

# Federal Risk and Authorization Management Program (FedRAMP)

ISPAB Update  
October 22, 2014





# FedRAMP Current State

## FedRAMP to Date

- Operational for over 2 years
- Mandatory compliance date has passed (June 2014)
- ~40% of *agency* reported use of cloud through PortfolioStat is FedRAMP compliant cloud
  - PMO estimates actual number around 25%

## Agency use of FedRAMP

- 22 of 24 CFO Act Agencies actively reviewing FedRAMP security authorization packages
  - Over 500 active reviewers of FedRAMP security authorization packages
  - 50+ requests from other Federal entities (small and micro agencies, congress, courts)
- 30 ATO letters provided by Agencies

## Estimated Cost Savings

- 160 identified instances of agency cloud FISMA implementations using authorized CSPs
- \$250K average per authorization x 160 cloud implementations = \$40M savings
  - Based on 2012 FISMA metrics and agency provided estimates



# Cloud System Providers Progress



## Authorizations

- JAB P-ATOs - 12 cloud services
  - Includes services from IBM, Microsoft, Akamai, HP, Lockheed Martin
- Agency ATOs - 6 cloud services
  - Includes Amazon, AINs, USDA, Micropact, Salesforce

## In Process CSPs

- JAB P-ATO - 18 cloud services
  - Includes services from Dell, SecureKey, Oracle, Amazon, Microsoft, IT-CNP, IBM.
- Agency ATOs – 17 cloud services
  - Includes Microsoft, Google, Adobe, IBM, Oracle, Verizon

**FedRAMP Authorizations cover 500+ contracts and 160 known FISMA implementations**



# FedRAMP Ready Systems

## FedRAMP Ready Systems

- Released on October 16, 2014
- Goal is to assist agencies and CSPs achieve a FedRAMP authorization faster.

## Qualifications

- Documentation reviewed by FedRAMP PMO
- Minimum of FedRAMP PMO readiness review process
- CSPs will have varying degrees of readiness
  - Initial documentation
  - Testing completed by 3PAO
  - All required documentation
- Will also include open source code builds

The screenshot shows the cloud.cio.gov website. The header includes the cloud.cio.gov logo, a search bar, and navigation links: Learn (about cloud), Use (the cloud), Acquire (the cloud), Manage (your cloud), Secure (your cloud), and More (information). The breadcrumb trail is FedRAMP > Secure > FedRAMP Ready Systems. The main heading is 'FedRAMP Ready Systems' with the FedRAMP logo. The content explains that FedRAMP Ready systems have demonstrated readiness to meet FedRAMP requirements, covering a range of documentation and FedRAMP accredited 3PAO assessment results. It notes that not all systems in this category will be a CSP, and other categories may include build specifications and documentation for open source code. It states that systems must initiate a review of their documentation with the FedRAMP PMO, and that any system included must use an accredited 3PAO. Requests for documentation to be listed as FedRAMP Ready can be made through info@fedramp.gov. It also mentions that FedRAMP Ready systems allow potential agency customers and authorizing officials a starting point to initiate an authorization, and that systems with more complete documentation or assessments by an accredited 3PAO will allow potential agency customers and authorizing officials to go through the assessment and authorization process more rapidly to become FedRAMP compliant. Agency reviewers and authorizing officials should review the details of each system designated as FedRAMP Ready to fully understand how much work a CSP has completed and how much work remains to fully assess and authorize to become FedRAMP compliant. The systems listed as FedRAMP Ready include:

**Cloud Systems**

- ◆ OnCloud



# 3PAO Accreditation Program Privatization

## Cloud Auditor Accreditation (3PAO Program)

- First program (Federal or private) to accredit cloud auditors
- 31 organizations accredited to date
  - Including KPMG, Ernst & Young, Veris, Booz Allen Hamilton
  - ~60% are small businesses
  - One government agency (USDA ESC)
- Privatized in Nov 2013 with A2LA

## FedRAMP PMO 3PAO Program Oversight

- Define and update 3PAO requirements – ISO 17020 and FISMA
- Use a conformity assessment approach
- Can revoke accreditation at any time
- Requires 3PAO to agree to adhere to requirements for rigor and independence
- Access to evidence and reports created by A2LA

The screenshot shows the 'cloud.cio.gov' website with a navigation bar containing 'Learn', 'Use', 'Acquire', 'Manage', 'Secure', and 'More'. Below the navigation bar is a section titled 'Accredited 3PAOs' with the FedRAMP logo. The text below the title reads 'Below is the current listed of accredited 3PAOs.' followed by a table with three columns: Organization, POC, and POC Email.

| Organization                            | POC              | POC Email  |
|---|------------------|--|
| A-lign Security and Compliance Services | Gene Geiger      | <a href="mailto:gene.geiger@alignsecurity.com">gene.geiger@alignsecurity.com</a> |
| Blue Canopy                             | Jonathan Edwards | <a href="mailto:bcfedramp@bluecanopy.com">bcfedramp@bluecanopy.com</a>           |
| Booz Allen Hamilton                     | Amanda Cohen     | <a href="mailto:cohen_amanda@bah.com">cohen_amanda@bah.com</a>                   |
| BrightLine                              | Doug Barbin      | <a href="mailto:3PAO@brightline.com">3PAO@brightline.com</a>                     |
| Burke Consortium, Inc.                  | Steve Danz       | <a href="mailto:FedCloud@bcinow.com">FedCloud@bcinow.com</a>                     |
| COACT, Inc.                             | Stephen King     | <a href="mailto:sking@coact.com">sking@coact.com</a>                             |
| Coalfire Systems                        | Tom McAndrew     | <a href="mailto:3PAO@coalfire.com">3PAO@coalfire.com</a>                         |



# Major Update: NIST 800-53 Rev 4

## **Security Controls Baseline Update June 2014**

- Public comment period and PMO and JAB reviews
- Includes Privacy Appendix J

## **Rev. 4 Documentation Update Effort**

- Updates affected 13 core FedRAMP templates and documents
- Approximately 2000 hours to complete analysis and updates
- Approximately 1250 pages of edits

## **Major Overhauls and New Documentation**

- CONOPS updated to FedRAMP Security Assessment Framework
- Guide to Understanding FedRAMP including new lessons learned
- Creation of 80 test cases due to NIST not updating 800-53a



# Major Update: FedRAMP Baseline

## FedRAMP Baseline 800-53 Security Control Update

- Revision 3: 298 controls
- Revision 4: 325 controls

| Category of Changes          | #   |
|------------------------------|-----|
| Withdrawn by NIST            | 45  |
| Removed by Analysis          | 8   |
| Unchanged or Minimal Changes | 245 |
| Added by NIST                | 39  |
| Added by Analysis            | 41  |

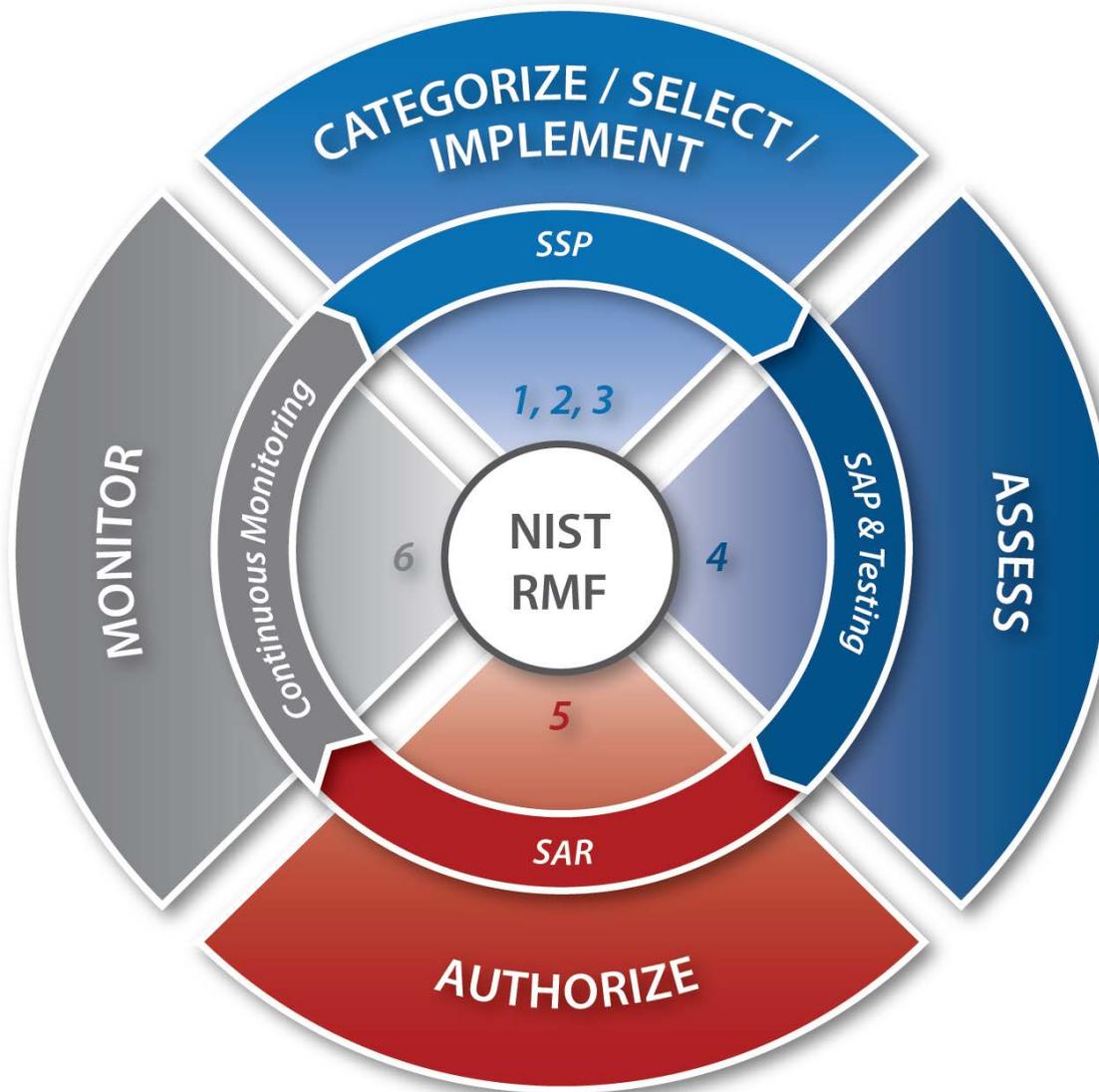
## JAB Members Approve Baseline

- Required by FedRAMP Policy Memo
- PMO has received recommended approval from JAB TRs



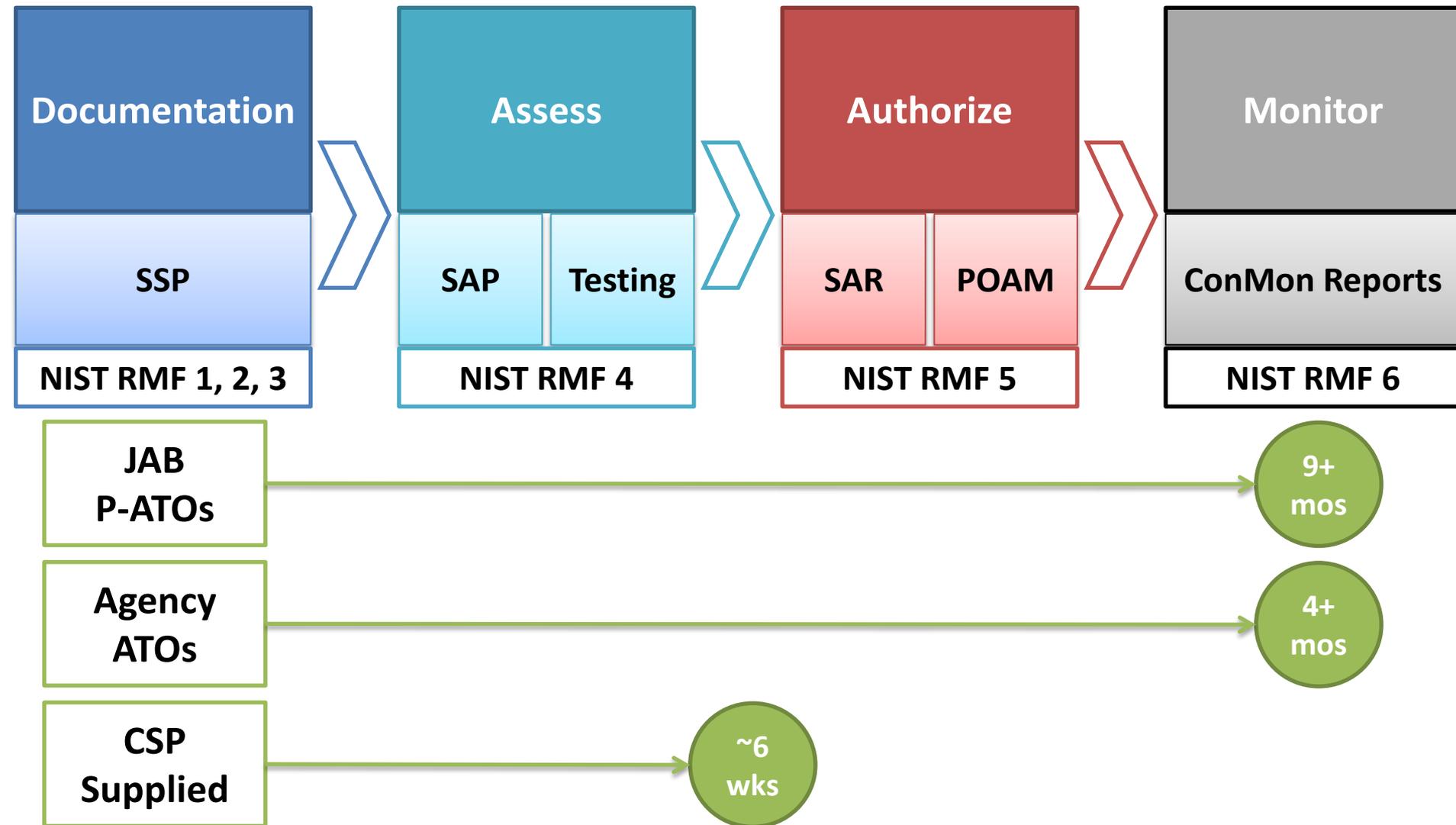
# FedRAMP Security Assessment Framework

*Replaces Concept of Operations (CONOPS)*





# Timeline for Security Assessment Framework





# FedRAMP 2 Year Roadmap

## Goals

1. Increase adoption and compliance
  - Greater agency involvement in ATOs
  - Provide enhanced training, education, and outreach
2. Improve efficiencies
  - Automation capabilities
  - Faster authorizations and more efficient ConMon reviews
  - Align CSPs with most appropriate authorizer: JAB or Agency
3. Continue to adapt
  - Refinement of ConMon with continuous authorization
  - Better integration with CDM and TIC
  - Establish high baseline

## Transparency

- Roadmap will be public document (November release)
- Remain accountable to all stakeholders for the continued evolution and success of the program



# Impact of FedRAMP

## Enables Cloud Security

- Successfully proven the USG 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
- FedRAMP is establishing a new marketplace for cloud vendors
  - Consistent positive press in Forbes, Wall Street Journal, Politico, InfoWeek, and others.

## 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 with 1 week review time and conservatively estimates a cost savings of 50% per authorization

## 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