FedRAMP
Federal Risk and Authorization Management Program

June 2014 Program Updates

Agenda

Topic	Speaker	Time
Welcome	Kathy Conrad	9:00 – 9:05
FedRAMP Update	Maria Roat	9:05 – 9:40
3PAO Program Update	Sam Dizor Carter	9:40 – 9:50
Security Assessment Framework	Matthew Goodrich	9:50 – 10:20
Questions and Answers		10:20 – 10:40
BREAK		10:40 – 10:50
FedRAMP Security Controls Update and NIST SP 800-53 Rev-4 Transition	Matthew Goodrich	10:50 – 11:20
Continuous Monitoring	Andrew Lins	11:20 – 11:40
Wrap-up and Questions and Answers		11:40 – 12:00

Welcome

Kathy Conrad
Acting Associate Administrator
GSA Office of Citizen Services and Innovative Technologies

FedRAMP Update

Maria Roat
FedRAMP Director
GSA Office of Citizen Services and Innovative Technologies

FedRAMP: A brief history

Feb 2010
Kundra Announces FedRAMP
Security Working Group concept announced

Nov 2010
Public Draft Released
Concept, Controls and Templates released for public comment

Jul-Sep 2011
3PAO Concept Planned
NIST, JAB and GSA work to establish 3PAO program concept

Jan 2012
JAB Finalizes Baseline
FedRAMP security controls for LOW and MODERATE released

Dec 2012
First Provisional Authorization
JAB grants Provisional ATO to Autonomic Resources

June 2014
Two-Year FedRAMP Operational Anniversary
FedRAMP now required for all cloud solutions covered by policy memo

2010 | 2011 | 2012 | 2013 | 2014

Jun 2010
JAB Drafts Baseline
Working with ISIMC & NIST, JAB develops initial baseline

Feb/Mar 2011
Tiger Teams Convene
FedRAMP conducts Gov-wide consensus meetings on comments

Dec 2011
OMB Releases Policy Memo
Federal CIO, Steven VanRoekel signs FedRAMP Policy

Feb 2012
CONOPS published
Timelines and processes articulated

Jun 2012
FedRAMP Launches
Templates published, staffing in place, CSPs start applying

May 2013
First Agency Authorization
HHS Issues ATO to Amazon

Transition to 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

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

- 4 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

JAB FedRAMP Provisional ATO

- **Autonomic Resources** IaaS
- **CGI Federal** IaaS
- **AT&T StaaS** Iaas
- **Akamai CDN** IaaS
- **HP ECS-VPC** IaaS
- **Lockheed Martin SolaS-I** IaaS
- **Microsoft GFS** IaaS
- **Microsoft Azure** PaaS
- **IBM** PaaS
- **Oracle FMCS** PaaS
- **Economic Systems FHR Navigator** SaaS
- **CTC URHD** SaaS

FedRAMP AGENCY Authority to Operate

- **Amazon US East West** IaaS
- **Amazon GovCloud** IaaS
- **USDA (NITC)** IaaS
- **AINS** eCase SaaS

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

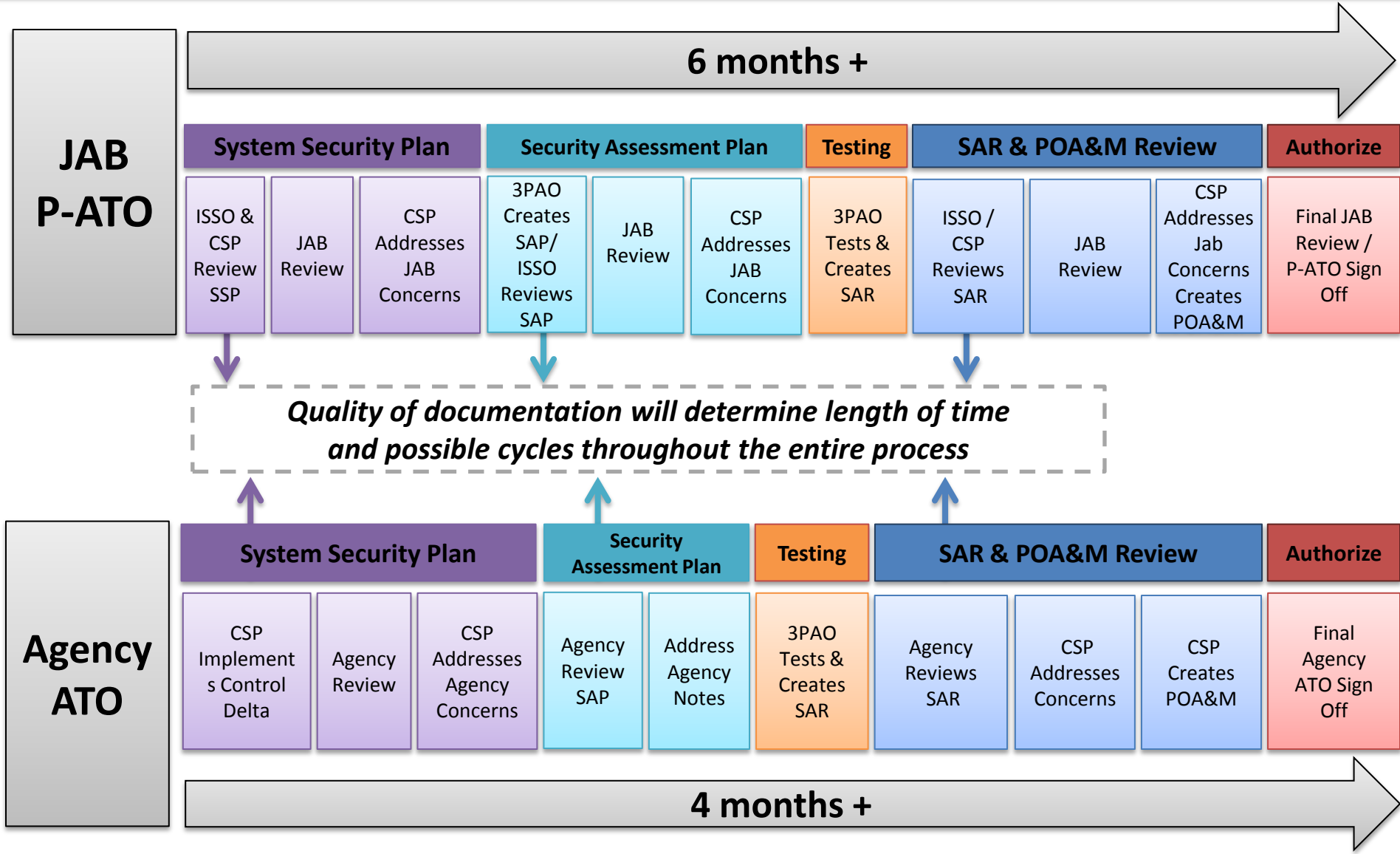
Agency ATO

- 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



Agency Responsibilities

- All **new** cloud projects must use FedRAMP baseline controls and templates for initiating, reviewing, granting, and revoking security authorizations
- All **existing** cloud projects (implemented or in the acquisition process) must meet FedRAMP requirements by June 2014
- **All cloud projects**
  - Establish and implement **continuous monitoring plans** through incident response and mitigation capabilities
  - Require cloud services providers to meet FedRAMP requirements via contractual provisions
  - Use FedRAMP repository as ATOs are granted by JAB
- Agencies must report to OMB annually cloud services that cannot meet FedRAMP requirements

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

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

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

3PAO Update

Samantha Dizor Carter
Senior Accreditation Officer
American Association for Laboratory Accreditation (A2LA)

Topics

- Overview of Accreditation
- Preparing for an on-site assessment
- On-site assessment overview
- Post assessment activities

Initial Accreditation Process

- Review all applicable requirements and ensuring the organization is in compliance with those requirements
- Identify desired scope of accreditation
- Submit application and fees
- On-site assessment of organization
- Resolve any deficiencies within required time frame
- Final accreditation made by the accreditation body
  - FedRAMP determines inclusion in 3PAO program once 3PAO is accredited by A2LA

Application for Accreditation

- Application
- Quality Manual
- Organization Chart
- Completed Assessor Checklist
  - ISO/IEC 17020
  - FedRAMP Program Checklist
- Scope: If additional accreditation beyond FedRAMP is desired
- New applicants: System Security Plan, Security Assessment Plan, and Security Assessment Report
- Renewal Application or applicants already accredited by FedRAMP: provide a list of all jobs completed.

After Application Submittal

- Application checked for completeness
- Assessor assigned with organization's approval
- Assessor contacts the organization to request documents and determine an assessment date

About Assessors

- Technical experts in their field, assigned to organizations in their field only
- Considered to be fact finders – they collect information to show an organization's conformance with applicable requirements
- Trained and evaluated by qualified A2LA staff
- Undergo periodic refresher training
- Required to stay current on changes within their discipline

On-site Assessment

- Interview technical staff to verify knowledge of technical procedures and policies
- Witness inspection activities being performed
- Inspect equipment and facilities
- Conduct field visits if available
- Collect evidence that the quality manual meets the accreditation criteria and is being implemented by the organization
- Collect objective evidence to demonstrate that the organization is in compliance with all of the requirements for accreditation and their own policies and procedures

What is Audited

- Management Requirements
  - Management or administrative activities
  - Organization, control of quality records
  - Strict adherence to documented procedures
  - Internal audits, management review records
  - Corrective and preventative actions
  - Contract review
  - Training records
  - Purchasing records

What is Audited

- Technical Requirements
  - Performance of inspections
  - Sampling of inspection activities
  - Review of System Security Reports, Security Assessment Plans, and Security Assessment Reports
  - Interview with inspectors
  - Review training program and supervision for new employees

Deficiency (Nonconformity)

- A departure from or an instance of noncompliance with a condition or criterion for accreditation
  - ISO/IEC 17020
  - Method
  - Specific FedRAMP program requirement
  - Organizations own policies and procedures

After the Assessment

- Assessor will leave the deficiency report with all deficiencies listed
- Initial corrective action response including supporting documentation is required within 30 days of the assessment
- Corrective action must include a root cause analysis
  - An investigation into what caused the nonconformance
- Corrective action and supporting documentation is reviewed by A2LA staff; additional information is requested if needed
- The Accreditation Council is balloted
- Accreditation is granted when all issues are resolved and all fees are paid

Following Initial Accreditation

- An organization is accredited for a two (2) year period
- Surveillance assessment is performed around first year after being accredited
  - One day assessment to ensure deficiencies cited during the initial assessment are closed and to review certain quality system documents
- Full reassessment around the second year of being accredited
- Annual Review after first renewal of accreditation

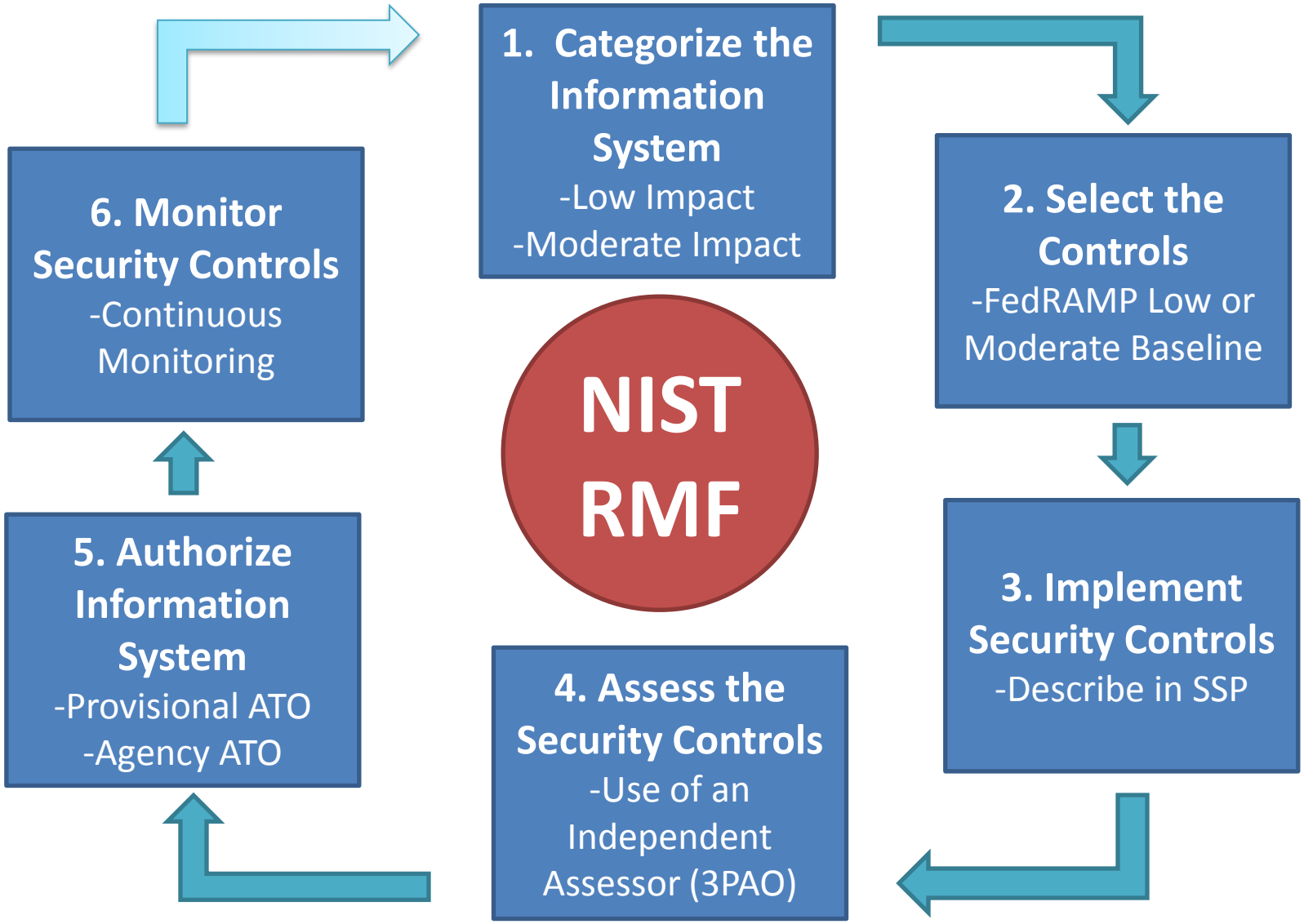
Current Status of Applications

- Total number of complete applications received: 22
  - Currently accredited 3PAOs: 8
  - Potential 3PAOs: 14
- Application Processing Status
  - On-site assessments scheduled: 7
  - On-site assessments completed: 3
- Early 2015 or before - A2LA completes accreditation process for initial applicants
- Early 2016 or before - All current FedRAMP 3PAOs that plan to continue with FedRAMP accredited through A2LA

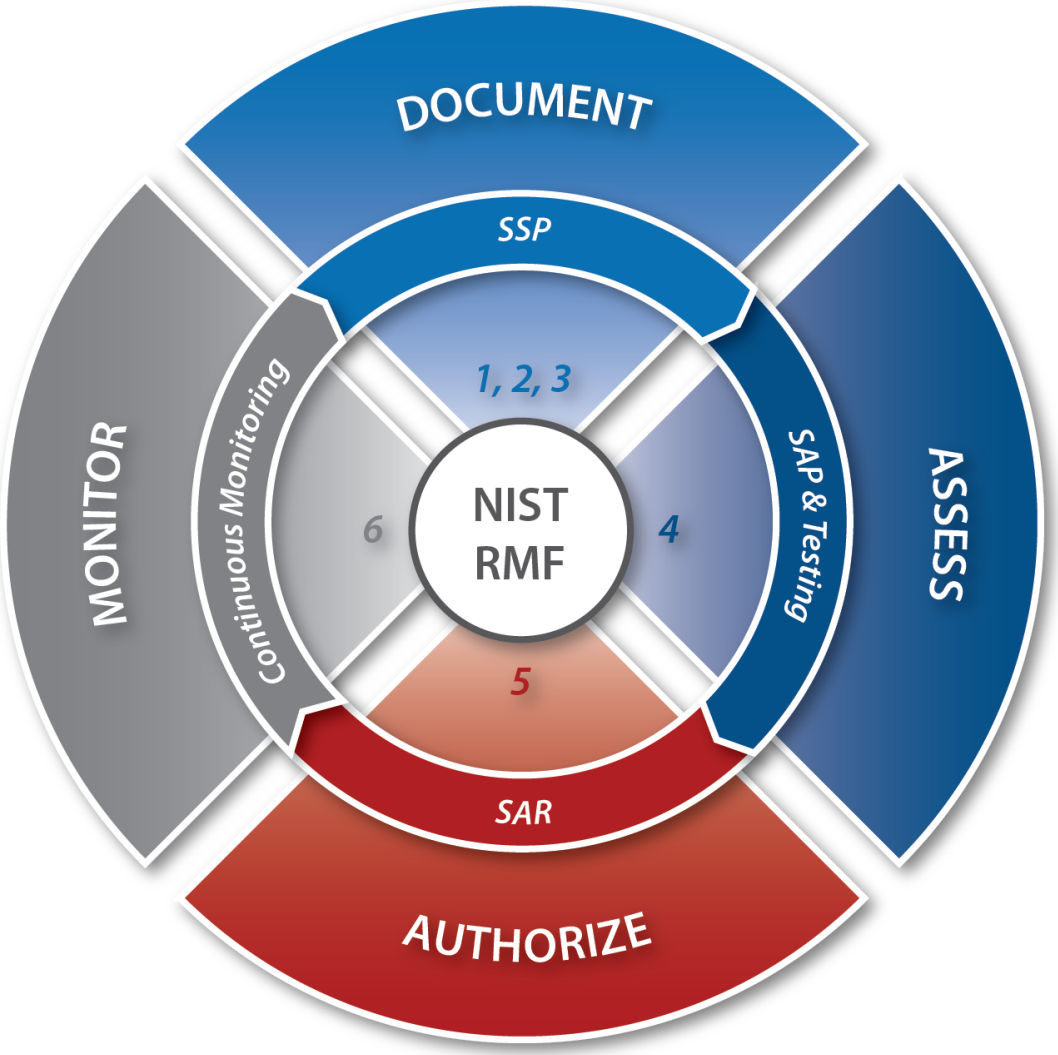
Security Assessment Framework

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

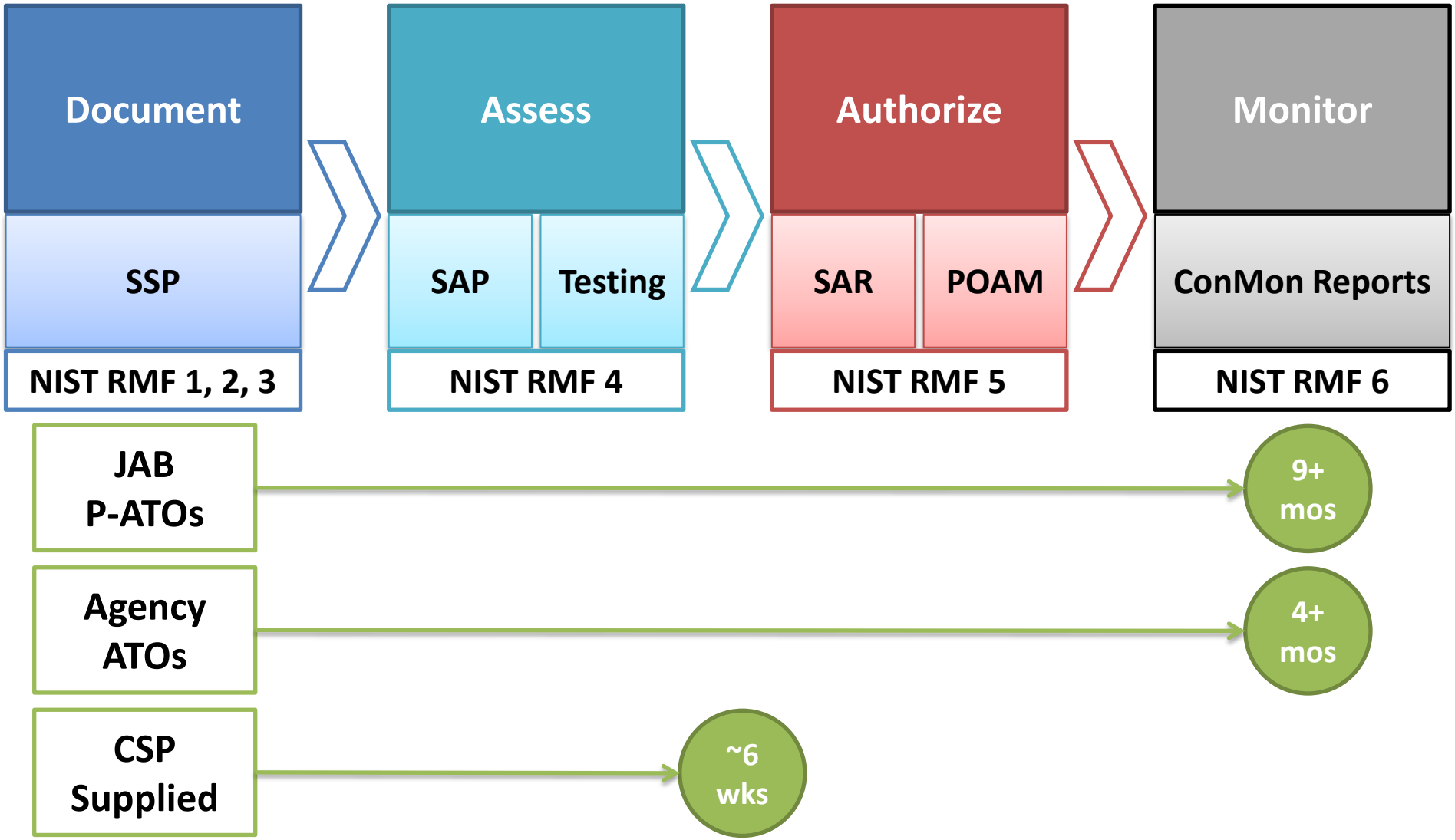
FedRAMP Relationship to the NIST Risk Management Framework



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

Questions and Answers

BREAK

FedRAMP Security Controls Update and NIST SP 800-53 Rev-4 Transition

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

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 were 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

- Released April 22, 2014
- 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

Continuous Monitoring

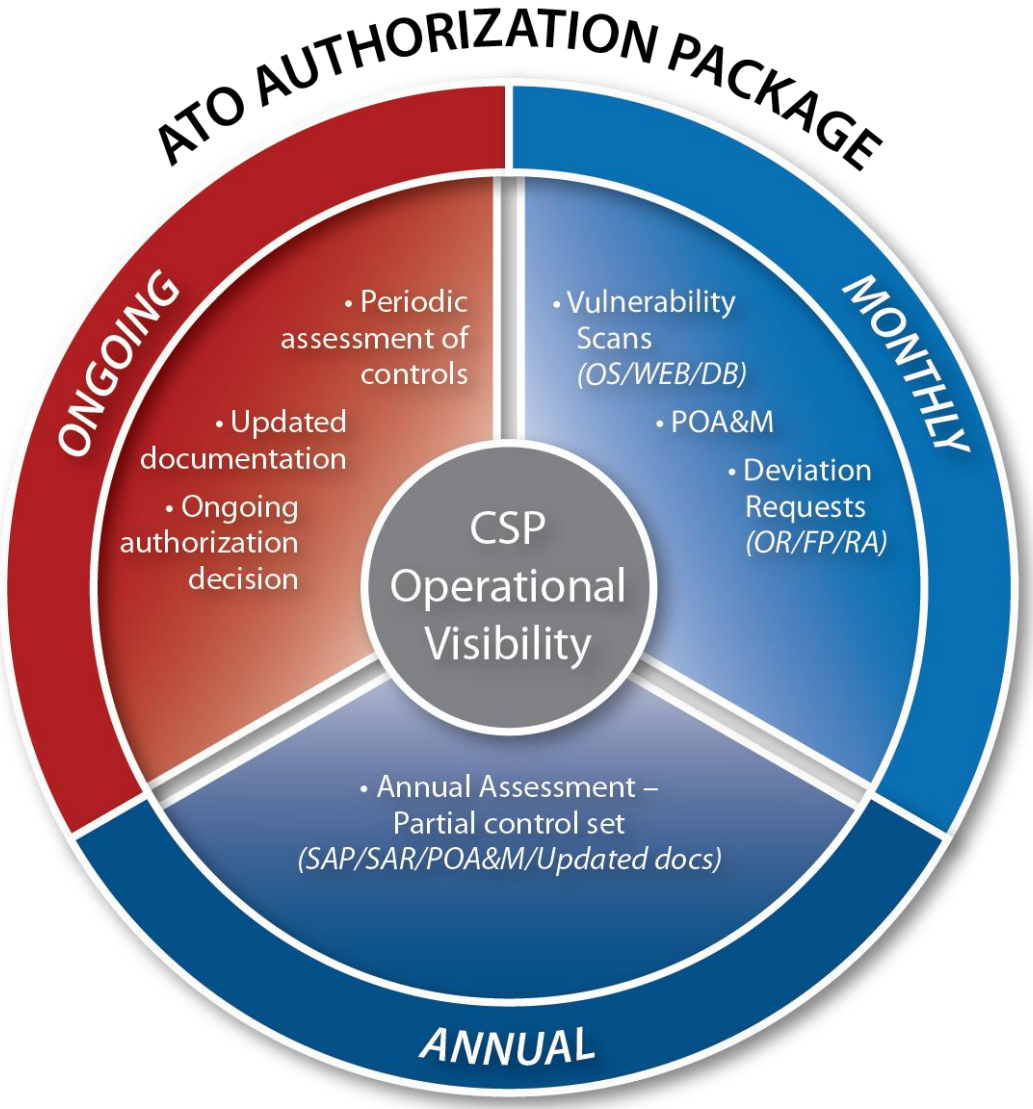
Andrew Lins
FedRAMP ISSO
GSA Office of Citizen Services and Innovative Technologies

Continuous Monitoring Process Areas

Continuous Monitoring

	Cloud Service Provider	Authorizing Official
1 Operational Visibility	Annual Assessment	Review control reporting provided by CSP
2 Change Control	Obtains Change Reports / POA&M Updates	Ensure POA&M / System Changes meet ATO requirements
3 Incident Response	Notifications	Responds to Incidents & Coordinate with US-CERT

ConMon Process: Operational Visibility



ConMon Process: Change Control

CSP Responsibilities

- Notifies Authorizing Officials of any planned non-routine changes to the system
- Submits Change Form
- Updates documentation
- Submits SAP and SAR as required
- Notifies customers

Authorizing Official Responsibilities

- Determines type of change and potential impact to authorization
- Reviews/verifies forms and reports
- Authorizing Official approves as required

ConMon Process: Change Control

Planned Change

Routine Maintenance	Addition of New Component Within Boundary – Doesn't Affect Customer	Addition of New Component that Impacts Boundary	Extension of Boundary for Authorization	Emergency Changes in Response to incident/event or system failure
• CSP self-tests and provides results to ISSO as part of ongoing continuous monitoring deliverables	• CSP self-tests and provides results to ISSO as part of ongoing continuous monitoring deliverables	• 3PAO Testing required (SAP/SAR) • Authorizing Official Review	• 3PAO Testing for updated and/or reauthorization package submission • Authorizing Official Review	• Notify ISSO in accordance with IR Plan • Change Form submission and testing results (i.e. security impact assessment)

Action

ConMon Process: Incident Response

CSP Responsibilities

- Follows CSP IR Plan and FedRAMP IR Communication Plan for notification requirements to FedRAMP, Agencies, and US-CERT
- Submits after-action report, including root cause analysis to FedRAMP and Authorizing Officials
- Submits after-action report to US-CERT as required
- Follows change management controls procedures as required

ISSO Responsibilities

- Notifies Authorizing Official management
- Continues to monitor and coordinate with CSP as required
- Reviews after-action report and root cause analysis and other artifacts that may be provided
- Follows Agency IR procedures for reporting to US-CERT

FedRAMP Incident Communication Plan

(DRAFT)

Version 1.0

February 15, 2013

For Official Use Only

Continuous Monitoring Responsibilities By Authorization Type

Authorizing Official (Authorization Level)	Responsibility for Continuous Monitoring
CSP Supplied	CSP
Agency	Agency
JAB	FedRAMP JAB

Authorizing Official Responsibilities	Leveraging Agency Responsibilities
Analyzes all artifacts submitted – scans, POA&M, Deviation Requests, and evidence/artifacts for accuracy and consistency	Reviews artifacts in the Secure Repository to ensure acceptable risk posture is maintained
Coordinates with CSPs to address questions/discrepancies/concerns	Monitors security controls that are agency responsibilities
Reports monthly to Authorizing Official on status and risk posture	

Lessons Learned

- Inventory Management
  - Maintaining an accurate inventory
- Configuration Management
  - Reopened vulnerabilities
- Automated Tool Usage
  - Understanding how to configure and interpret scan results
  - Authentication/Privileges
  - Completeness/Accuracy

Lessons Learned (Continued)

- Schedule of Deliverables
  - Align schedule with patch and release releases
  - Plan for holidays/employee leave
- Deviation Requests
  - Provide sufficient details/evidence for deviation requests
- Quality
  - Leverage lessons learned from P-ATO process into continuous monitoring deliverables

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