



## FedRAMP Government Discussion

Matt Goodrich, FedRAMP Director

January 14, 2015

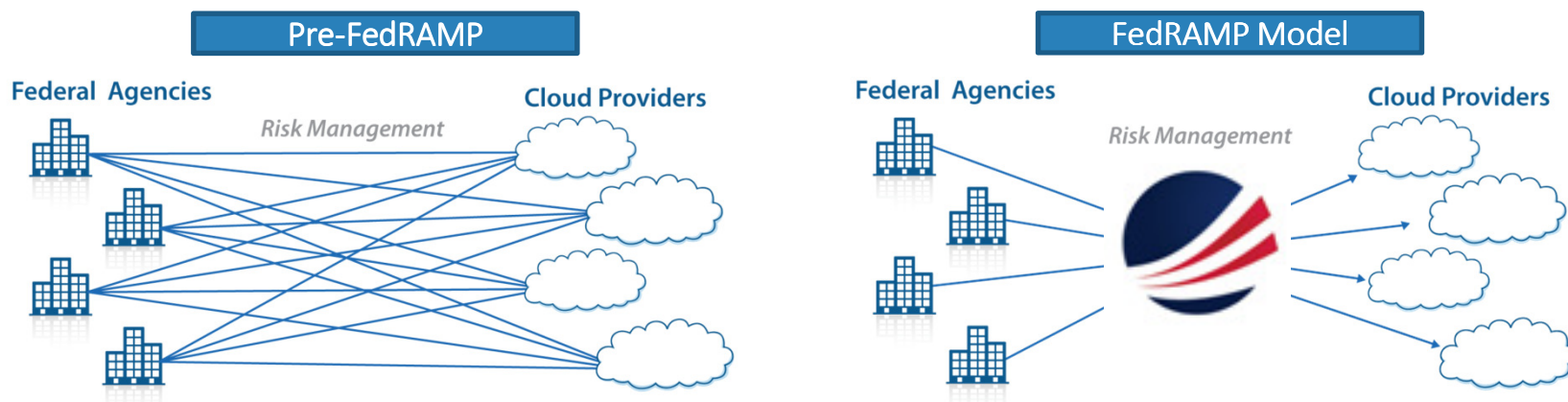
[www.fedramp.gov](http://www.fedramp.gov)



# FedRAMP Overview

## Ensuring Secure Cloud Computing

- FedRAMP was established via OMB Memo in December 2012.
- FedRAMP is the first government-wide security authorization program for FISMA – mandatory for all agencies and all cloud services
- FedRAMP’s framework is being modeled in other government security programs (mobile, data) and by other countries (Canada, UK, EU, China)
- FedRAMP’s focus is to ensure the rigorous security standards of FISMA are applied while introducing efficiencies to the process for cloud systems, key of which is re-use
- Conservative cost estimates for FedRAMP is \$40M for the govt alone





# FedRAMP Overview Current Statistics

The cloud systems below meet FedRAMP requirements.

**JAB Provisional Authorizations**

- Akamai - Content Delivery Services (IaaS)
- AT&T - Storage as a Service (IaaS)
- Autonomic Resources LLC - ARC-P (IaaS)
- CGI Federal - CGI Federal Cloud (IaaS)
- Concurrent Technologies Corporation (leveraging Autonomic Resources) - Unclassified Remote Hosted Desktops (URHD) (SaaS)
- Economic Systems - Federal Human Resources Navigator (SaaS)
- Hewlett Packard - HP Enterprise Cloud Services - Virtual Private Cloud (ECS-VPC) (IaaS)
- IBM - SmartCloud for Government (IaaS)
- Lockheed Martin - Solutions as a Service (SolaaS) Community Cloud (IaaS)
- Microsoft - Cloud Infrastructure (IaaS)

**Related Content**

- FedRAMP Package Request Form
- Cloud Systems in Process

The Cloud Service Providers (CSPs) listed below are actively pursuing either a FedRAMP Joint Authorization Board (JAB) Provisional Authorization or a FedRAMP Agency Authorization.

Provisional Authorization Path	Agency Authorization Path
<p>A CSP pursuing a JAB Provisional Authorization officially kicked off with the FedRAMP PMO and is assigned a FedRAMP ISSO to work through meeting the FedRAMP security requirements through the JAB. Additionally, a CSP has engaged the services of an accredited 3PAO to complete their security assessment.</p> <ul style="list-style-type: none"> <li>• Amazon</li> <li>• AT&amp;T</li> <li>• Autonomic Resources</li> <li>• CA Technologies</li> <li>• CenturyLink Technology Solutions</li> <li>• Clear Government Solutions (CGS)</li> <li>• Dell</li> <li>• Fiberlink, an IBM Company</li> </ul>	<p>A CSP pursuing an Agency Authorization committed to working with a Federal agency through the FedRAMP process to meet the FedRAMP security requirements through that agency. If you are a CSP actively working on a FedRAMP Agency authorization, and the cloud service is not identified, contact the FedRAMP PMO (<a href="mailto:info@FedRAMP.gov">info@FedRAMP.gov</a>) to add the cloud service to this page.</p> <ul style="list-style-type: none"> <li>• Acquia</li> <li>• Adobe Systems</li> <li>• Applian</li> <li>• Avue Technologies</li> <li>• BMC Software</li> <li>• Cornerstone OnDemand</li> <li>• Decision Lens Inc.</li> <li>• Google</li> </ul>

## Authorizations

- JAB P-ATOs - 15
  - Includes services from IBM, Microsoft, Akamai, HP, Lockheed Martin
- Agency ATOs - 11
  - Includes Amazon, AINs, USDA, Micropact, Salesforce

## In Process CSPs

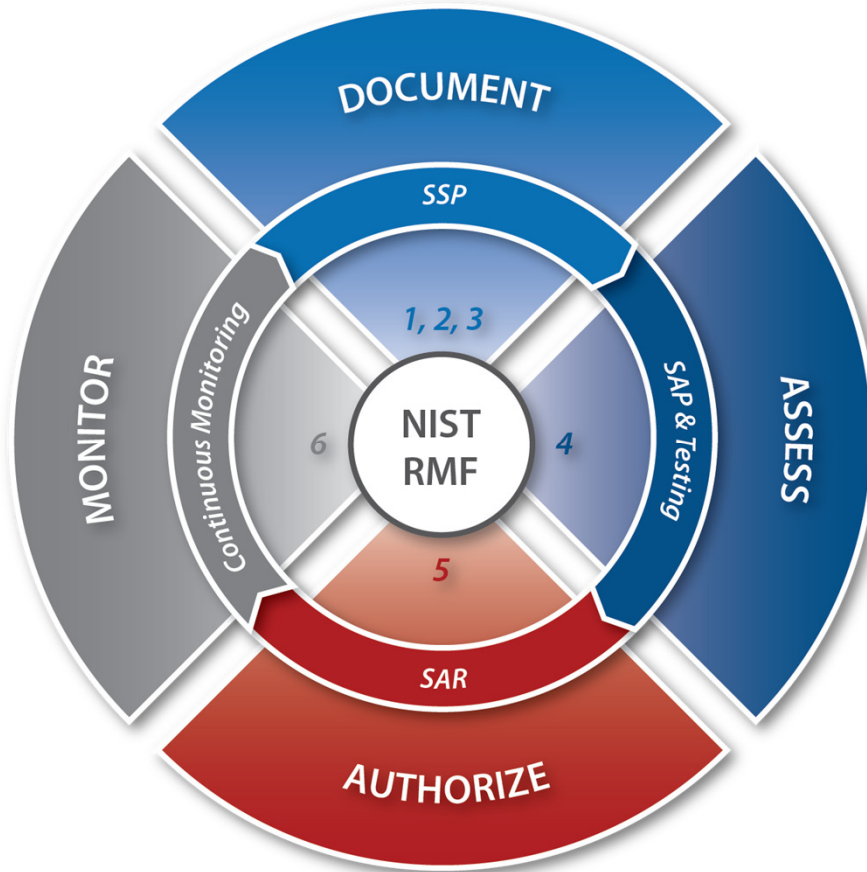
- JAB P-ATO – 15
  - Includes services from Dell, SecureKey, Oracle, Amazon, Microsoft, IT-CNP, IBM
- Agency ATOs – 23
  - Includes Microsoft, Google, Adobe, IBM, Oracle, Verizon



## Agency ATO Quick Guide



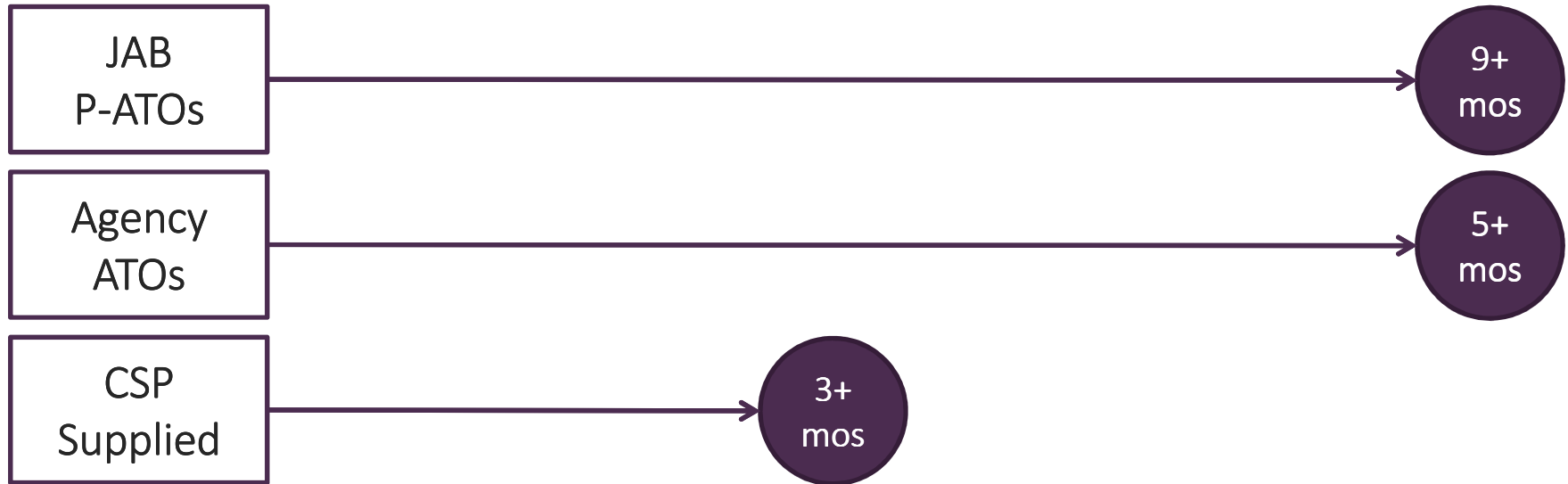
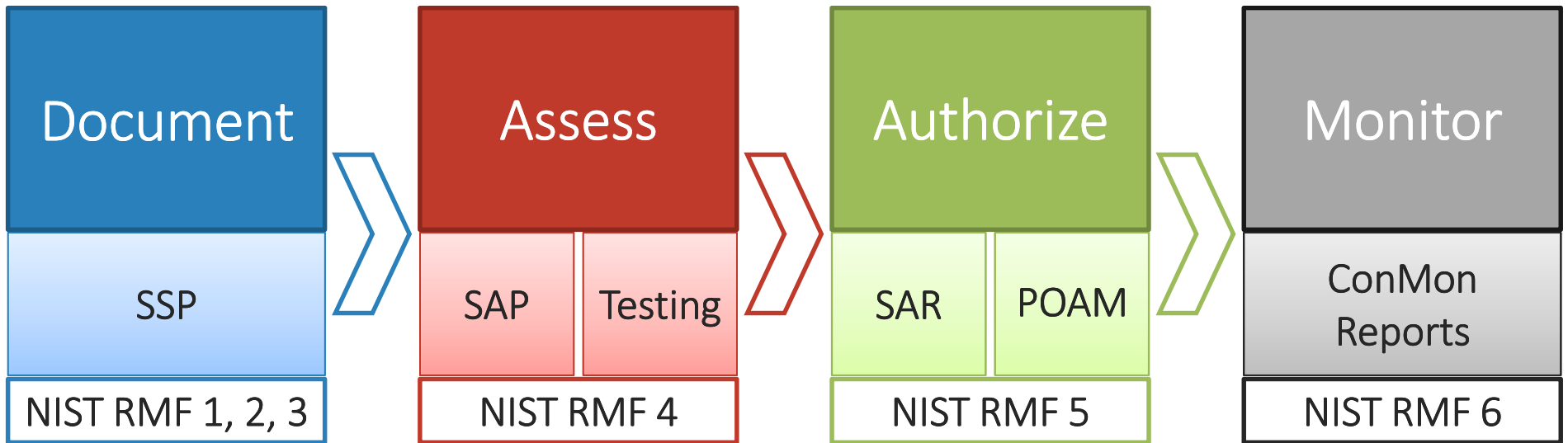
# Agency ATO Guide FedRAMP Security Assessment Framework



- The agency ATO process should follow the FedRAMP Security Assessment Framework (SAF)
- The SAF is based on the NIST Risk Management Framework
- The FedRAMP Security Assessment Framework is available at [FedRAMP.gov](https://www.fedramp.gov) on the Templates and Key Documents webpage



# Agency ATO Guide Timeline for the SAF





# Agency ATO Guide Considerations During SAF

## TRUSTED INTERNATE CONNECTIONS (TIC)

- CSPs are required to support agency TIC implementations
  - CSPs do not host TIC components in their environments

## FEDERAL INFORMATION PROCESSING STANDARD (FIPS) PUB 140-2

- CSPs are required to implement only FIPS Pub 140-2 for all cryptographic implementations
  - External interfaces with Federal customers

## PERSONAL IDENTITY VERIFICATION (PIV)

- Agencies are required to use PIV for multi-factor authentication
  - CSPs are required to support PIV as a multi-factor solution



# Agency ATO Guide

## Document Checklist – Templates Available

- ATO Packages submitted to FedRAMP should have the following FedRAMP templates included. The PMO will check these documents for completeness
- FedRAMP Templates are available at [FedRAMP.gov](http://FedRAMP.gov) on the Templates and Key Documents webpage
- We suggest that you use the Test Cases that we released in Excel format for public comment:  
<http://cloud.cio.gov/document/rev-4-test-case-workbook>

### FedRAMP Templates Available:

- FIPS 199
- Control Implementation Summary (CIS)
- System Security Plan
- Information System Security Policy
- User Guide
- E-Authentication Template
- Privacy Threshold Analysis (PTA) / Privacy Impact Analysis (PIA)
- Rules of Behavior (ROB)
- IT Contingency Plan
- Security Assessment Plan (SAP)
- Test Case Workbook
- Security Assessment Report (SAR)
- Plan of Action and Milestone (POA&M)
- ATO Letter
- Cert Letter





# Agency ATO Guide

## Document Checklist – Docs w/o Templates

- The Agency ATO Packages submitted to FedRAMP should have the following documents included. The PMO will check these documents for completeness
- The documents listed on this slide do not have an FedRAMP template

### No Template Available:

- Policies and procedures
- Business Impact Analysis
- Configuration Management Plan
- Incident Response Plan
- Interconnection Security Agreement (ISA / MOU)
- Penetration Test Plan



# Agency ATO Guide

## Granting an ATO

### GRANTING AN AUTHORITY TO OPERATE (ATO)

- Once a review is complete, an authorization should be granted and provided to the FedRAMP PMO
- Authorization for Cloud Providers should not be tied to individual Applications or Platforms
  - CSPs are intended for multiple tenants, use by different customers
  - Authorizations should be viewed as building blocks
- For Microsoft packages, consuming agencies will need to leverage all of the packages that relate to the service being consumed
  - e.g. GFS, Azure, O365
- Customer Agencies will ALWAYS have some responsibility for controls
  - e.g. an agency will always have to enforce 2 factor authentication



# Agency ATO Guide

## Sample ATO and Cert Letter Template

- Included with the authorization package should be a Certification Letter and ATO Memo detailing your agency's authorization.
- A sample Certification Letter is attached below:



Sample Cert  
Letter

- You can find the Sample [FedRAMP ATO Memo Template](#) at FedRAMP.gov on the Templates and Key Documents webpage