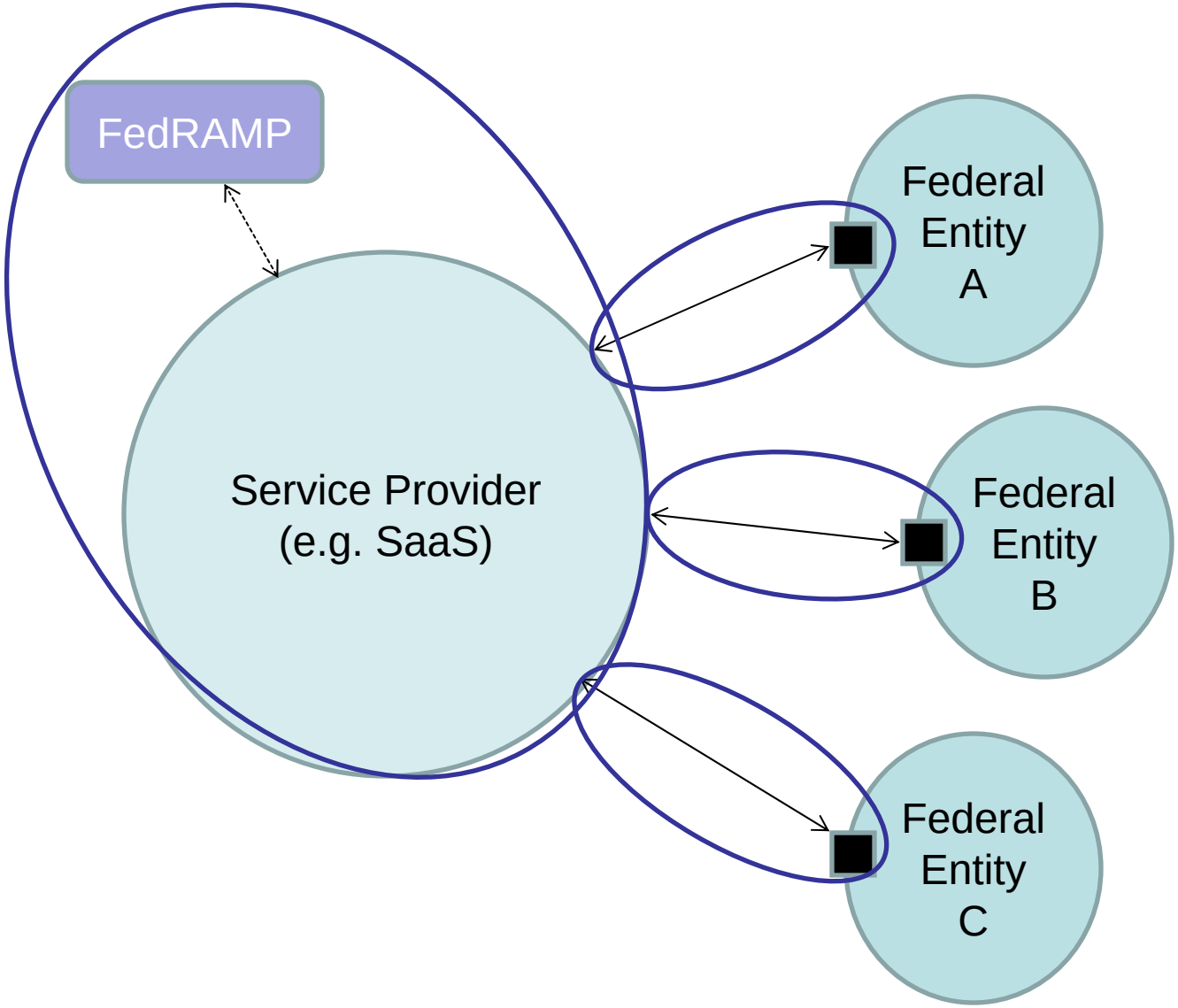
Process for Agency - Only Authorization:



Agency-only Authorization Process (cont)



System Boundaries – Leveraging C&A



Agency Control Responsibilities (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 Security Controls

GSA

- **Development of Controls**
  - The FedRAMP security controls are based on NIST SP 800-53 R3 controls for low and moderate impact systems
  - The CCSWG began working on the common security requirements during the winter of 2009 using GSA's work with Google as a baseline from which to start
  - The CCSWG went through iterations of the security controls taking input from the membership of the CCSWG (including but not limited to NASA, DoD, DOE, DHS, DOJ, HHS and NIST)
  - The CCSWG then submitted the common security requirement recommendations to the FedRAMP Joint Authorization Board (JAB) for review.

FedRAMP Security Controls (cont)

GSA

- **FedRAMP JAB Review of Controls**
  - FedRAMP JAB is comprised of 3 permanent members – DoD, DHS, and GSA.
  - The JAB technical representatives met over the course of 3 months to review the security controls to align them with what their respective agencies would require for cloud systems.
  - The JAB technical representatives approved version 1 of the common security requirements in June of 2010.
- **Nature of Common Security Requirements**
  - The common security requirements are for moderate and low Impact systems.
  - Heightened security requirements from 800-53 baseline
    - 13 additional controls and control enhancements for Low Systems
    - Approximately 50 additional controls and control enhancements for Moderate Systems
  - Additional requirements address issues of multi-tenancy, shared resource pooling, lack of trust, visibility, and control of the service provider's infrastructure.
  - Evaluated the high watermark of the JAB agency requirements and made adjustments to ensure that the requirements provide a high level of security without being overly restrictive

Questions