Federal Risk and Authorization Management Program (FedRAMP)

NIST

June 5, 2013

Matt Goodrich, JD

FedRAMP, Program Manager | Federal Cloud Computing Initiative| OCSIT | GSA

GSA®

FedRAMP℠

What is FedRAMP?

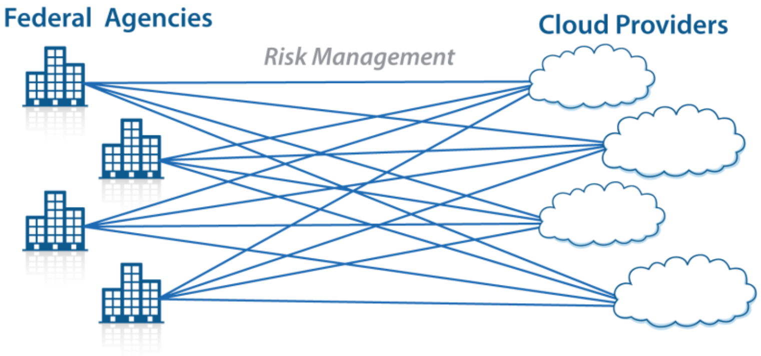
FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

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

Why FedRAMP?

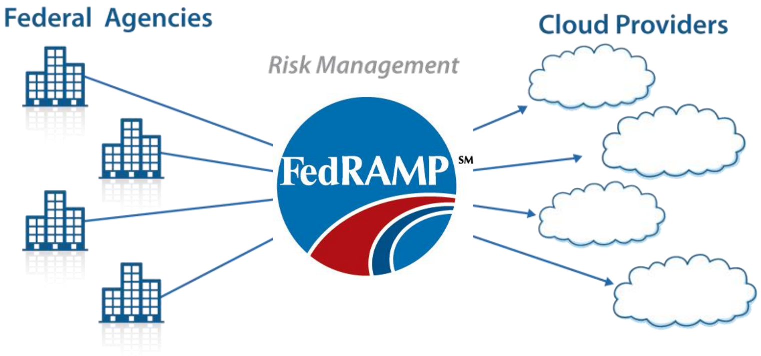
Problem:

- A duplicative, inconsistent, time consuming, costly, and inefficient cloud security risk management approach with little incentive to leverage existing Authorizations to Operate (ATOs) among agencies.



Solution: FedRAMP

- Uniform risk management approach
- Standard set of approved, minimum security controls (FISMA Low and Moderate Impact)
- Consistent assessment process
- Provisional ATO

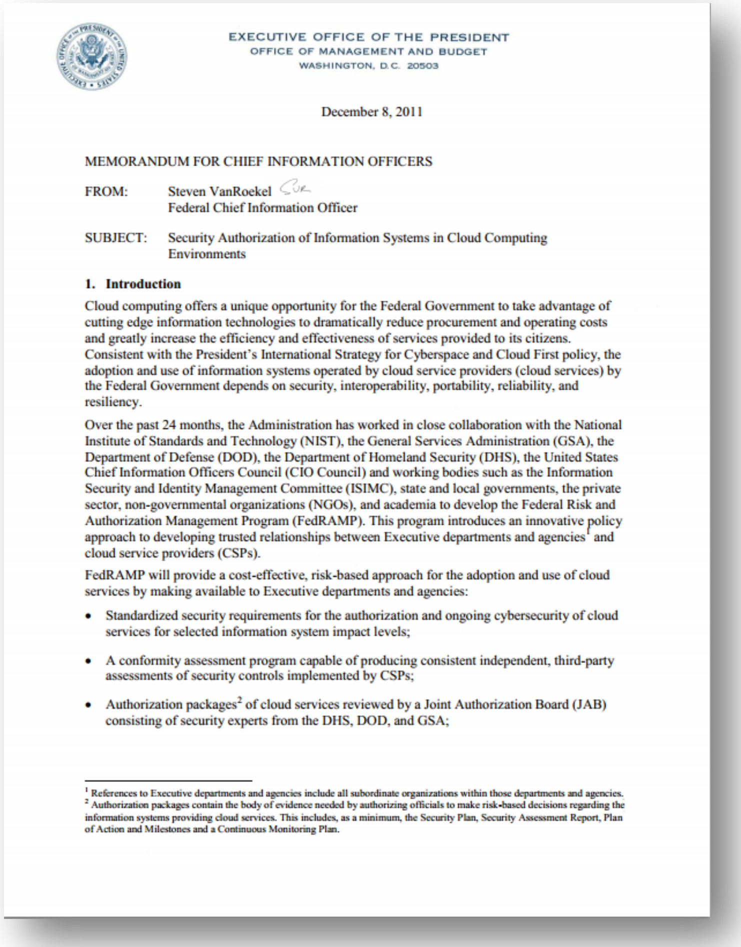


FedRAMP Policy Memo

OMB Policy Memo

December 8, 2011

- Mandates FedRAMP compliance for all cloud services used by the Federal government
  - All new services acquired after June 2012
  - All existing services by June 2014
- Establishes Joint Authorization Board
  - CIOs from DOD, DHS, GSA
  - Creates the FedRAMP requirements
- Establishes PMO
  - Maintained at GSA
  - Establishes FedRAMP processes for agency compliance
  - Maintains 3PAO program



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

December 8, 2011

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Steven VanRoekel
Federal Chief Information Officer

SUBJECT: Security Authorization of Information Systems in Cloud Computing Environments

1. Introduction

Cloud computing offers a unique opportunity for the Federal Government to take advantage of cutting edge information technologies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its citizens. Consistent with the President's International Strategy for Cyberspace and Cloud First policy, the adoption and use of information systems operated by cloud service providers (cloud services) by the Federal Government depends on security, interoperability, portability, reliability, and resiliency.

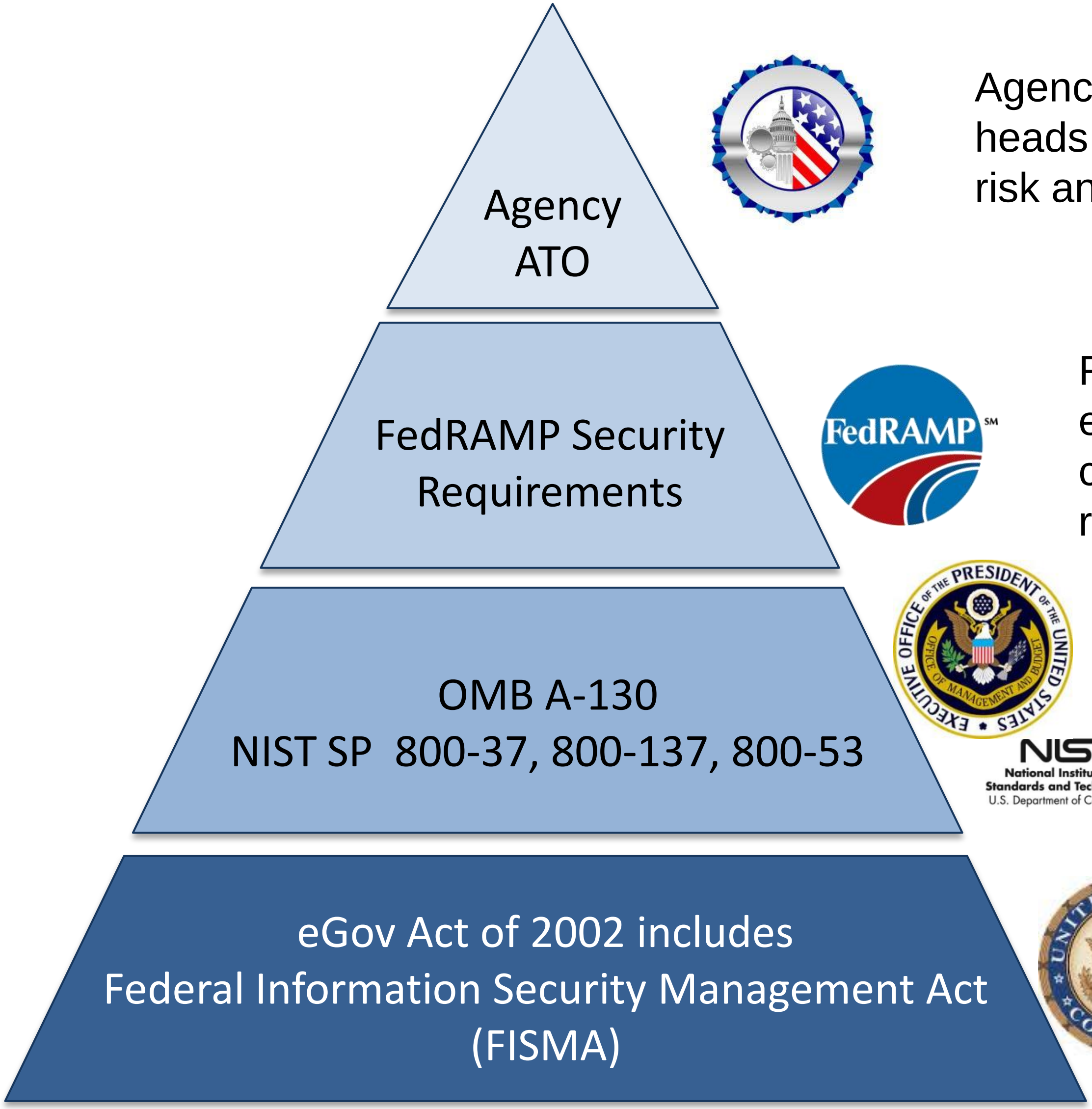
Over the past 24 months, the Administration has worked in close collaboration with the National Institute of Standards and Technology (NIST), the General Services Administration (GSA), the Department of Defense (DOD), the Department of Homeland Security (DHS), the United States Chief Information Officers Council (CIO Council) and working bodies such as the Information Security and Identity Management Committee (ISIMC), state and local governments, the private sector, non-governmental organizations (NGOs), and academia to develop the Federal Risk and Authorization Management Program (FedRAMP). This program introduces an innovative policy approach to developing trusted relationships between Executive departments and agencies[1] and cloud service providers (CSPs).

FedRAMP will provide a cost-effective, risk-based approach for the adoption and use of cloud services by making available to Executive departments and agencies:

- Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels;
- A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by CSPs;
- Authorization packages[2] of cloud services reviewed by a Joint Authorization Board (JAB) consisting of security experts from the DHS, DOD, and GSA;

[1] References to Executive departments and agencies include all subordinate organizations within those departments and agencies.
[2] Authorization packages contain the body of evidence needed by authorizing officials to make risk-based decisions regarding the information systems providing cloud services. This includes, as a minimum, the Security Plan, Security Assessment Report, Plan of Action and Milestones and a Continuous Monitoring Plan.

FedRAMP Policy Framework



Agency ATO

FedRAMP Security Requirements

OMB A-130
NIST SP 800-37, 800-137, 800-53

eGov Act of 2002 includes
Federal Information Security Management Act (FISMA)

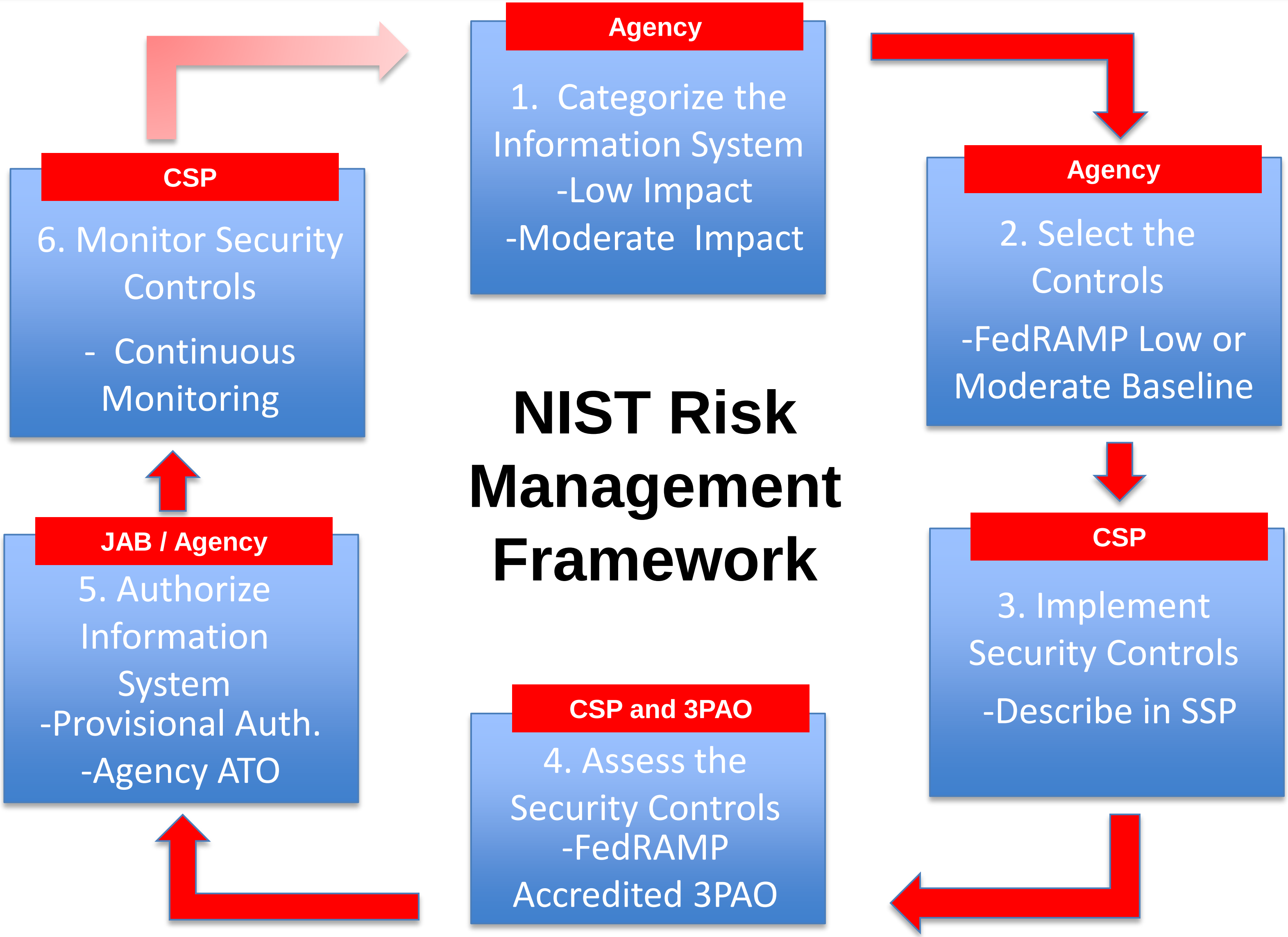
Agencies leverage FedRAMP process, heads of agencies understand, accept risk and grant ATOs

FedRAMP builds upon NIST SPs establishing common cloud computing baseline supporting risk based decisions

OMB A-130 provide policy, NIST Special Publications provide risk management framework

Congress passes FISMA as part of 2002 eGov Act

FedRAMP and NIST RMF 800-37



NIST Risk Management Framework

Agency

1. Categorize the Information System
-Low Impact
-Moderate Impact

Agency

2. Select the Controls
-FedRAMP Low or Moderate Baseline

CSP

3. Implement Security Controls
-Describe in SSP

CSP and 3PAO

4. Assess the Security Controls
-FedRAMP Accredited 3PAO

JAB / Agency

5. Authorize Information System
-Provisional Auth.
-Agency ATO

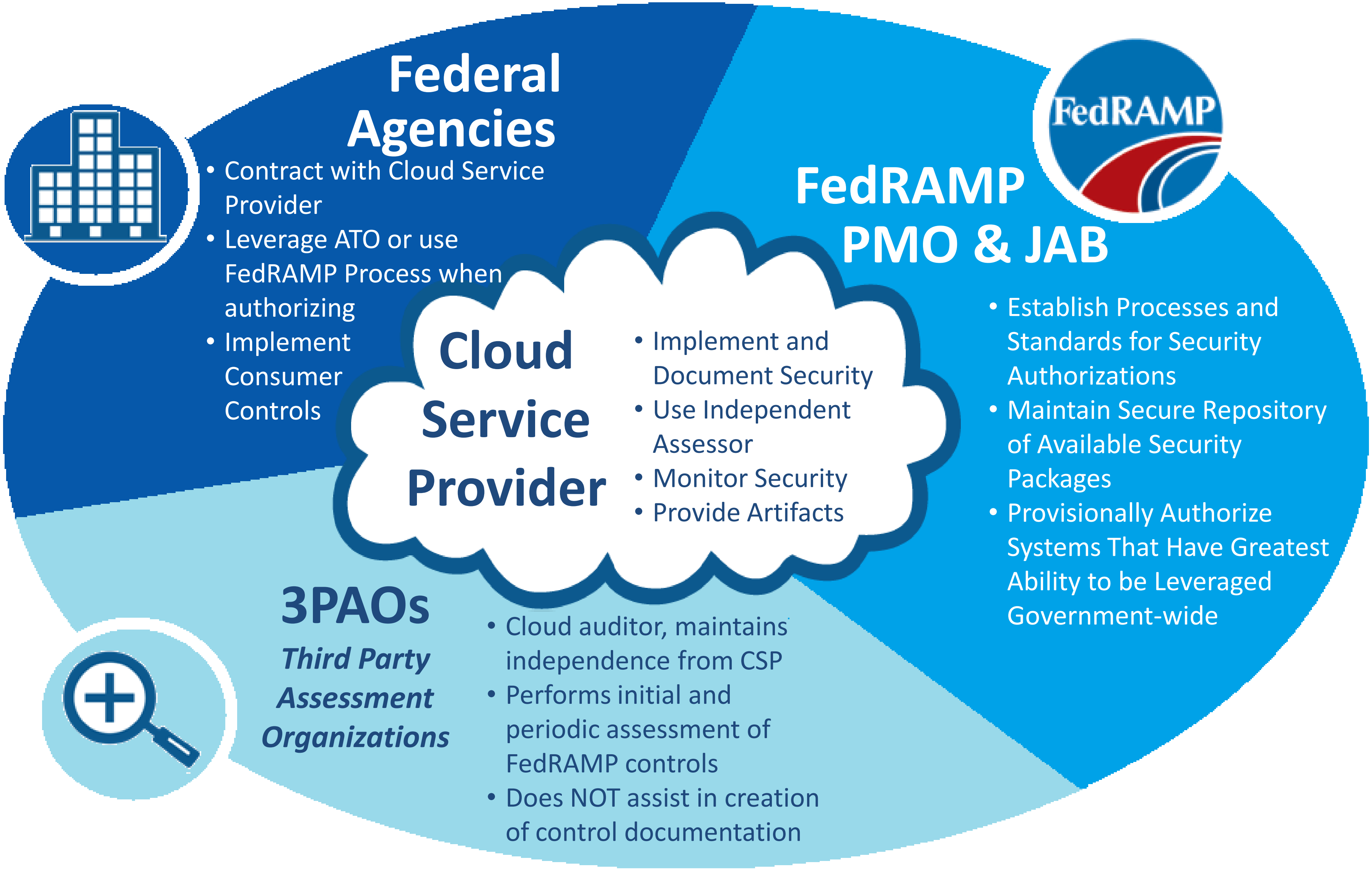
CSP

6. Monitor Security Controls
- Continuous Monitoring

FedRAMP Standardizes RMF for Cloud

NIST SP 800-37 Step	FedRAMP Standard
1. Categorize System	Low and Moderate Impact Levels
2. Select Controls	Control Baselines for Low and Moderate Impact Levels
3. Implement Security Controls	Document control implementations using the FedRAMP templates Implementation Guidance in “Guide to Understanding FedRAMP”
4. Assess the Security Controls	FedRAMP accredits 3PAOs 3PAOs use standard process, templates
5. Authorize the System	Joint Authorization Board or Agency AO authorize the system that can be leveraged due to increased trust
6. Continuous Monitoring	CSPs conduct monitoring in accordance with Continuous Monitoring Strategy and Guide

FedRAMP Key Stakeholders & Responsibilities



Federal Agencies

- Contract with Cloud Service Provider
- Leverage ATO or use FedRAMP Process when authorizing
- Implement Consumer Controls

FedRAMP PMO & JAB

- Establish Processes and Standards for Security Authorizations
- Maintain Secure Repository of Available Security Packages
- Provisionally Authorize Systems That Have Greatest Ability to be Leveraged Government-wide

Cloud Service Provider

- Implement and Document Security
- Use Independent Assessor
- Monitor Security
- Provide Artifacts

3PAOs

Third Party Assessment Organizations

- Cloud auditor, maintains independence from CSP
- Performs initial and periodic assessment of FedRAMP controls
- Does NOT assist in creation of control documentation

Mythbusting FedRAMP

Lots of Confusion Still about FedRAMP, need to address top areas of concern:

- Who defines cloud?
- Control responsibility between vendors and stacking of authorizations
- Perception of delays in authorizations
- Ability of vendor to meet Federal requirements
- Difference between Agency ATO's and JAB Provisional ATOs
- 3PAO Privatization efforts – impact on the program

What is the Definition of Cloud?

Cloud First Policy

- Agencies must default to cloud based products and services when spending any new money on IT
  - New services, recompetes, additional services
- Agencies must justify to OMB when a cloud provider is NOT selected

When a cloud service provider is selected, FedRAMP governs the security authorization process.

Cloud Definition

- FedRAMP is not arbiter of what is and what is not cloud.
- We will authorize anything that is “cloud” esque
- If any agency submits a FedRAMP package for a system they deem cloud, FedRAMP will review that system as cloud – we will not interfere with or negate an agency determination of cloud.

Vendor Abilities to Meet Federal Requirements

Many cloud vendors are new to FISMA and it takes time to meeting Federal Requirements

- Clearly Defined Boundaries
- FIPS 140-2 Encryption
- Authenticated Scans
- Remediation of Vulnerabilities
- Multi-Factor Authentication

Delays in Authorizations

FedRAMP is a rigorous process, with increased scrutiny on meeting security requirements

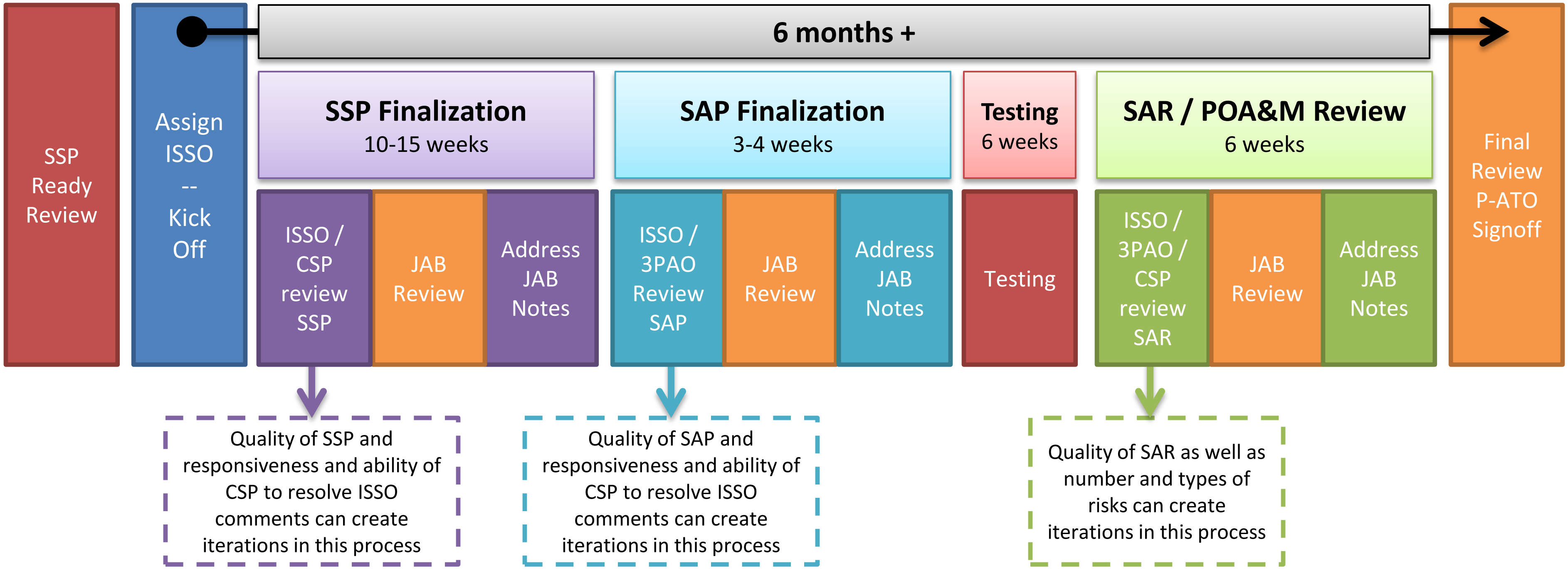
- Currently 2 JAB provisional ATO's: CGI Federal, Autonomic Resources
- Currently 2 Agency ATOs: Amazon's US East/West, and Amazon's GovCloud

- FISMA process takes time
- Difference between efficient and expedient
- Transparency
- New process for many vendors
- Updated CONOPs and standardization of timelines

- AGENCY ATO'S AND JAB PROVISIONAL ATO'S

FedRAMP Provisional Authorization

Timeframe Overview



SSP Ready Review

Assign ISSO -- Kick Off

6 months +

SSP Finalization 10-15 weeks

ISSO / CSP review SSP

JAB Review

Address JAB Notes

SAP Finalization 3-4 weeks

ISSO / 3PAO Review SAP

JAB Review

Address JAB Notes

Testing 6 weeks

Testing

SAR / POA&M Review 6 weeks

ISSO / 3PAO / CSP review SAR

JAB Review

Address JAB Notes

Final Review P-ATO Signoff

Quality of SSP and responsiveness and ability of CSP to resolve ISSO comments can create iterations in this process

Quality of SAP and responsiveness and ability of CSP to resolve ISSO comments can create iterations in this process

Quality of SAR as well as number and types of risks can create iterations in this process

Key

🟥 CSP Action	🟪 FedRAMP / CSP Action	🟦 FedRAMP / 3PAO Action
🟦 FedRAMP Action	🟧 FedRAMP JAB Action	🟩 FedRAMP / 3PAO / CSP Action

JAB Provisional ATO vs Agency ATO

Timeframe

- JAB 25+ weeks minimum
- Agency 14+ weeks minimum

Level / Depth of Review

- JAB: Four sets of eyes (PMO, DoD, DHS, GSA)
- Agency: One set of eyes (agency)

Risk Acceptance Level

- JAB: Low risk tolerance level, security for security
- Agency: Varying levels of risk acceptance, business needs can justify more risk as can individual agency policies

Continuous Monitoring

- JAB: JAB will maintain, agencies need to review
- Agency: Agency must work with CSP to complete

Why should Agencies do Agency ATOs?

Mandatory to meet FedRAMP Requirements

- OMB Policy Memo - Reporting to OMB through PortfolioStat
- Not new process – current NIST / FISMA authorization process standardized

Timeframe

- If business needs exist to use a service now, agency doesn't have to wait on JAB
- Can complete an authorization faster than the JAB

Not ALL cloud providers will receive a JAB ATO

- JAB will only authorize those systems they see as being leveraged the most government-wide
- JAB will not authorize systems that do not meet certain capabilities and Federal requirements

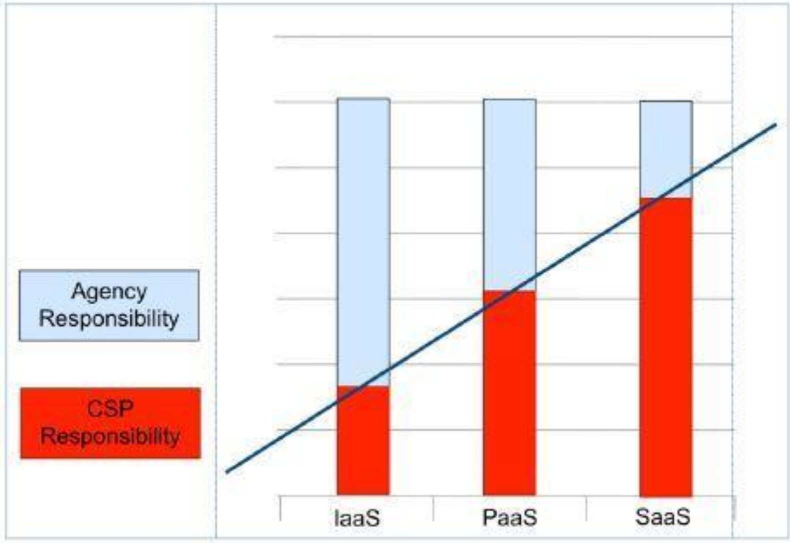
Acceptance risk level is flexible

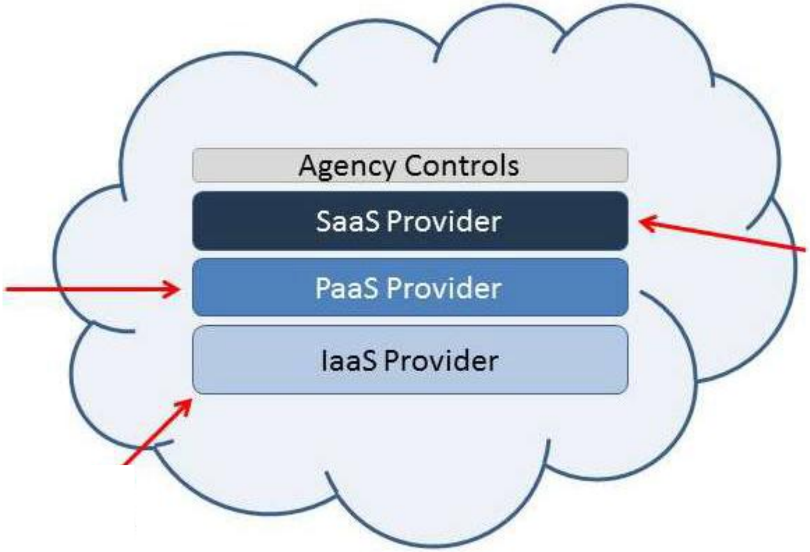
- HHS can vary acceptable risk levels based on many factors JAB doesn't consider (e.g. flexible baseline, types of data, business need, cost, ROI, etc.)

More Influence over CSP

- Contract with CSP allows agency to enforce capabilities
- FedRAMP does not have contracts with CSPs

Control Responsibility and Stacking Authorizations





Provider/Consumer responsibilities and how they interact

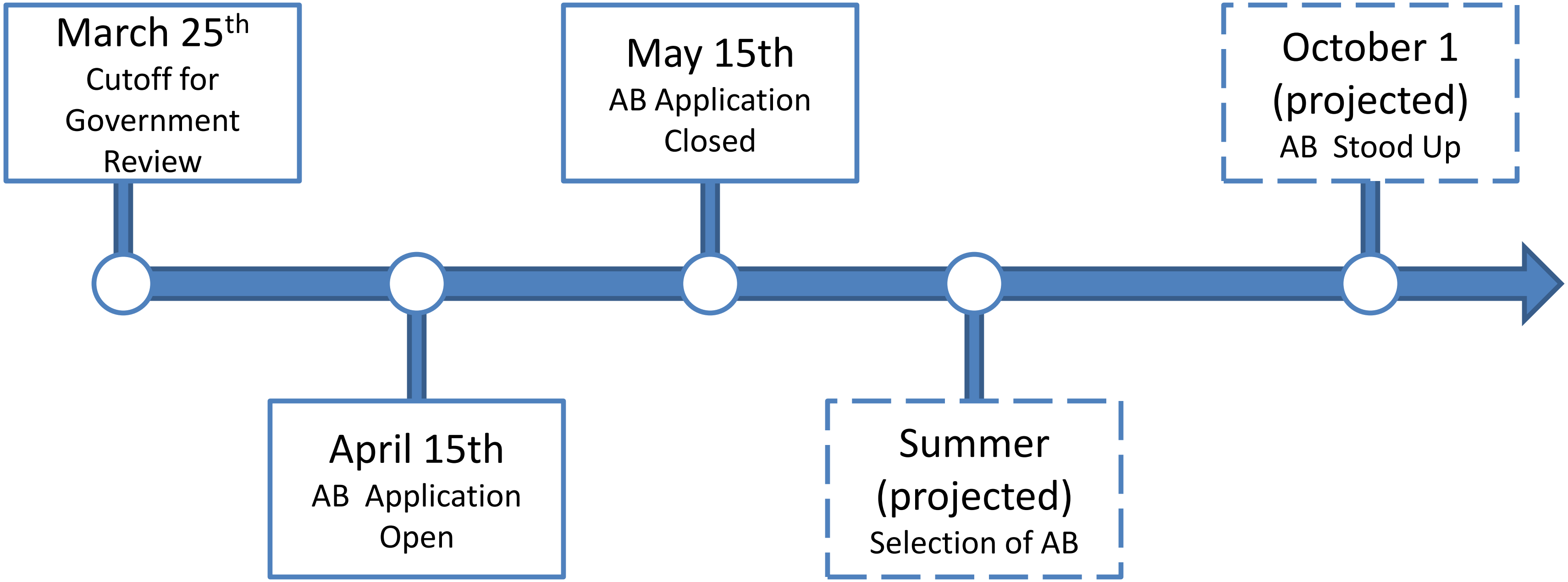
- There is no distinct line of where I/P/S offerings begin and end. The differences between vendors is part of what defines offerings as well as gives vendors advantages over competitors.
- However, I/P/S offerings create unique boundaries that “sit on top” of each other, and the consumer/agency responsibility is above all of these.
- Authorizations can be stacked on top of each other to create a singular authorization for a type of service.

3PAO Privatization

3PAO Privatization is designed to keep rigor of 3PAO program and free government resources

- Same process that was done for Health IT, NAVLAP, UL, etc.
- FedRAMP will maintain ownership of accreditation list and is final source of accreditation decision
- Privatization is for accreditation reviews of applicants ONLY
- Privatization will also allow for increased surveillance post accreditation

Privatization Timeframe



Tentative Timeline for 3PAO Privatization

- Currently reviewing AB applications
- We are evaluating all possibilities and approaches for transition of currently accredited 3PAOs to privatized accreditation review
- CSPs and Federal agencies will not be impacted due to privatization efforts – SARs will be accepted from anyone who is on the accredited list

For more information, please contact us or visit us the following website:

www.FedRAMP.gov
Email: info@fedramp.gov

Follow us on twitter @ FederalCloud