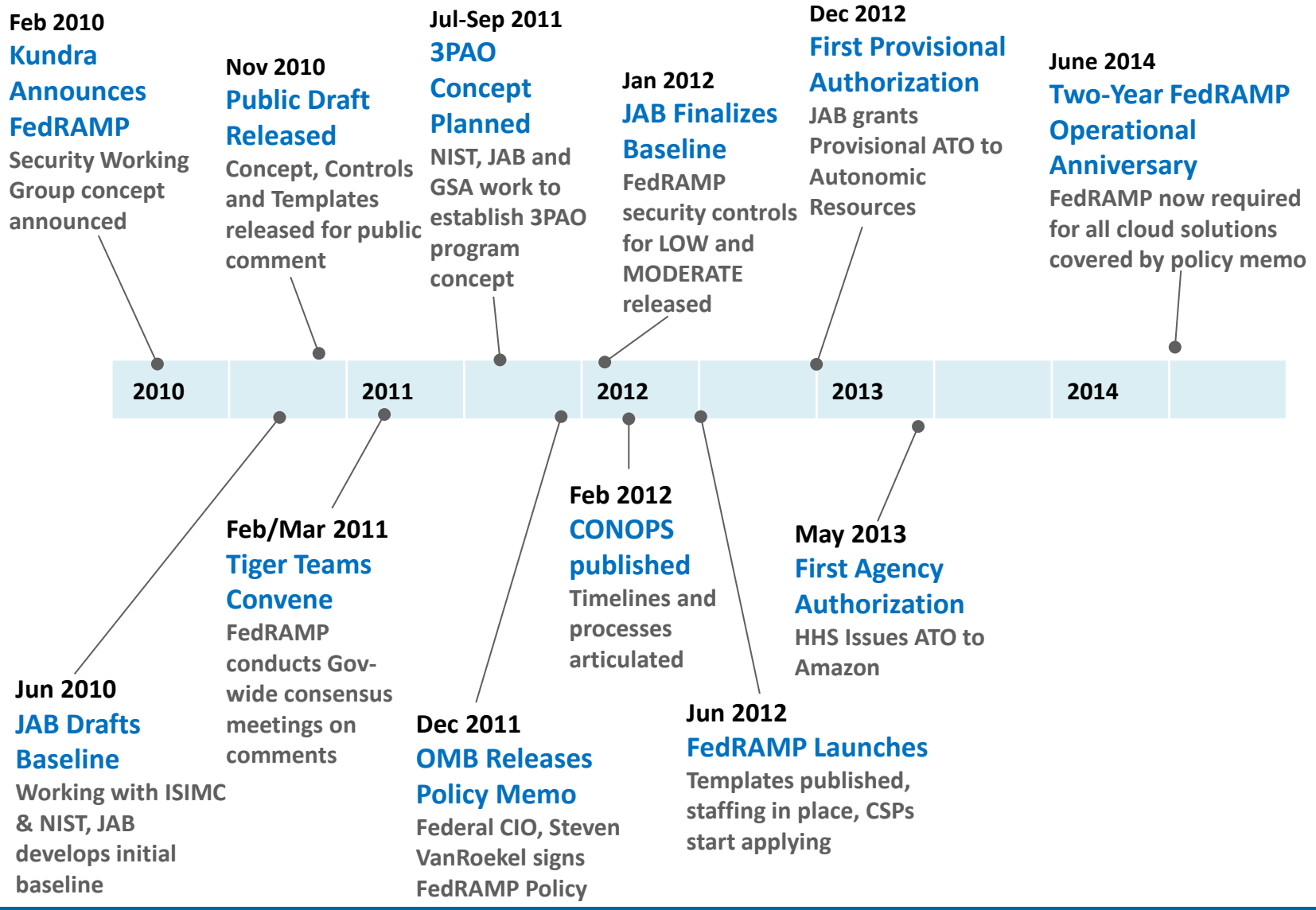
FedRAMP
Federal Risk and Authorization Management Program

Federal Computer Security Program Managers' Forum

Claudio Belloli
FedRAMP Information Systems Security Manager
GSA

August 19, 2014

FedRAMP: A brief history



FedRAMP is in Full Operations

- Repeatable processes for continuous monitoring activities
- Agency outreach
- Additional access controls in the secure repository
- Agency ATO's accessible and leveraged by other agencies
- Guide to FedRAMP updated to reflect lessons learned in IOC
- Manual dashboards in use for internal, JAB and other stakeholder reporting
- Privatization of 3PAO Accreditation
  - A2LA selected as the accreditation body

FedRAMP Key Stakeholders & Responsibilities

Federal Agencies

- Contract with Cloud Service Provider
- Leverage ATO or use FedRAMP process when authorizing
- Implement consumer controls

Cloud Service Provider

- Implement and document security
- Use Independent Assessor
- Monitor security
- Provide artifacts

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

3PAOs

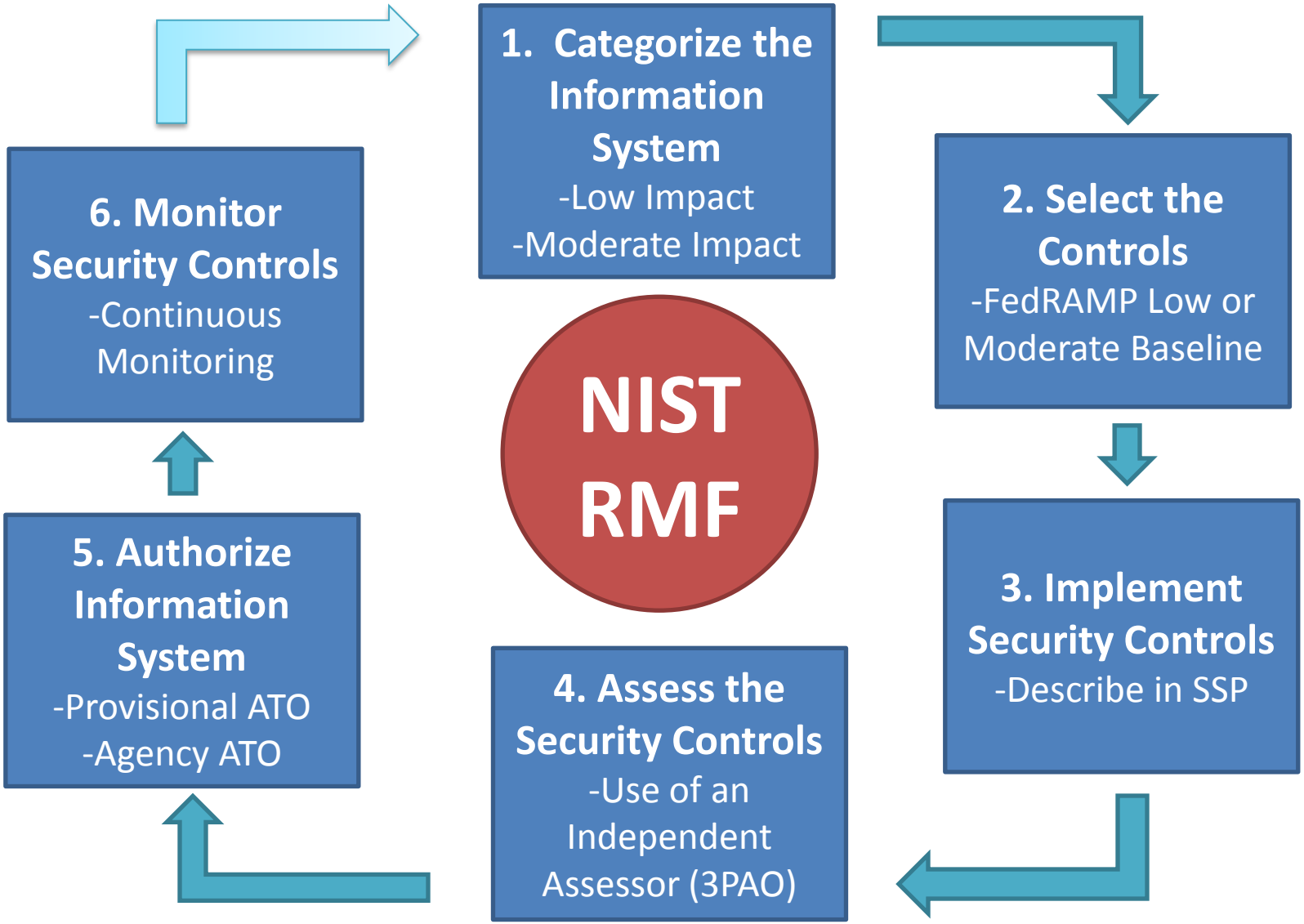
Third Party Assessment Organizations

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

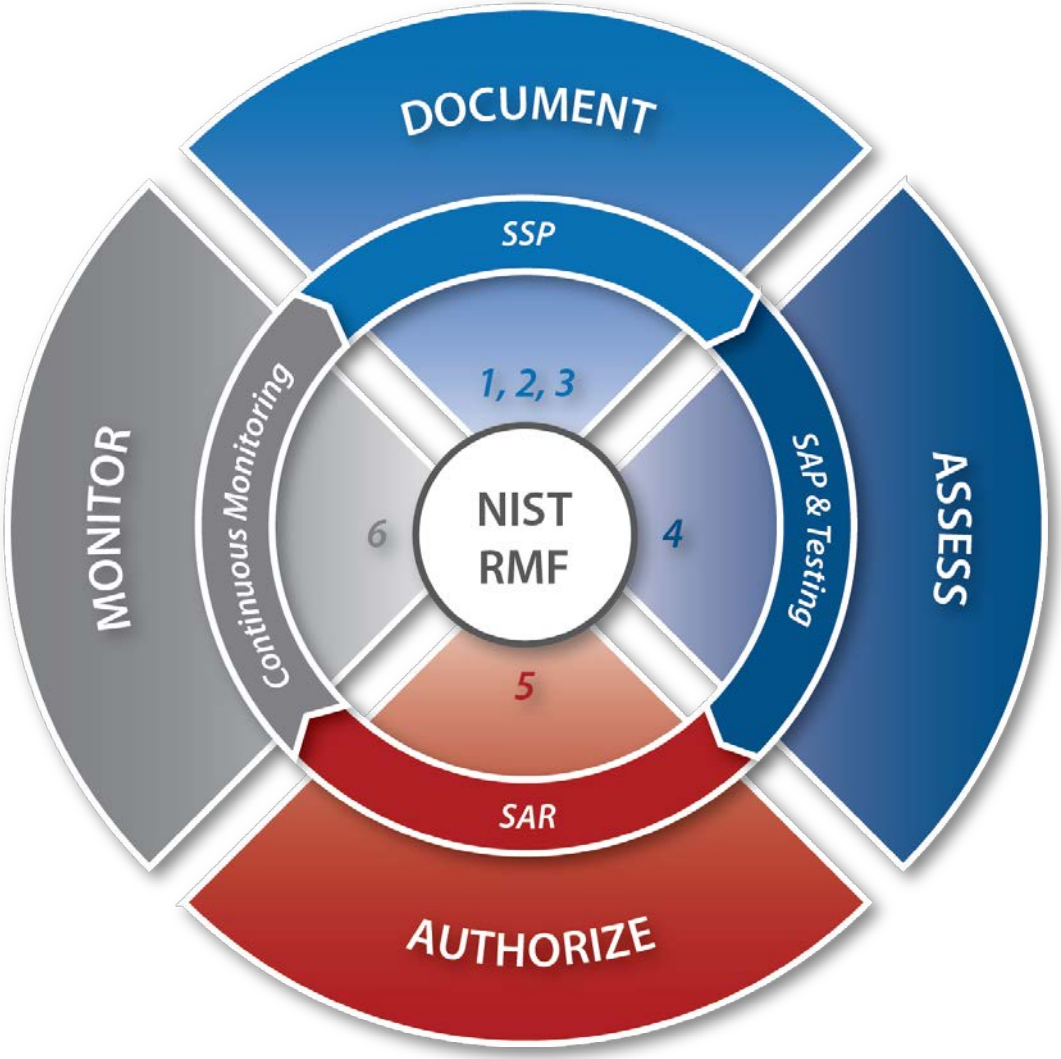
Agency Responsibilities

- As of June 5, 2014, all cloud projects must meet the FedRAMP requirements when initiating, reviewing, granting, and revoking security authorizations
  - Use of FedRAMP security controls baseline
  - Use of mandatory templates
  - Provide FedRAMP PMO with ATO letters
  - Use FedRAMP repository for all ATOs where re-use is possible
- Agencies must enforce FedRAMP via contractual provisions
  - Template contract language available on FedRAMP.gov
  - Includes generic security section as well as control specific contract clauses
- Agencies must report to OMB via PortfolioStat cloud services that cannot meet FedRAMP requirements

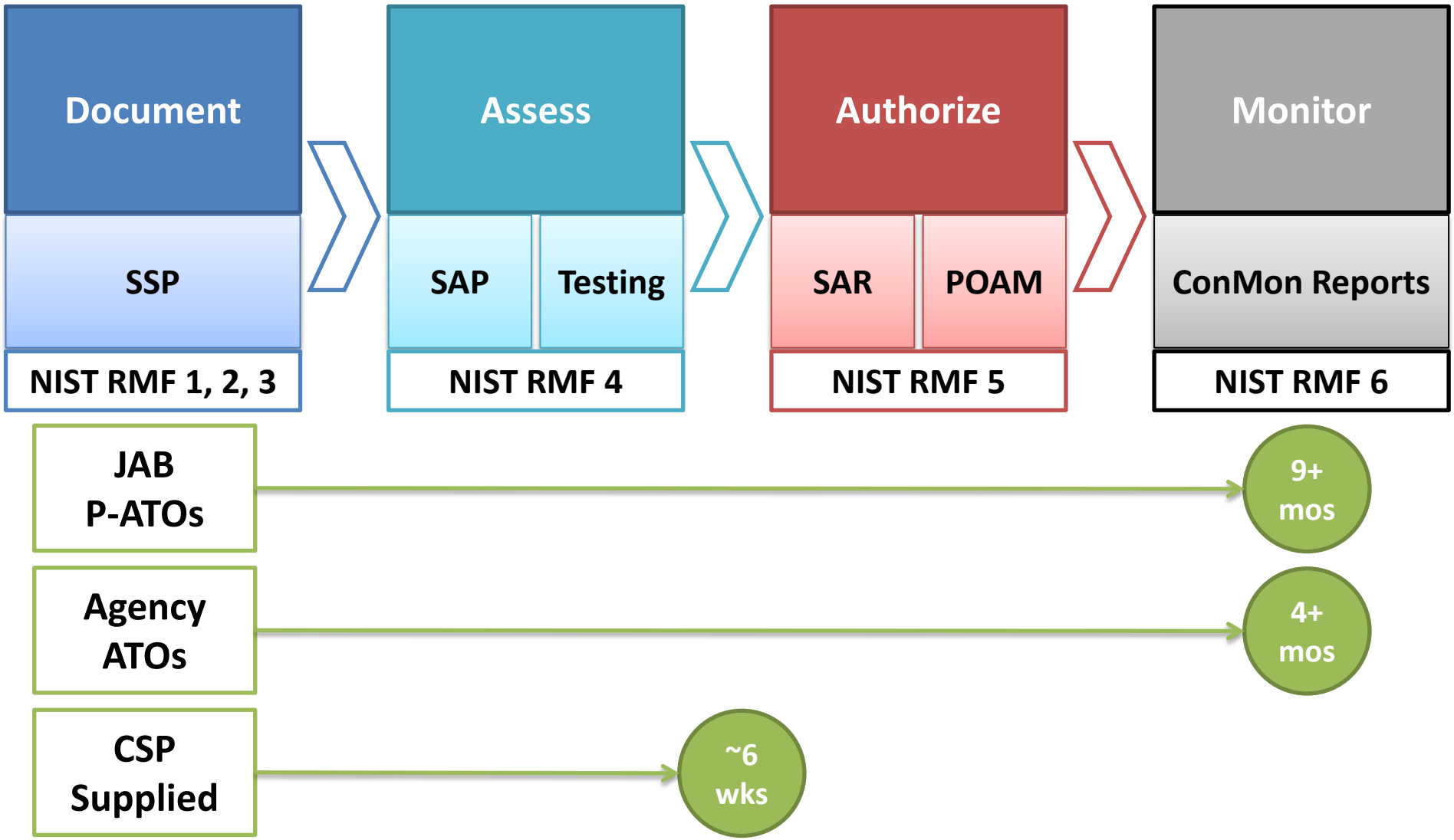
FedRAMP Relationship to the NIST Risk Management Framework



FedRAMP Security Assessment Framework (SAF) and NIST Risk Management Framework



Timeline for the SAF



SAF Process Area: Document

Document

System Security Plan

Categorize the Information System	Select the Security Controls	Implement the Security Controls
▪ NIST RMF Step 1 ▪ Determine impact level by using the FIPS 199 Form ▪ FedRAMP only supports Low and Moderate impact levels	▪ NIST RMF Step 2 ▪ Use the FedRAMP low or moderate baseline security controls ▪ 125 controls for low ▪ 325 for moderate	▪ NIST RMF Step 3 ▪ Use FedRAMP templates ▪ Templates include considerations specific to cloud implementations ▪ Implementation guidance in Guide to Understanding FedRAMP

SAF Process Area: Assess

Assess

Security Assessment Plan

Testing

Assess the Security Controls

- NIST RMF Step 4
- Independent Assessors must be used
- FedRAMP accredits independent assessors through the 3PAO accreditation program
- Highly encourage all agencies to use accredited 3PAOs for FedRAMP assessments
- Use FedRAMP SAP template
- FedRAMP tailored test cases
- Create unique test cases for any CSP alternative implementations

SAF Process Area: Authorize

Authorize

Security Assessment Report	Plan of Action and Milestones (POA&M)

Authorize the Information System

- NIST RMF Step 5
- Independent Assessors provide a SAR detailing risks of the system
- CSP must create POA&M which determines timeline for remediation and/or mitigations of each risk identified in the SAR
- Authorizing official makes a risk based decision for authorization of CSP
- If CSP has risk posture that is acceptable, agencies will still have certain responsibilities for the authorization (e.g. multi-factor authentication, access control, TIC, etc.)
- Two types of authorizations: JAB Provisional ATOs and Agency ATOs
- CSP supplied packages will NOT have an authorization, but WILL have a SAR and POA&M

SAF Process Area: Monitor

Monitor

Continuous Monitoring

Monitor Security Controls

- NIST RMF Step 6
- Risk Management Framework with cloud gets away from a “point in time” approach to security authorizations
- 3 key steps: Operational Visibility, Change Control, and Incident Response
- FedRAMP Continuous Monitoring Strategy and Guide defines the process for CSPs to meet continuous monitoring requirements through periodic reporting, making plans for changes to the system, and how to respond appropriately to incidents that may occur within a CSP system once authorized

Overview: FedRAMP SAF Standardizes RMF for Cloud

FedRAMP SAF Process	NIST SP 800-37 Step	FedRAMP Standard
Document	1. Categorize System	Low and Moderate Impact Levels
	2. Select Controls	Control Baselines for Low and Moderate Impact Levels
	3. Implement Security Controls	Use FedRAMP templates Implementation Guidance in "Guide to Understanding FedRAMP"
Assess	4. Assess the Security Controls	FedRAMP accredits 3PAOs 3PAOs use standard process and templates
Authorize	5. Authorize the System	ATOs with JAB P-ATO or Agency ATO CSP Supplied packages
Monitor	6. Continuous Monitoring	Use Continuous Monitoring Strategy and Guide

FedRAMP Authorization Paths

JAB Provisional Authorization (P-ATO)

- Prioritizes authorizing cloud services that will be widely used across government
- CIOs of DoD, DHS and GSA must agree that the CSP:
  - Strictly meets all the controls
  - Presents an acceptable risk posture for use across the federal government
- Conveys a baseline level of likely acceptability for government-wide use
- CSPs must use an accredited Third Party Assessor Organization (3PAO)
- FedRAMP PMO manages continuous monitoring activities; agencies review results

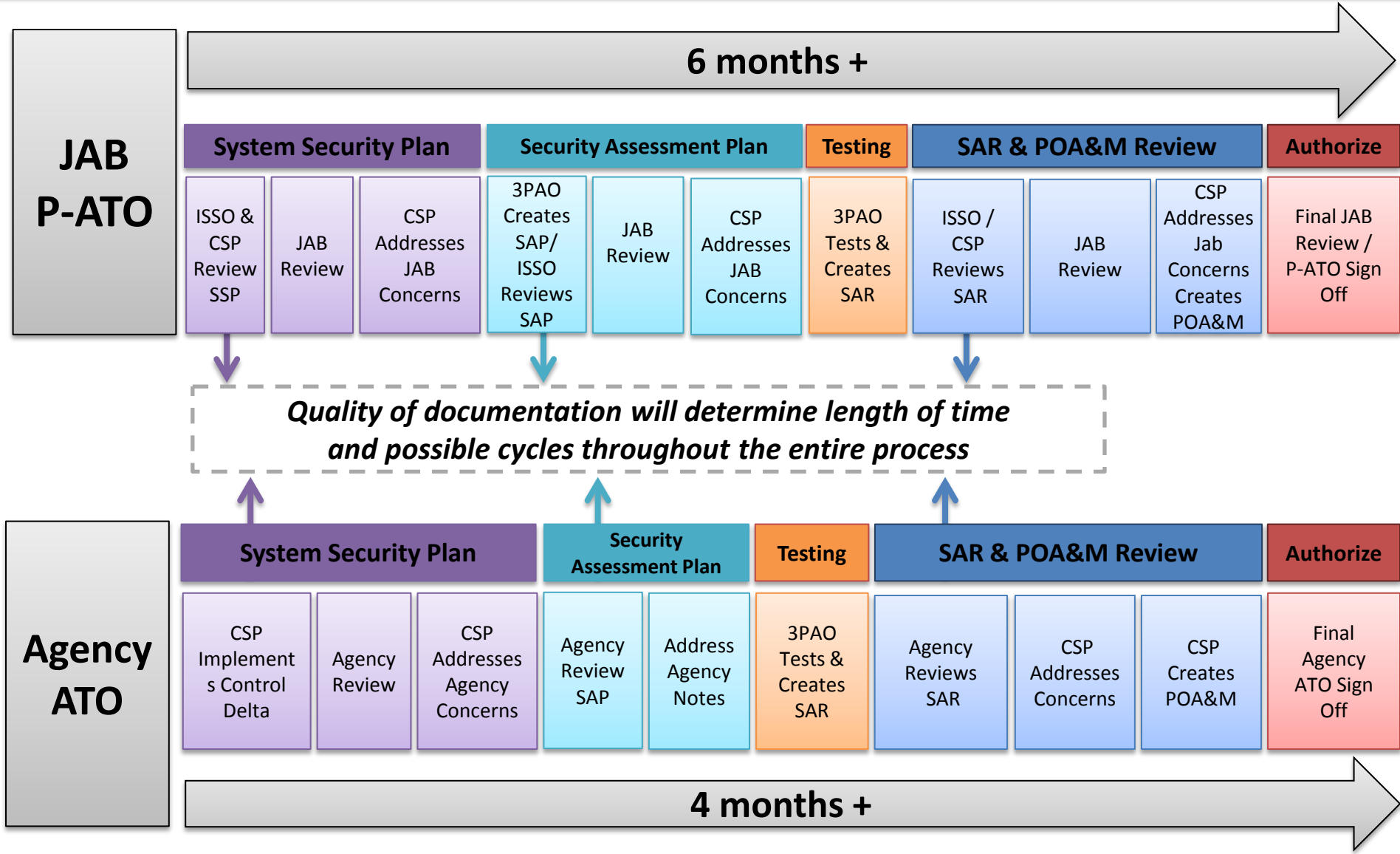
Agency ATO

- Issued by the agency only
- Agencies have varying levels of risk acceptance
- Agency monitors the CSPs continuous monitoring activities
- Option to use a 3PAO or independent assessor to perform independent testing

CSP Supplied

- Submitted directly by CSP to FedRAMP
- CSP without ATO
- CSP must use an accredited 3PAO

Authorization Process – JAB and Agencies



Authorization Progress to Date

JAB Provisional Authorizations

- 12 cloud services approved
- FedRAMP authorizations cover 250+ government contracts
- Agencies expected to update ATO memos for these services

Agency issued ATOs

- 5 cloud services authorized by agencies

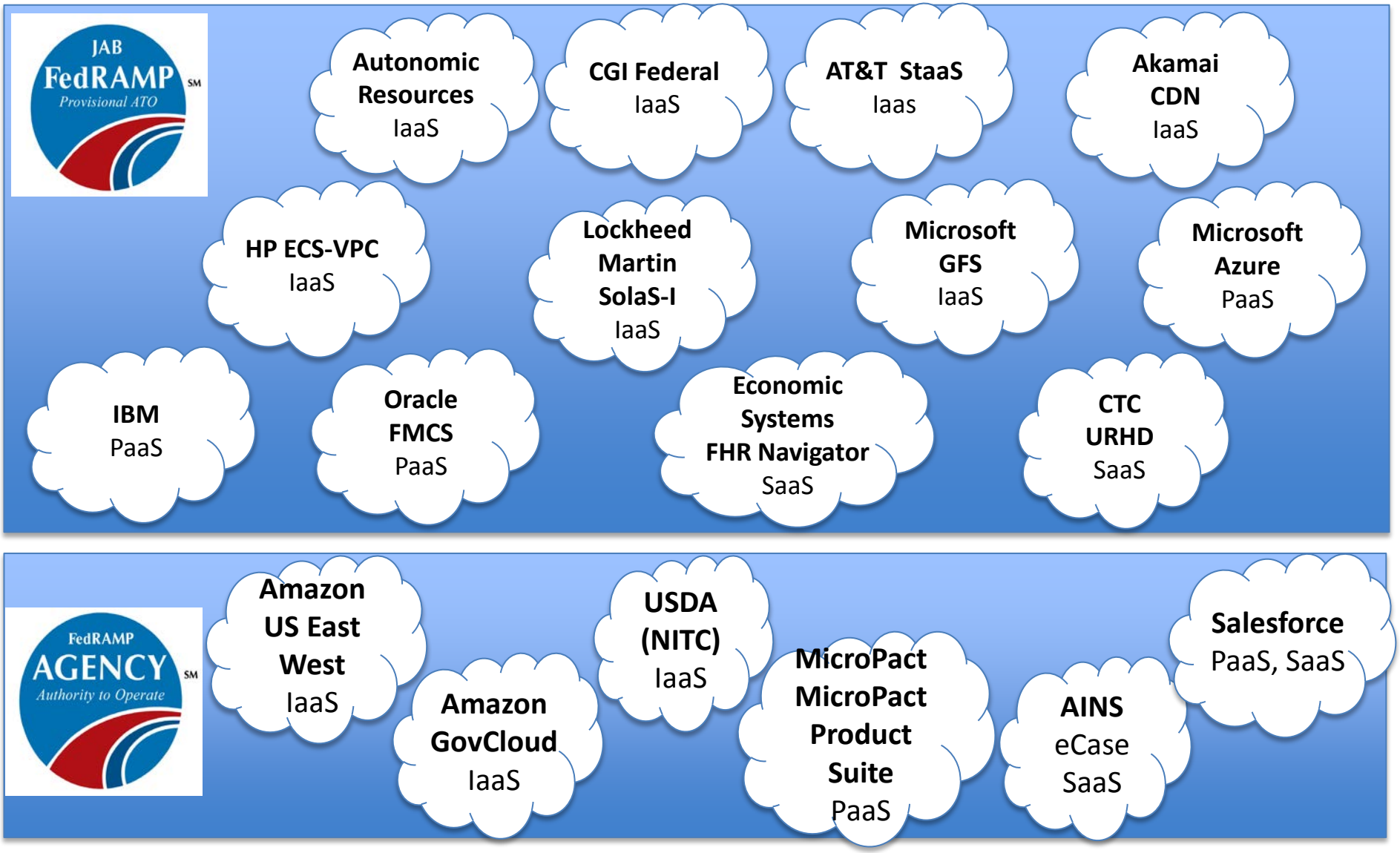
FedRAMP Pipeline

- 25 cloud services in process for JAB Provisional or Agency Authorization
- 8 cloud services awaiting kick-off

FedRAMP Cost Savings

- $40 million in cost savings based on known FISMA reporting

Available P-ATOs and Agency ATOs



June Deadline and PortfolioStat

June 2014

- All CSPs used by Federal agencies need to meet FedRAMP requirements
  - Baseline security controls, independent assessment, use templates, make documentation available in the repository for leveraging
- Agencies must enforce FedRAMP with cloud providers via contracts

PortfolioStat Reporting

- New questions regarding FedRAMP
- Agencies must rationalize lack of FedRAMP compliance
- Agencies must identify plans to meet FedRAMP requirements

PortfolioStat Analysis

- PMO reviews PortfolioStat reporting by agencies
- Compare with other data points
- Provide OMB with analysis for Agency PortfolioStat session

FedRAMP Security Controls Baseline Update

Security Controls Baseline Update

- Extensive public comment period
- PMO and JAB reviews

FedRAMP Baseline

Category of Changes	# Controls
Revision 3 Baseline	298
Withdrawn by NIST from Previous FedRAMP Baseline	*(41)*
Removed by Analysis FedRAMP Baseline	*(8)*
Not Selected in Rev. 4	*(4)*
Carryover Controls	245
Added by NIST	39
Added by analysis	41
Revision 4 Baseline	**325**

NIST SP 800-53 Rev 4 Update Overview

- Rev. 4 Documentation Update Effort
  - 15 total documents to be released
  - Updates affected 13 core FedRAMP templates and documents
  - Creation of 2 additional documents
  - Approximately 1250 pages of edits
  - 3000+ hours of work to complete

- Major Overhauls and New Documentation
  - CONOPS updated to FedRAMP Security Assessment Framework
  - Guide to Understanding FedRAMP including new lessons learned
  - Creation of test cases for 80 new controls due to NIST not updating test cases for 800-53 Revision 4

NIST SP 800-53 Rev 4 Templates

- All FedRAMP Rev-4 documents and template updates released on June 6, 2014
- PMO will follow NIST style of public comment period on documentation
- PMO will have periodic updates to documentation available for public comment periods with advance notice published on www.fedramp.gov

PMO is always open to suggestions for new formats, problems with documents, or other feedback on templates

NIST SP 800-53 Rev 4 Transition Plan

Transition Plan

- CSPs divided in to 3 categories

	Initiation	In Process	Continuous Monitoring
Transition Timeframes	Must use new requirements for authorization	Must update at first annual assessment	Must update at annual assessment – at least 6 months to plan

Detailed Transition Plan for CSPs

- Overview of controls selected for annual assessment
  - New controls (80)
  - Core controls (~40)
  - Controls selection based on risk management approach

Overall level of effort:

- Normal annual assessment 100-120 controls
- Rev 4 transition ~150 controls

NIST SP 800-53 Rev 4 Transition Plan (continued)

- CSPs in the in-process and continuous monitoring stages have to update to new baseline during annual assessment
  - Providers must implement new controls
- Documentation (SSP and supporting documents) must be updated using the new templates to indicate implementation of Rev 4 controls
  - Testing will be around 140/150 controls
    - Annual core controls
    - New Controls
    - Delta of Controls needed to be assessed due to changes to system

Lessons Learned

Authorization

- Tailoring of test cases is critical for unique architectural design
- Information security is a business issue
  - Technology is easy; business processes and procedures, guidelines and practices are what makes security work
- A risk is not mitigated because “it’s believed” a service is only available internally

Continuous Monitoring

- Same tools used for testing and on-going continuous monitoring
- Locking down the system critical to successful testing
- Planning significant change in advance
- Alignment of scanning, patching and testing schedules

Lessons Learned

CSP readiness tied to a number of factors

- Size of CSP infrastructure, alternate implementations, vulnerabilities or risks identified, type of service offering(s)
- Alignment of corporate business strategy to sell cloud services to the government
- Processes and procedures
- Able to address controls in preparation check list
  - Section 5.1 of the Guide to Understanding FedRAMP

Future: Increased Agency ATOs, Working Groups

Agency ATOs

- CSPs and agencies need to work together to initiate and grant authorizations
- CSPs need to analyze customer base
- Agency path best suited for majority of CSPs

Working Groups

- PortfolioStat reporting identified FedRAMP POCs
- Assist in cross-agency authorizations
- Increase guidance and address common issues
- Give platform for CSPs to reach out to agencies

Impact of FedRAMP

Enables Cloud Security

- Successfully proven the U.S. government can securely use all types of cloud computing
- Created a standards based approach to security through risk management
- Implements continuous diagnostics and mitigation (CDM) for cloud
  - On-going visibility into CSP risk posture
  - Trend analysis of vulnerabilities and incidents
- Establishing a new marketplace for cloud vendors

Accelerates USG adoption of Cloud Computing

- Enables agencies achieve cost savings and efficiency through cloud computing
- Accelerates time to market for cloud services when authorizations re-used
  - DOI leveraged 6 authorizations and conservatively estimates a cost savings of 50% per authorization
  - HHS estimates cost savings at over $1M for their authorization and leveraging of Amazon alone

Ahead of the Curve

- Commercial industry is looking to FedRAMP as a model for building standards based security for cloud services
- Other countries are also looking to FedRAMP for their security frameworks

Questions and Answers

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

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

Follow us on twitter @ FederalCloud