



## Federal Risk and Authorization Management Program (FedRAMP)

ISPAB Presentation

February 3, 2012

GSA

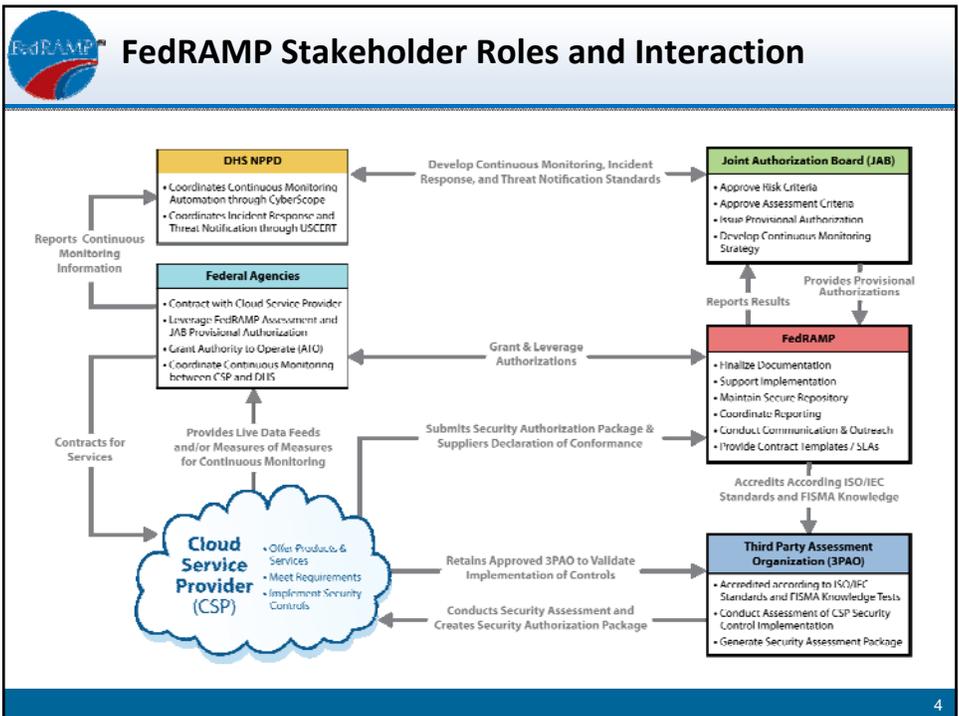
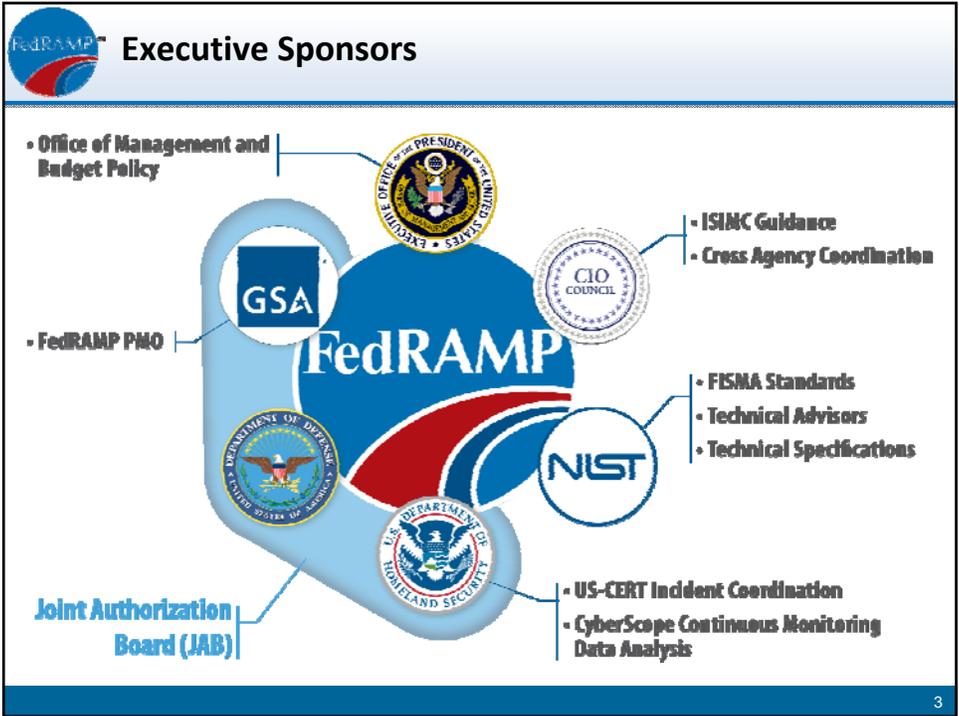


### What is FedRAMP?

*FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.*

- This approach uses a “do once, use many times” framework that will save cost, time, and staff required to conduct redundant agency security assessments.







## FedRAMP Phases and Timeline

Phased evolution towards sustainable operations allows for the management of risks, capture of lessons learned, and incremental rollout of capabilities

	FY12	FY12	FY13 Q2	FY14
	Pre Launch Activities	Initial Operational Capabilities (IOC)	Full Operations	Sustaining Operations
	Finalize Requirements and Documentation in Preparation of Launch	Launch IOC with Limited Scope and Cloud Service Provider (CSP)s	Execute Full Operational Capabilities with Manual Processes	Move to Full Implementation with On-Demand Scalability
<b>Key Activities</b>	<ul style="list-style-type: none"> <li>Publish FedRAMP Requirements (Security Controls, Templates, Guidance)</li> <li>Publish Agency Compliance Guidance</li> <li>Accredit 3PAOs</li> <li>Establish Priority Queue</li> </ul>	<ul style="list-style-type: none"> <li>Authorize CSPs</li> <li>Update CONOPS, Continuous Monitoring Requirements and CSP Guidance</li> </ul>	<ul style="list-style-type: none"> <li>Conduct Assessments &amp; Authorizations</li> <li>Scale Operations to Authorize More CSPs</li> </ul>	<ul style="list-style-type: none"> <li>Implement Electronic Authorization Repository</li> <li>Scale to Steady State Operations</li> </ul>
	Gather Feedback and Incorporate Lessons Learned			
<b>Outcomes</b>	<ul style="list-style-type: none"> <li>Initial List of Accredited 3PAOs</li> <li>Launch FedRAMP into Initial Operating Capabilities</li> </ul>	<ul style="list-style-type: none"> <li>Initial CSP Authorizations</li> <li>Established Performance Benchmark</li> </ul>	<ul style="list-style-type: none"> <li>Multiple CSP Authorizations</li> <li>Defined Business Model</li> <li>Measure Benchmarks</li> </ul>	<ul style="list-style-type: none"> <li>Authorizations Scale by Demand</li> <li>Implement Business Model</li> <li>Self-Sustaining Funding Model Covering Operations</li> <li>Privatized Accreditation Board</li> </ul>

## Federal Risk and Authorization Management Program (FedRAMP)

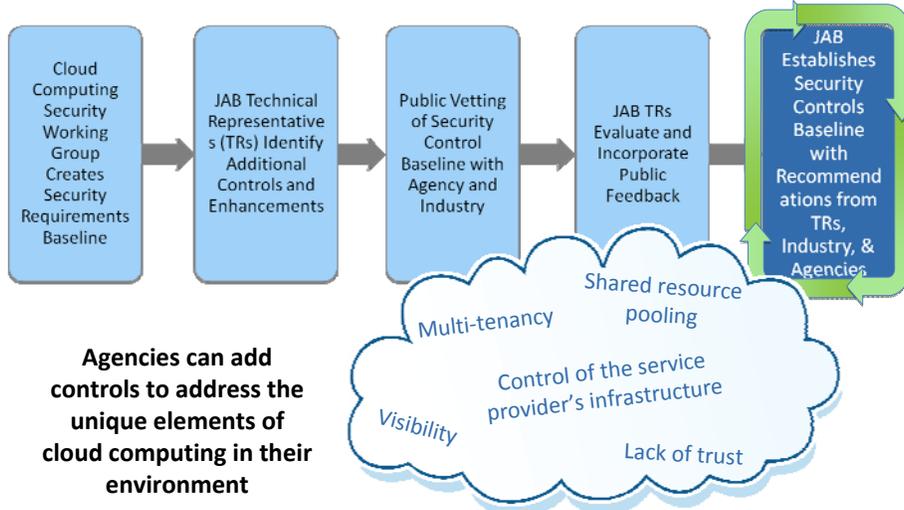
FedRAMP Security Controls Baseline





## Establishing Baseline FedRAMP Security Controls

Source of controls - NIST SP 800-53 R3 for low and moderate impact systems



7



## Security Controls

See [FedRAMP.gov](http://FedRAMP.gov) for list of security controls

Impact level	NIST Baseline Controls	Additional FedRAMP Controls	Total Controls Agreed to By JAB for FedRAMP
Low	115	1	116
Moderate	252	45	297

### Areas with additional controls

Access Control (6)	Audit and Accountability (5)	Security Assessment and Authorization (1)	Configuration Management (4)
Contingency Planning (2)	Identification and Authentication (3)	Incident Response (1)	Maintenance (1)
Media Protection (1)	Risk Assessment (4)	System and Services Acquisition (4)	System and Communications Protection (11)
System and Information Integrity (1)			

8



## Fully Implemented Control Examples

### Risk Acceptability Criteria:

- controls that must be fully implemented – or risk level is unacceptable for CSP risk posture
- established by JAB
- relate to OMB Policy Memos, NIST Special Publications, or other Federal mandates

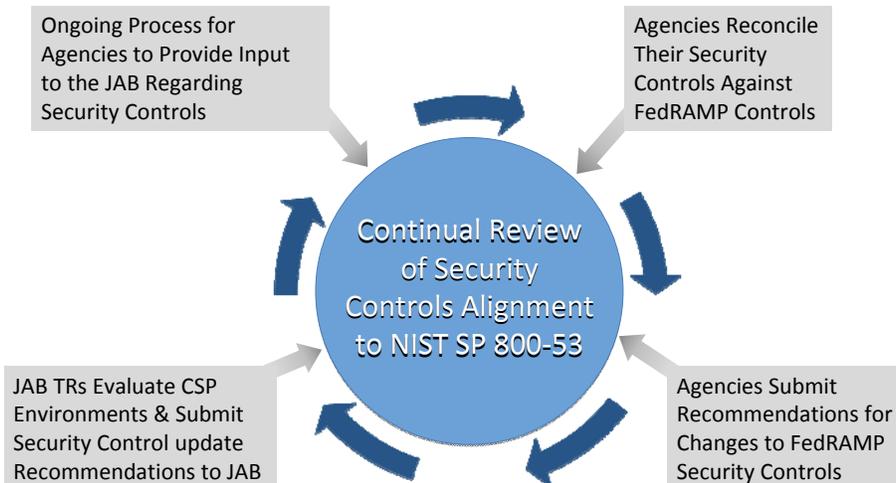
### Examples:

Description***	Rationale	Associated Controls
Two Factor Authentication for access	Provides additional assurance that the user has been identified and authentication.	IA-2 (1) (2) (3)
Incident Handling and Incident Reporting consistent with Federal Guidelines	CSPs must support agency needs in handling and reporting incidents.	IR-4, IR-6
Boundary protection and effective separation of logical and physical devices within the authorization boundary	All points surrounding the accreditation boundary must be identified and protected.	SC-7

\*\*\*The three criteria listed are not comprehensive. The risk acceptability criteria will be made publicly available once finalized by the JAB.



## Maintenance of Security Controls





## Agency Additional Controls

*FedRAMP baseline security controls standardize how Federal Agencies and CSPs assess and authorize cloud solutions for government use.*

Agencies may have a need to add additional controls to address specific agency security needs:

### Agency Adds Prior to FedRAMP JAB Initiation

- Agency adds controls during initiation with FedRAMP JAB
- JAB considers request and approves the controls for the Security Authorization Package for the specific CSP

*Agencies are responsible for Continuous Monitoring activities associated with the additional controls*

### Agency Adds After FedRAMP JAB Initiation

- Agency may negotiate additional controls with CSP directly
- Agency must assess controls, FedRAMP will NOT evaluate additional controls

*Agencies are responsible for the Continuous Monitoring activities associated with the additional controls*

### Agency Request Addition to FedRAMP Control Baseline

- Agency requests JAB to add controls to the Baseline
- "If controls are added to the Baseline, stakeholders will incorporate additional controls into their reviews - see change control process in the FedRAMP Concept of Operations

11



## FedRAMP Template Contract Clauses and SLAs

*The FedRAMP PMO will be releasing template contract clauses and SLAs for agencies to use when procuring cloud solutions*

### Standard Contract Clause Templates

- Templates will be designed for agencies to leverage for use within cloud procurements
- Templates will help agencies address:
  - Overall security requirements
  - Ensure all agency FedRAMP requirements are met within the contract
  - Address unique contract issues related to security such as data location, two factor authentication, etc.

### SLA Guidance

- Guidance will be designed to help agencies ensure CSP services meet acceptable levels of service
- Guidance will be aligned with NIST Cloud Computing Roadmap
- Guidance will help agencies address:
  - Unique areas per deployment model (infrastructure, software, platform)
  - Creating clear definitions for agreements

All templates and guidance are available for agencies to leverage, but are not FAR or official government clauses and can be altered as agencies see appropriate.

12

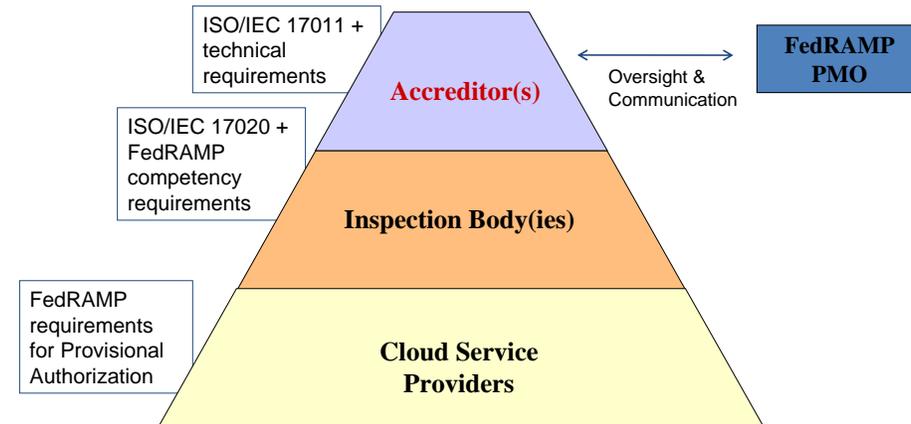


# Federal Risk and Authorization Management Program (FedRAMP)

## Overview of Third Party Assessment Organization (3PAO) Accreditation



## Notional Conformity Assessment Hierarchy for Inspection

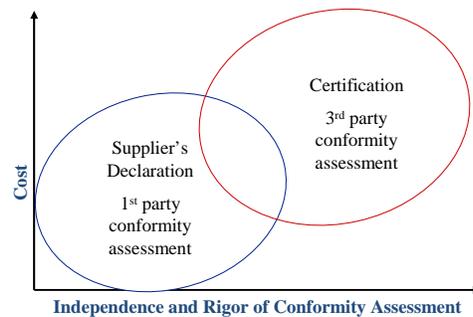


ISO/IEC 17011: Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies  
ISO/IEC 17020: General criteria for the operation of various types of bodies performing inspection



## Federal Programs using Conformity Assessment Approaches

- Examples: Health IT, FCC, CPSC (toys), WaterSense, CMVP
  - Balance confidence to impact of non-conformance
  - Maximize confidence and minimize market burden and cost
  - Maximize private sector business to minimize Fed resource



15



## 3PAO Conformity Assessment Process

***FedRAMP requires CSPs to use Third Party Assessment Organizations (3PAOs) to independently validate and verify that they meet FedRAMP security requirements***

***Conformity assessment process to accredit 3PAOs based on NIST program***

***Conformity assessment process accredits 3PAOs based on:***

- (1) Independence and quality management in accordance with ISO standards; and*
- (2) Technical competence through FISMA knowledge testing.*

**Benefits of leveraging a formal 3PAO approval process:**

- Consistency in performing security assessments
- Ensures 3PAO independence from Cloud Service Providers
- Establishes an approved list of 3PAOs for CSPs and Agencies to use

16



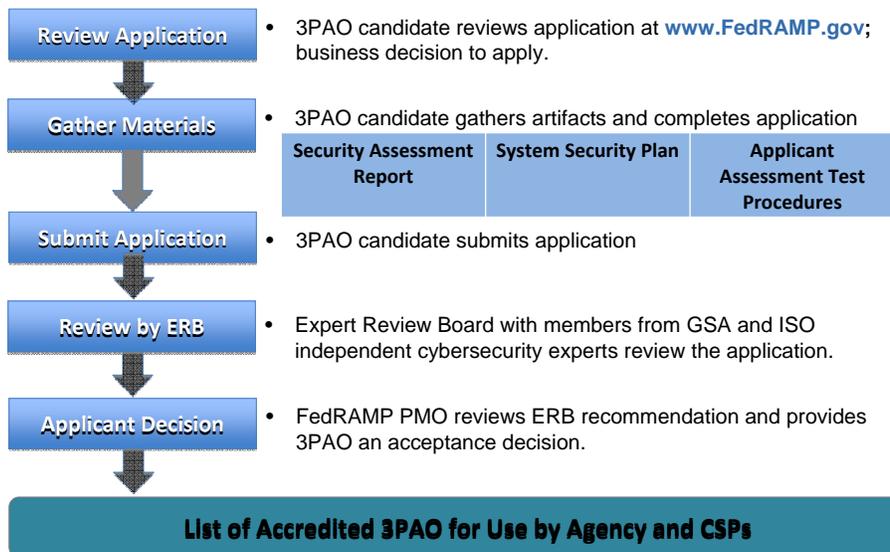
## 3PAO Technical Requirements

- Maintain competency in FedRAMP program requirements
- Maintain competency in assessment of cloud-based information systems
- Maintain quality system consistent with program requirements and supporting NIST publications
- Select assessment team personnel collectively that have relevant knowledge, skills and abilities for conduct of given security assessment
- Prepare Security Assessment Plan (SAP) for each assessment consistent with program requirements
- Review assessment plan with CSP
  - Appropriate for the computing environment
- Conduct security assessment following SAP
- Prepare Security Assessment Report (SAR) consistent with FedRAMP program requirements

17



## 3PAO Acceptance Process



18



## 3PAO Application Process

- Application received by today at 5:00 will be considered for initial list
- After initial batch, applications will be queued in order received
- Applicant undergoes a FedRAMP requirements evaluation by FedRAMP PMO and Expert Review Board (GSA & NIST)
  - Completeness check
  - Review of documents and evidence received with application form
  - Determination that applicant meets ISO/IEC 17020:1998
  - Determination that applicant has required technical competence
  - Determination that applicant meets additional FedRAMP program-specific requirements

19



## 3PAO Application Process (cont.)

- If requirement(s) are not met
  - Applicant receives a non-conformity letter
  - Applicant may address with a revised application
  - Non-conformance letters received prior to Jan 20 indicates that applicant will not be considered for initial list; however can be listed subsequently
- All applicants meeting the requirements
  - Receive an accreditation memo stating acceptance as FedRAMP 3PAO
  - Will be listed, AS A GROUP, on the initial list of FedRAMP-accredited 3PAOs
- Subsequent accredited 3PAOs will be added to the list, in real-time upon release of accreditation memo

20



## Federal Risk and Authorization Management Program (FedRAMP)

### Agency Responsibilities

GSA



### Agency Responsibilities



- Must use FedRAMP baseline controls and templates for initiating, reviewing, granting, and revoking security authorizations for cloud services
- Establish and implement continuous monitoring plans through incident response and mitigation capabilities
- Require cloud services providers to meet FedRAMP requirements via contractual provisions
- Identify Agency cloud services that cannot meet FedRAMP requirements including rationale and proposed resolution



## Agency Timeline

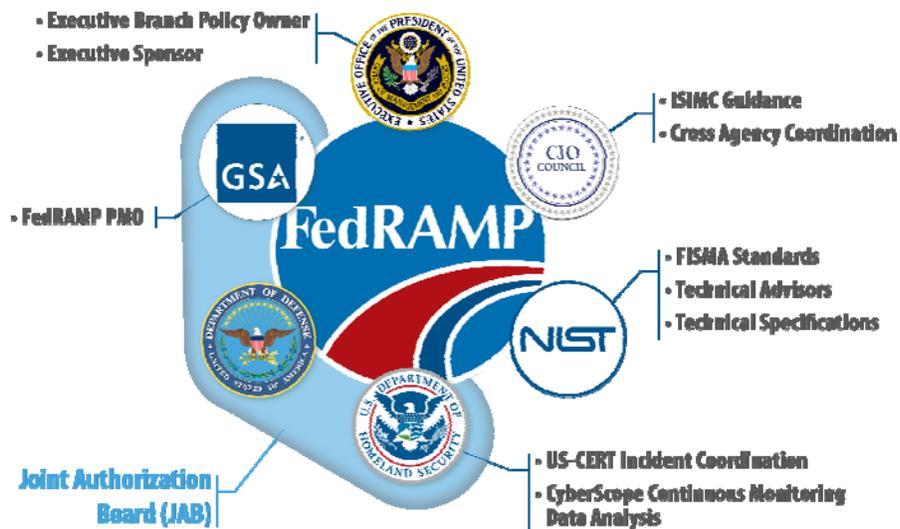


- **June 2012**
  - New cloud projects must begin using FedRAMP baseline controls and templates once FedRAMP has declared Initial Operating Capability
- **June 2014**
  - All cloud projects currently implemented or in the acquisition process have 2 years to meet FedRAMP requirements

23



## FedRAMP Stakeholders



24



## Executive Sponsor/CIO Council



- Established Federal policy for the protection of Federal information in cloud services – Memo released 12/8/11
- Described the key components of FedRAMP and its operational capabilities
- Defined Executive department and agency responsibilities using FedRAMP in the acquisition of cloud services
- **Send questions about FedRAMP policy to [fedramp@omb.eop.gov](mailto:fedramp@omb.eop.gov)**



- Publish and disseminate information from the FedRAMP PMO and JAB to Executive departments and agencies including:
  - Standardized baseline of security controls, privacy controls, and controls selected for continuous monitoring
- Coordinate vetting of controls and requirements from JAB

25



## Joint Authorization Board – DoD, DHS, GSA

- Define FedRAMP security authorization requirements
- Approve accreditation criteria for third party assessment organizations
- Establish a priority queue for authorization package reviews
- Review FedRAMP authorization packages
- Grant joint provisional authorizations
- Ensure that provisional authorizations are reviewed and updated regularly



26



## NIST/DHS



- Developed 3PAO Conformity Assessment Program
- Technical advisors regarding FISMA compliance through special publications
  - SP800-53, 800-37, FIPS 199 & 200
- Advise JAB on compliance requirements



- Leads operations of agency cybersecurity - FISMA
- Manages FedRAMP continuous monitoring
  - Data feed criteria
  - Reporting structure
  - Threat notification coordination
  - Incident response

27



## General Services Administration

- Liaison between Agencies, CSPs, and JAB to provide FedRAMP provisional authorizations
- Delivers program communication
- Creates contract language templates and sample service level agreements for use in cloud service acquisitions
- Creates standard process flows, procedures and templates for agencies to use



28

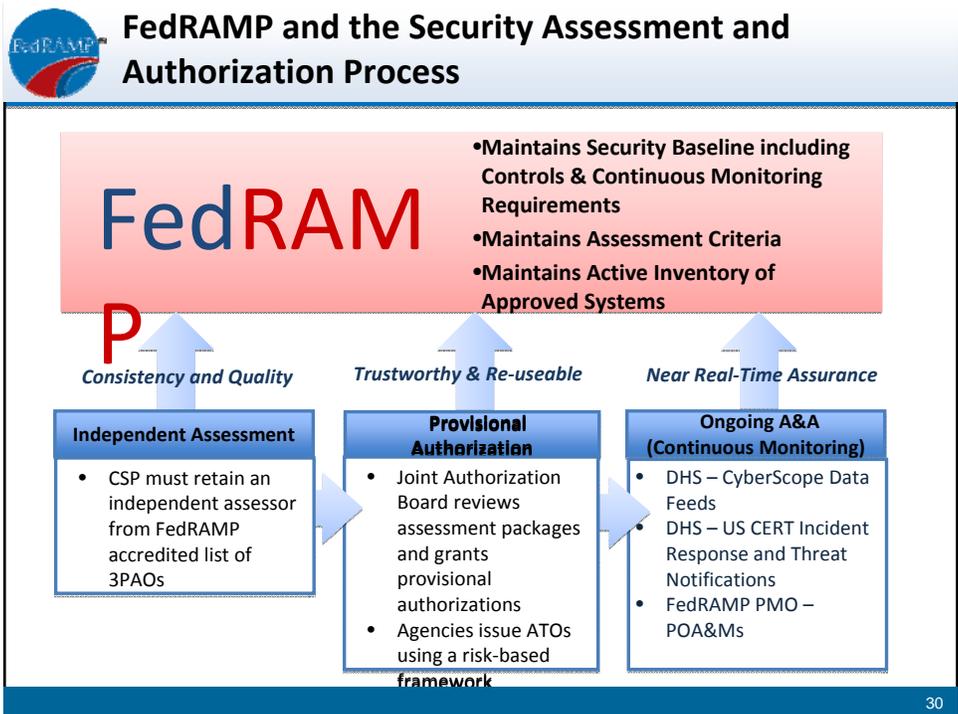


# Federal Risk and Authorization Management Program (FedRAMP)

## FedRAMP Concept of Operations Overview

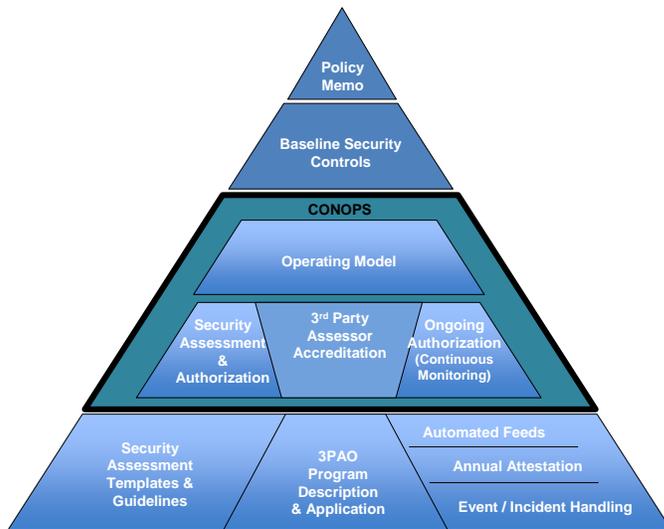
Matthew Goodrich  
 FedRAMP Program Manager  
 GSA Office of Citizen Services and Innovative Technologies







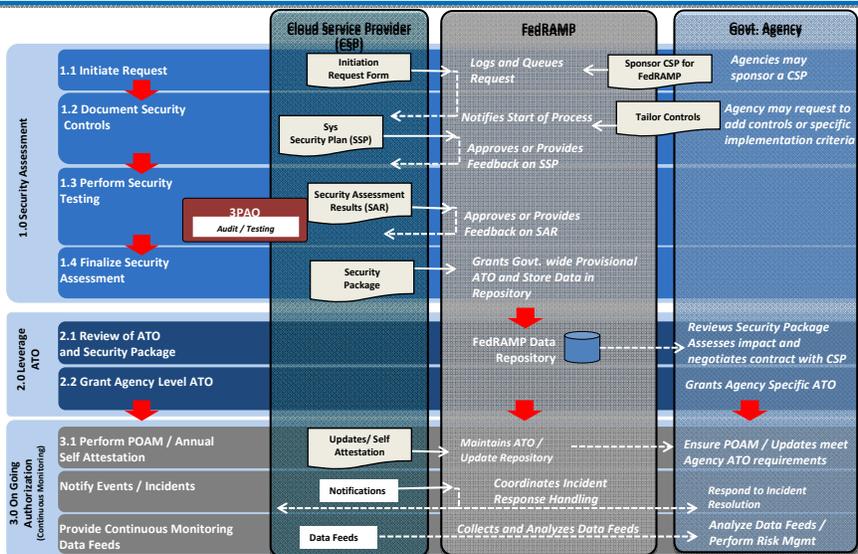
## FedRAMP Document Hierarchy



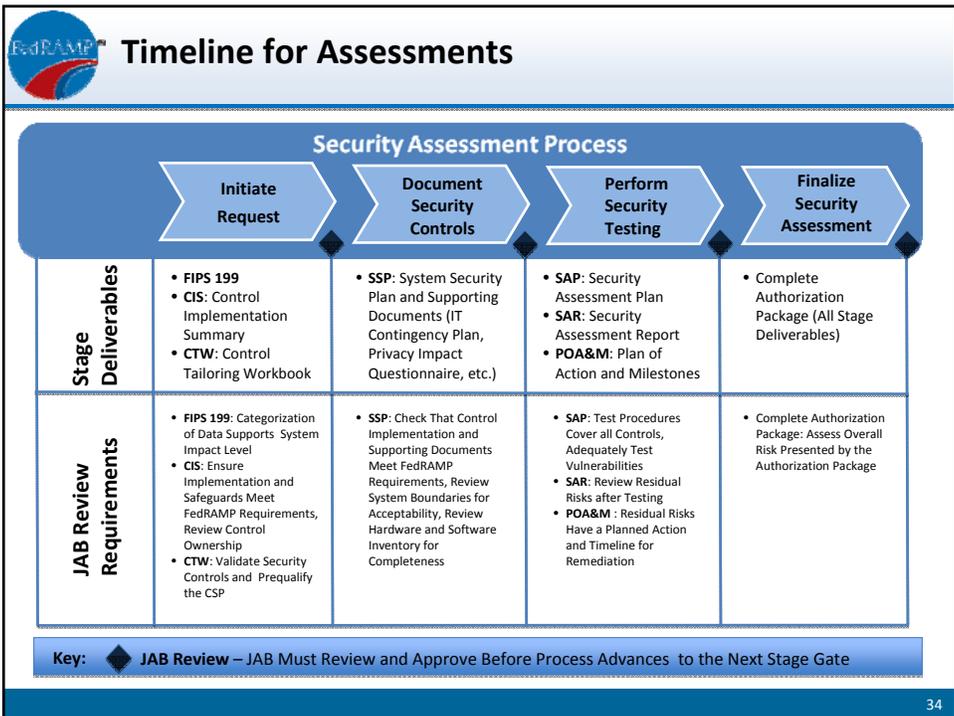
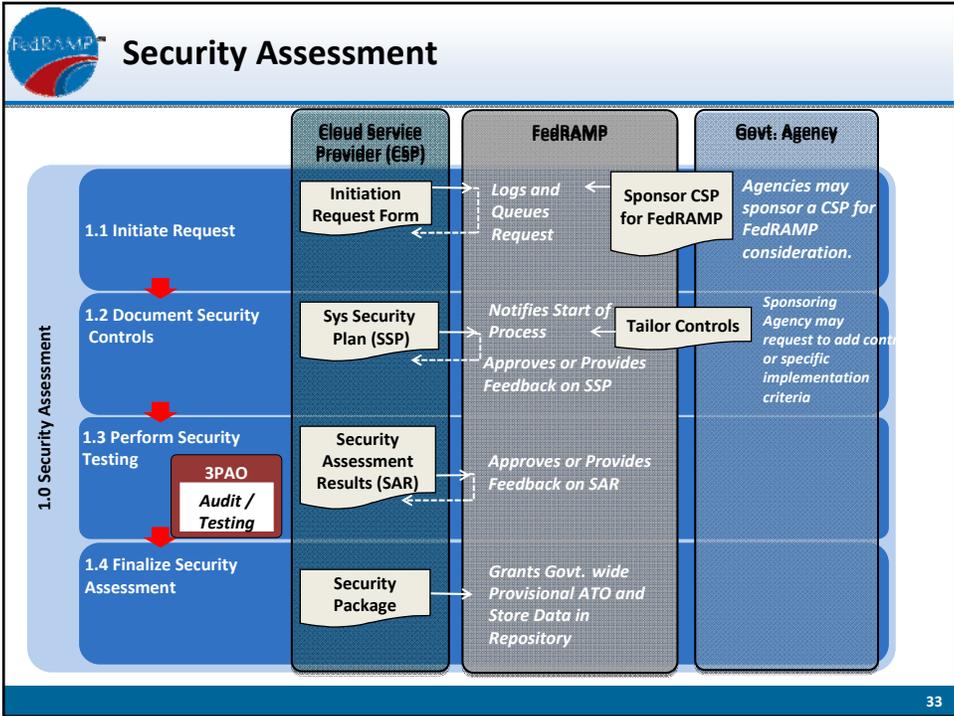
31



## FedRAMP Concept of Operations – High Level

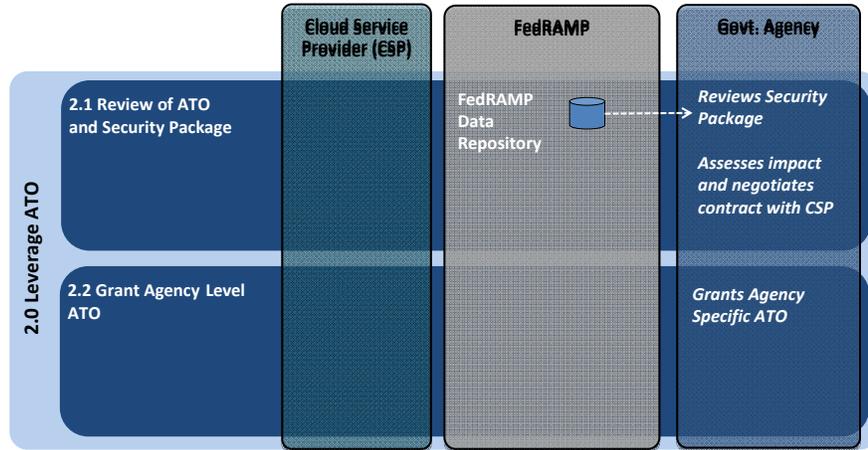


32





## Leveraging Authorizations



35



## FedRAMP Repository

*FedRAMP will maintain a repository of standardized security assessment packages Federal Agencies can leverage to make their own risk-based decisions to grant an Authority to Operate for a cloud solution for their Agency.*

This repository is key to the “do once, use many times” approach.

Per OMB policy memo, all assessment packages must use the FedRAMP security requirements – which includes the FedRAMP baseline set of controls as well as all FedRAMP templates

Category	FedRAMP 3PAO	ATO Status
CSP Supplied	✓	n/a
Agency ATO**	✗	Agency
Agency ATO with FedRAMP 3PAO	✓	Agency
JAB Provisional ATO	✓	JAB (+Agency)

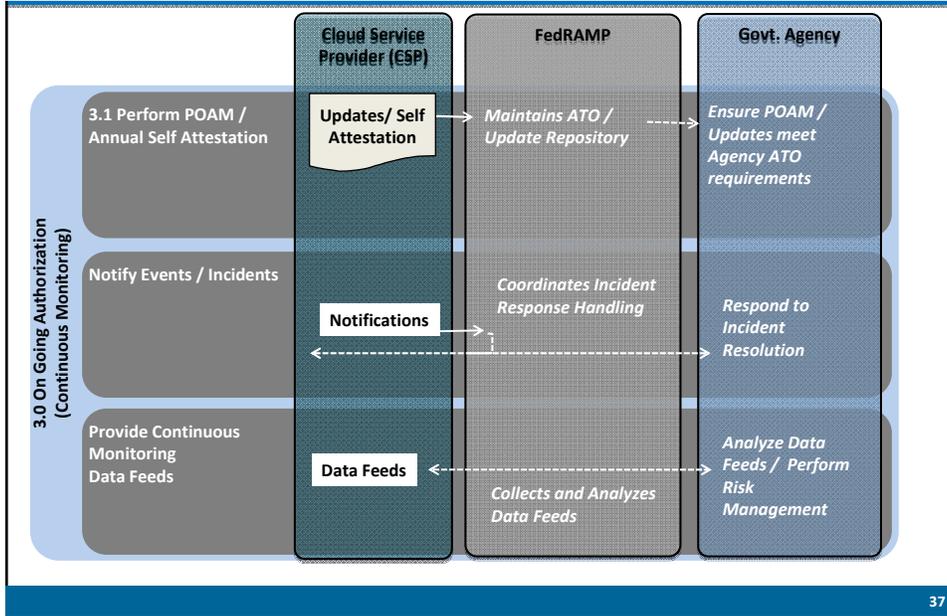
↑  
Level of Gov't Review

\*\* A&A packages without a FedRAMP 3PAO do not meet the independence requirements created by the JAB and will not be reviewed by FedRAMP but can still be leveraged

36



## Ongoing Assessment and Authorization



## Federal Risk and Authorization Management Program (FedRAMP)

Question and Answer Session

January 20, 2012





## What's Next

Activity	Date
FedRAMP CONOPS Release	February 5, 2012
Release of Initial List of 3PAOs	March – April 2012
Launch FedRAMP Initial Operating Capabilities	June 2012
Initial CSP Authorizations	Q4 2012, Q1 2013

\*After initial batch, applications for 3PAOs processed on an ongoing basis.

39

GSA



*For more information, please contact us or visit us at any of the following websites:*

<http://FedRAMP.gov>

<http://gsa.gov/FedRAMP>

Follow us on [twitter](#) @ FederalCloud