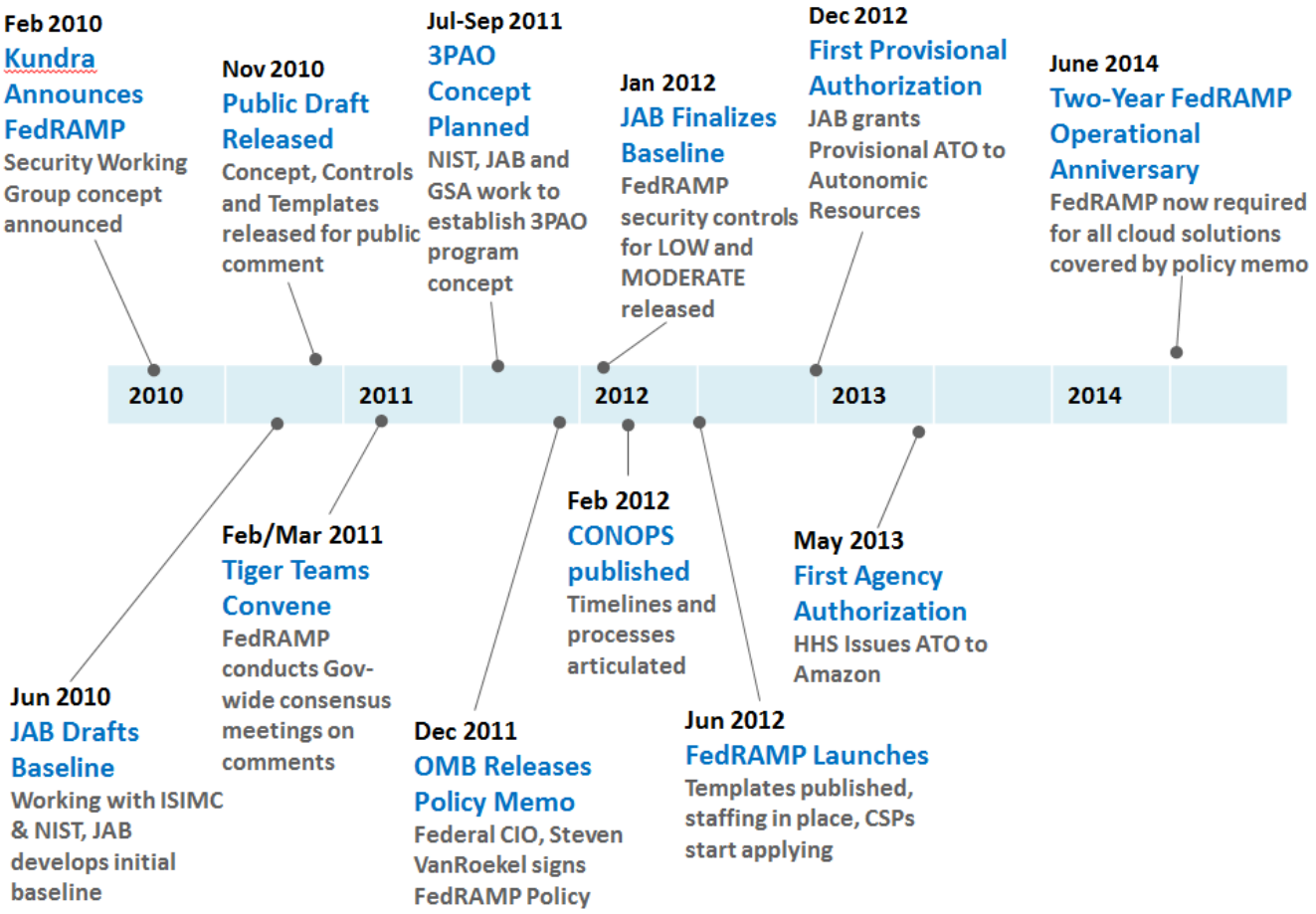
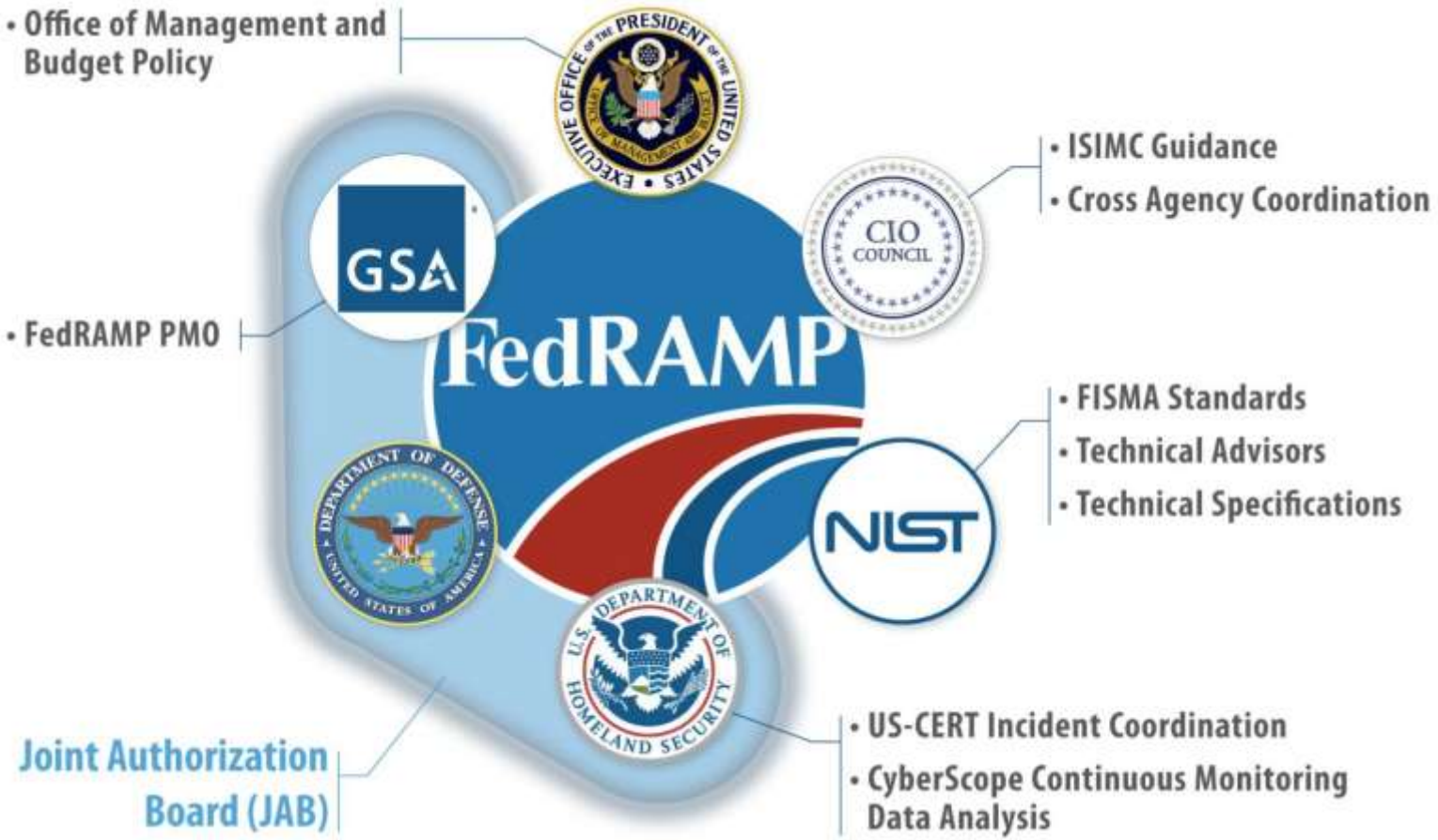
FedRAMP and the A2LA Accreditation Process for Third Party Assessment Organizations (3PAOs)

Ashley Kamauf
A2LA

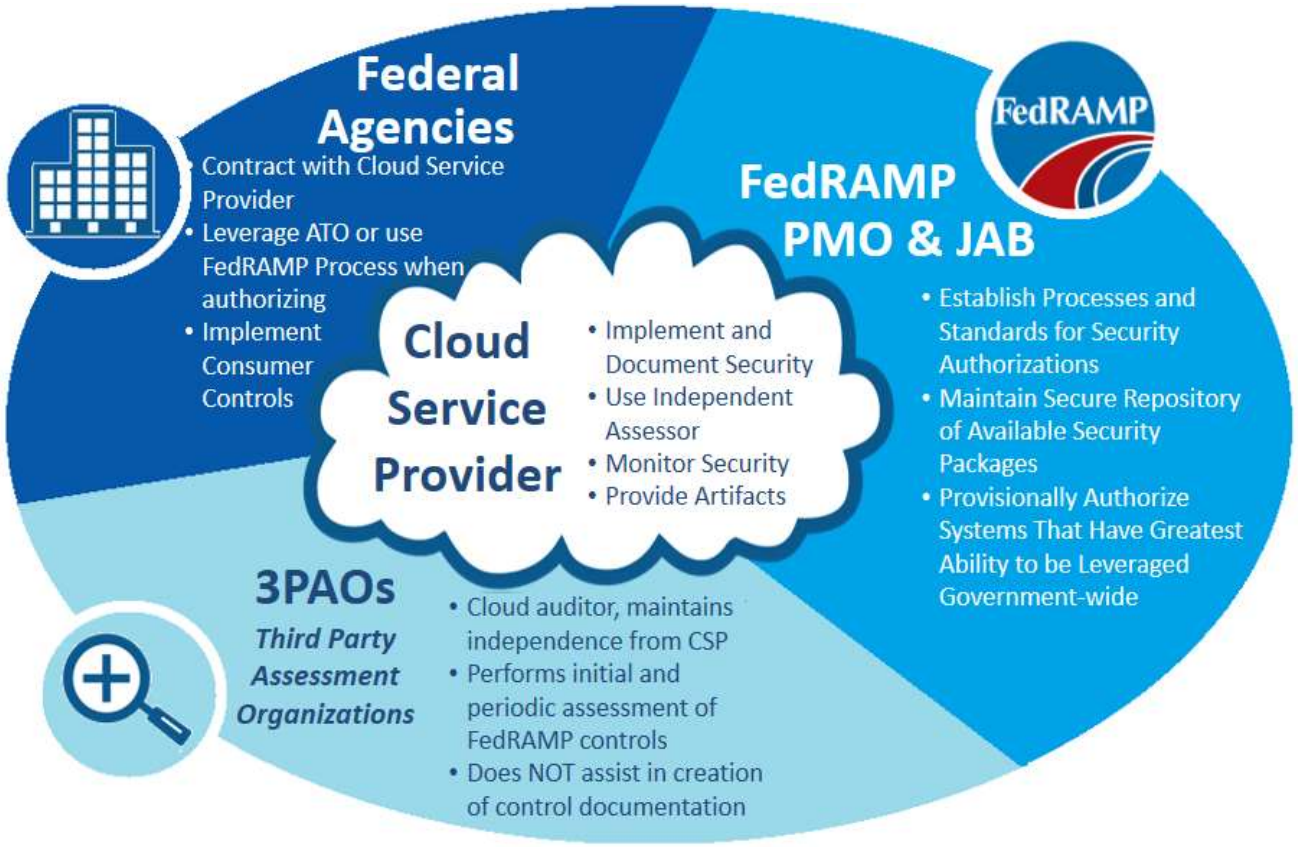
FedRAMP: A Brief History



FedRAMP Governance Entities



FedRAMP Key Stakeholders & Responsibilities



What are the benefits of the FedRAMP program?

- Improving cloud security
- Provides a baseline of secure functionality for government agencies
- All approved providers have an approved set of offerings that meet at least moderate FISMA requirements
- Outsource cloud maintenance to the CSP
- Cost savings (less maintenance)

Impact of FedRAMP

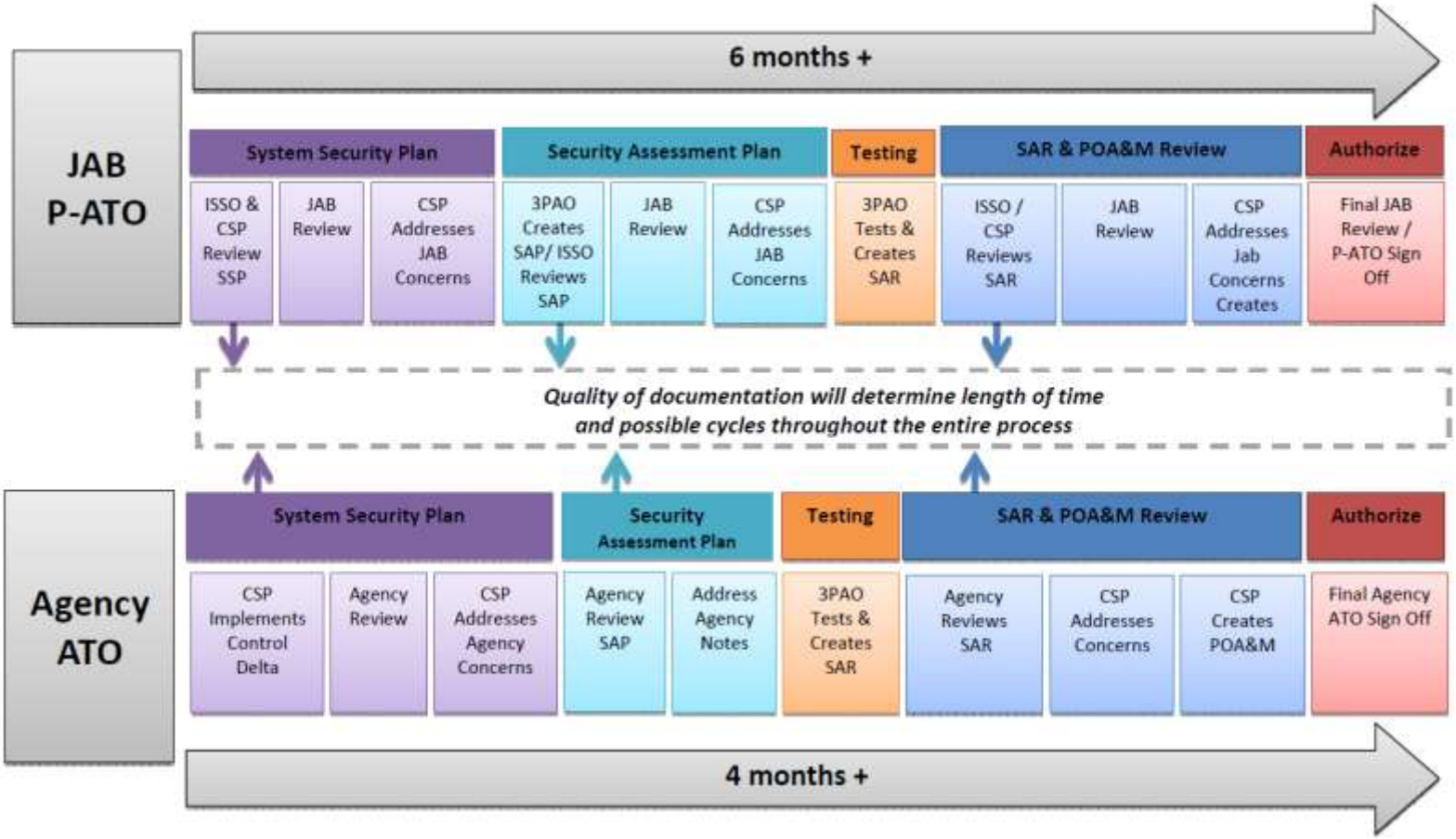
Enables Cloud Security

- Successfully proven the U.S. government can securely use all types of cloud computing
- Created a standards based approach to security through risk management
- Establishing a new marketplace for cloud vendors

Ahead of the Curve

- Commercial industry is looking to FedRAMP as a model for building standards-based security for cloud services

Authorization Timeline



A2LA 3PAO Assessment Process

- 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 decision made by the accreditation body

On-site Assessment

- Interview with technical staff to verify knowledge of technical procedures and organizational policies
- Witness inspection activities being performed
- Inspection of equipment and facilities
- Evidence that the quality manual meets the accreditation criteria and is being implemented by the organization
- Objective evidence collected 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 Plans (SSP), Security Assessment Plans (SAP), and Security Assessment Reports (SAR)
  - Interviews with inspectors
  - Review training program and supervision for new employees

Deficiencies

- Definition
  - Any nonconformity to accreditation requirements
- Including:
  - Policies and procedures do not conform to ISO/IEC 17020
  - Incomplete/unimplemented required policies or procedures
  - Organization does not conform to additional A2LA policies and program requirements
- Expectations:
  - Correct deficiency and submit evidence to A2LA within 30 days/6 month maximum for new organizations

After the Assessment

- Assessor will leave the deficiency report with all deficiencies listed
- Initial corrective action response including supporting documentation is submitted to A2LA
- 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

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

Questions?

Ashley Kamauf
Accreditation Officer II

akamauf@A2LA.org
(301) 644-3215