Federal Risk and Authorization Management Program (FedRAMP)

ISPAB

June 14, 2013

Matt Goodrich, JD

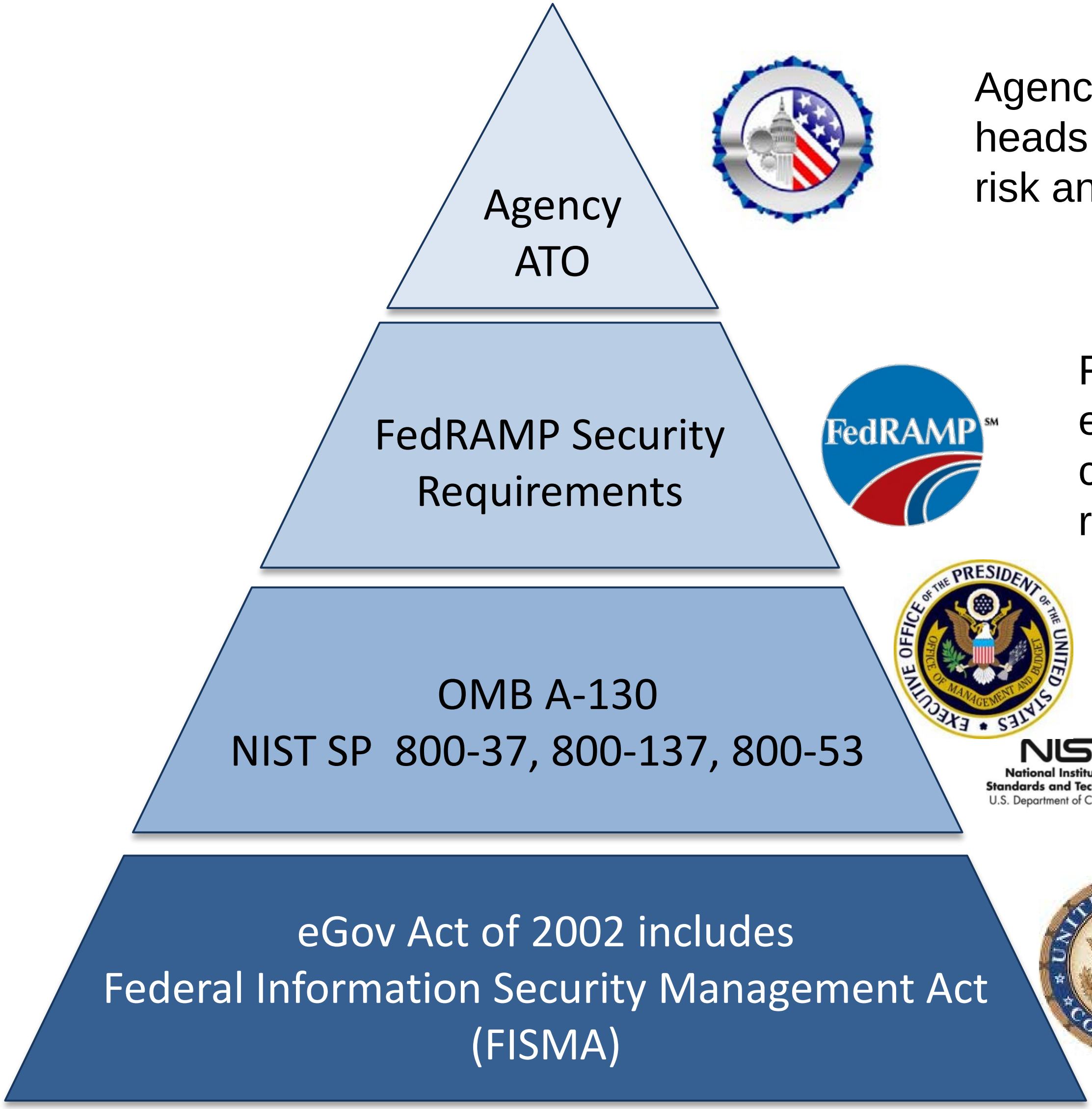
FedRAMP, Program Manager | Federal Cloud Computing Initiative| OCSIT | GSA

What is FedRAMP?

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

- This approach uses a “do once, use many times” framework that will save cost, time, and staff required to conduct redundant agency security assessments.

FedRAMP Policy Framework



Agency ATO

FedRAMP Security Requirements

OMB A-130
NIST SP 800-37, 800-137, 800-53

eGov Act of 2002 includes
Federal Information Security Management Act (FISMA)

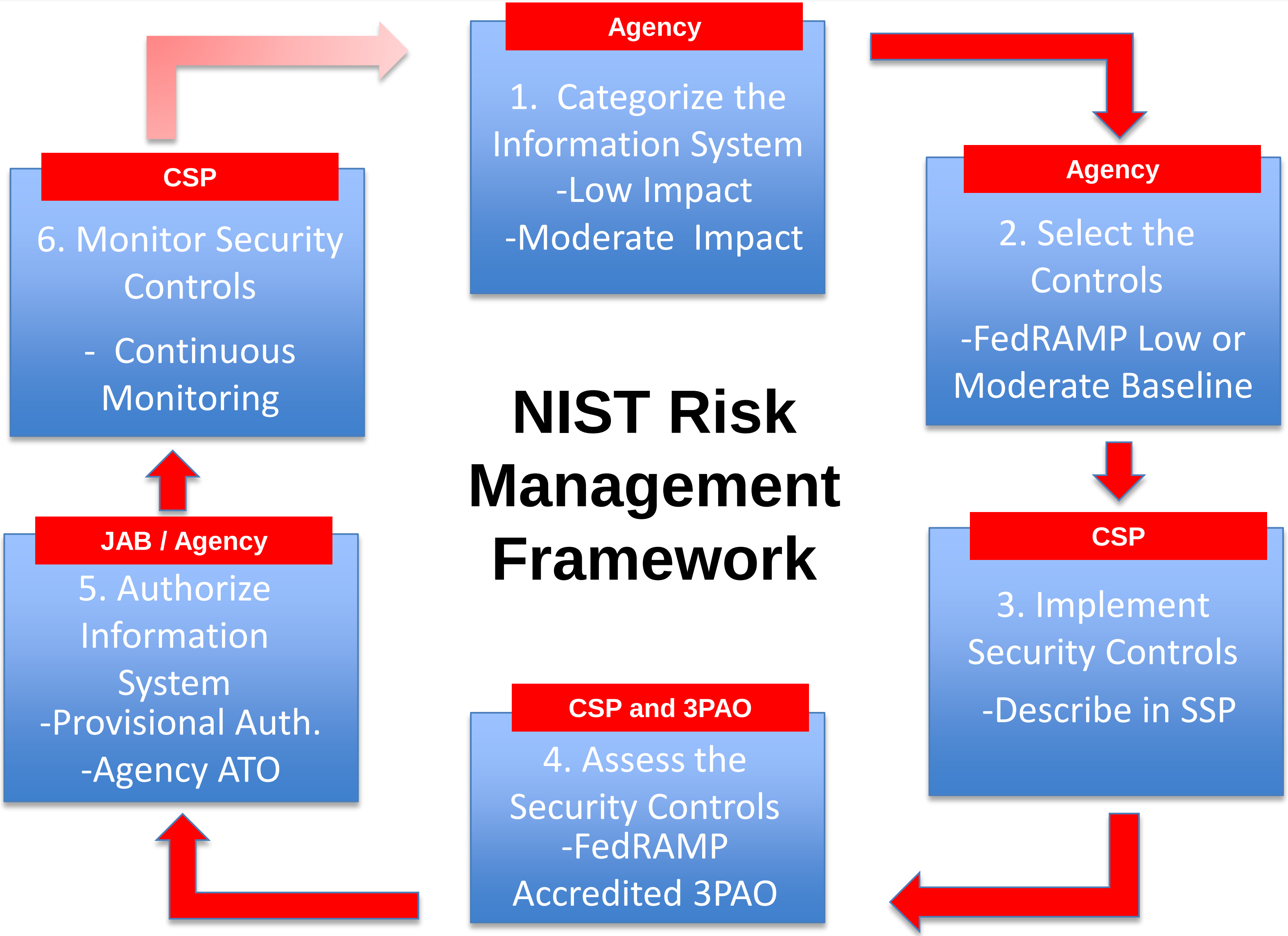
Agencies leverage FedRAMP process, heads of agencies understand, accept risk and grant ATOs

FedRAMP builds upon NIST SPs establishing common cloud computing baseline supporting risk based decisions

OMB A-130 provide policy, NIST Special Publications provide risk management framework

Congress passes FISMA as part of 2002 eGov Act

FedRAMP and NIST RMF 800-37



NIST Risk Management Framework

Agency

1. Categorize the Information System
-Low Impact
-Moderate Impact

Agency

2. Select the Controls
-FedRAMP Low or Moderate Baseline

CSP

3. Implement Security Controls
-Describe in SSP

CSP and 3PAO

4. Assess the Security Controls
-FedRAMP Accredited 3PAO

JAB / Agency

5. Authorize Information System
-Provisional Auth.
-Agency ATO

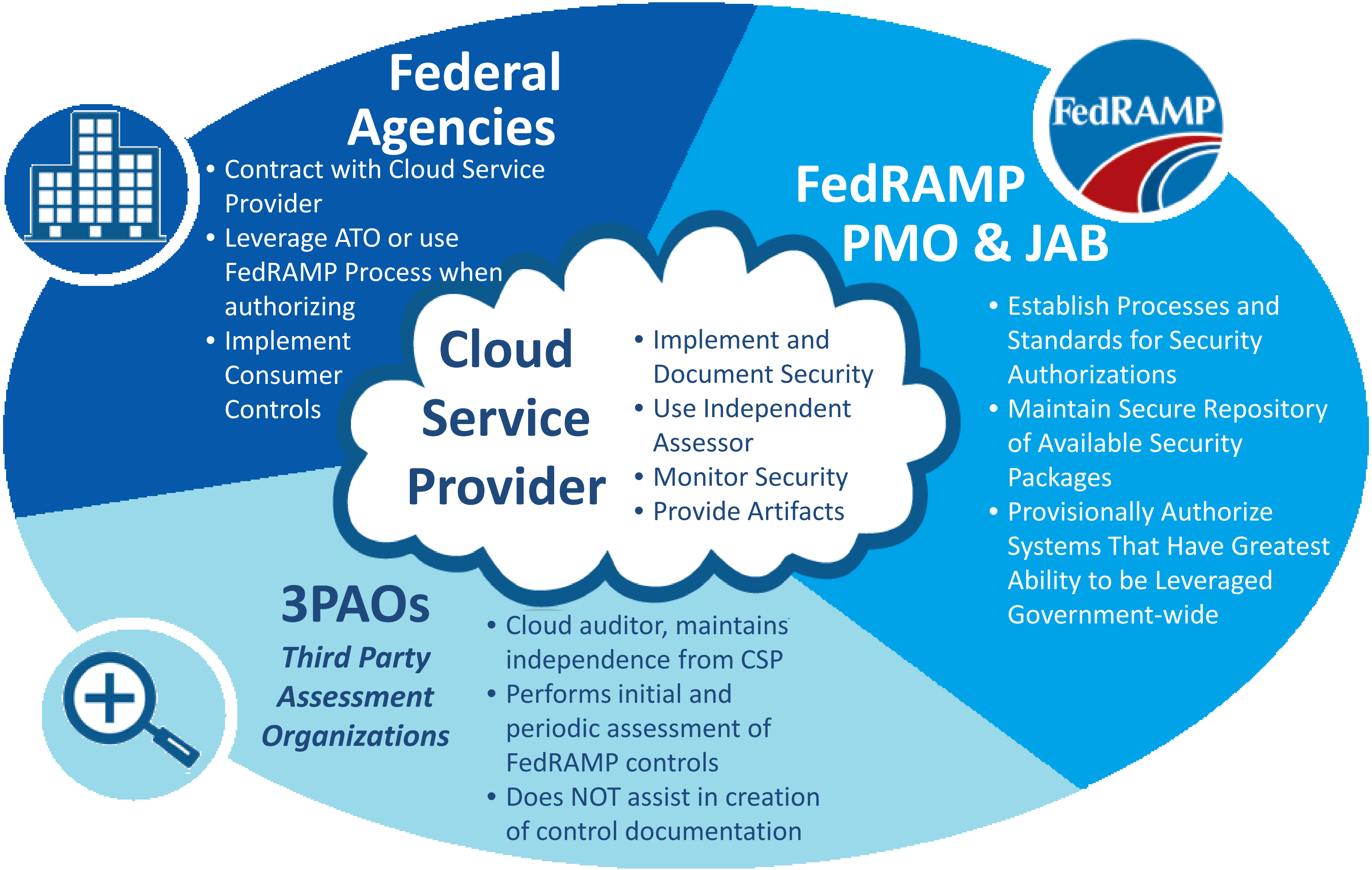
CSP

6. Monitor Security Controls
- Continuous Monitoring

FedRAMP Standardizes RMF for Cloud

NIST SP 800-37 Step	FedRAMP Standard
1. Categorize System	Low and Moderate Impact Levels
2. Select Controls	Control Baselines for Low and Moderate Impact Levels
3. Implement Security Controls	Document control implementations using the FedRAMP templates Implementation Guidance in “Guide to Understanding FedRAMP”
4. Assess the Security Controls	FedRAMP accredits 3PAOs 3PAOs use standard process, templates
5. Authorize the System	Joint Authorization Board or Agency AO authorize the system that can be leveraged due to increased trust
6. Continuous Monitoring	CSPs conduct monitoring in accordance with Continuous Monitoring Strategy and Guide

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

What is Driving Agencies to the Cloud?

Cloud First Policy

- Agencies must default to cloud based products and services when spending any new money on IT
  - New services, recompetes, additional services
- Agencies must justify to OMB when a cloud provider is NOT selected

When a cloud service provider is selected, FedRAMP governs the security authorization process.

Cloud Definition

- FedRAMP is not arbiter of what is and what is not cloud.
- We will authorize anything that is “cloud” esque
- If any agency submits a FedRAMP package for a system they deem cloud, FedRAMP will review that system as cloud – we will not interfere with or negate an agency determination of cloud.

Vendor Abilities to Meet Federal Requirements

Many cloud vendors are new to FISMA and it takes time to meeting Federal Requirements

- Clearly Defined Boundaries
- FIPS 140-2 Encryption
- Authenticated Scans
- Remediation of Vulnerabilities
- Multi-Factor Authentication

Delays in Authorizations

FedRAMP is a rigorous process, with increased scrutiny on meeting security requirements

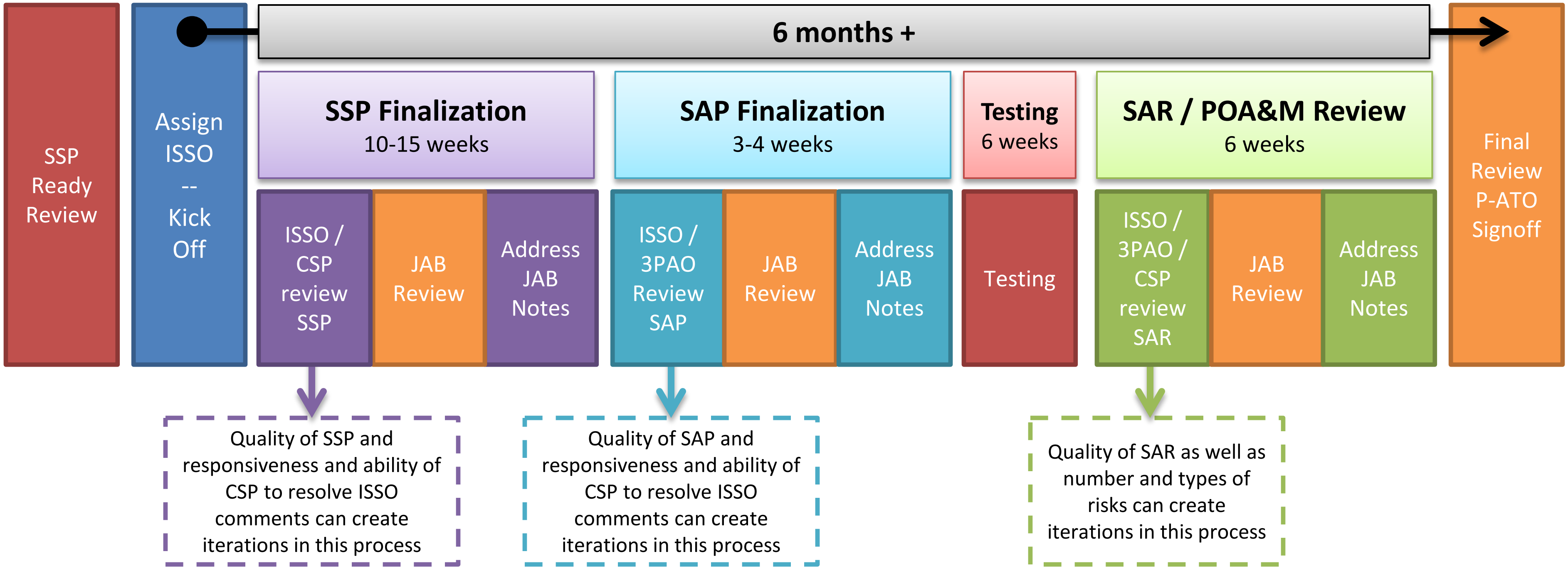
- Currently 4 JAB provisional ATO's: CGI Federal, Autonomic Resources, Lockheed Martin, HP
- Currently 2 Agency ATOs: Amazon's US East/West, and Amazon's GovCloud

- FISMA process takes time
- Difference between efficient and expedient
- Transparency
- New process for many vendors
- Updated CONOPs and standardization of timelines

- AGENCY ATO'S AND JAB PROVISIONAL ATO'S

FedRAMP Provisional Authorization

Timeframe Overview



SSP Ready Review

Assign ISSO -- Kick Off

6 months +

SSP Finalization 10-15 weeks

ISSO / CSP review SSP

JAB Review

Address JAB Notes

Quality of SSP and responsiveness and ability of CSP to resolve ISSO comments can create iterations in this process

SAP Finalization 3-4 weeks

ISSO / 3PAO Review SAP

JAB Review

Address JAB Notes

Quality of SAP and responsiveness and ability of CSP to resolve ISSO comments can create iterations in this process

Testing 6 weeks

Testing

SAR / POA&M Review 6 weeks

ISSO / 3PAO / CSP review SAR

JAB Review

Address JAB Notes

Quality of SAR as well as number and types of risks can create iterations in this process

Final Review P-ATO Signoff

Key

- 🟥 CSP Action
- FedRAMP Action
- FedRAMP / CSP Action
- 🟧 FedRAMP JAB Action
- FedRAMP / 3PAO Action
- 🟩 FedRAMP / 3PAO / CSP Action

JAB Provisional ATO vs Agency ATO

Timeframe

- JAB 25+ weeks minimum
- Agency 14+ weeks minimum

Level / Depth of Review

- JAB: Four sets of eyes (PMO, DoD, DHS, GSA)
- Agency: One set of eyes (agency)

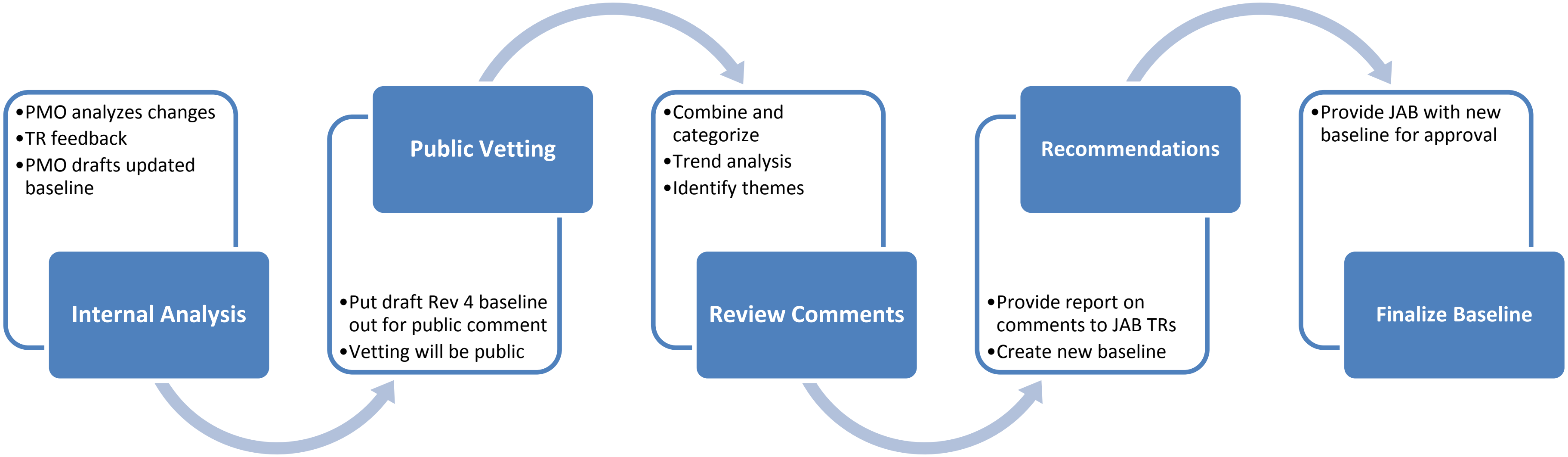
Risk Acceptance Level

- JAB: Low risk tolerance level, security for security
- Agency: Varying levels of risk acceptance, business needs can justify more risk as can individual agency policies

Continuous Monitoring

- JAB: JAB will maintain, agencies need to review
- Agency: Agency must work with CSP to complete

Baseline Controls: NIST 800-53 rev4 Updates



Internal Analysis

- PMO analyzes changes
- TR feedback
- PMO drafts updated baseline

Public Vetting

- Put draft Rev 4 baseline out for public comment
- Vetting will be public

Review Comments

- Combine and categorize
- Trend analysis
- Identify themes

Recommendations

- Provide report on comments to JAB TRs
- Create new baseline

Finalize Baseline

- Provide JAB with new baseline for approval

Impact of Revision 4 on FedRAMP Baseline

Description	Controls
No Change	65
Insignificant Change	36
Significant Change	156
New	40
Total	297

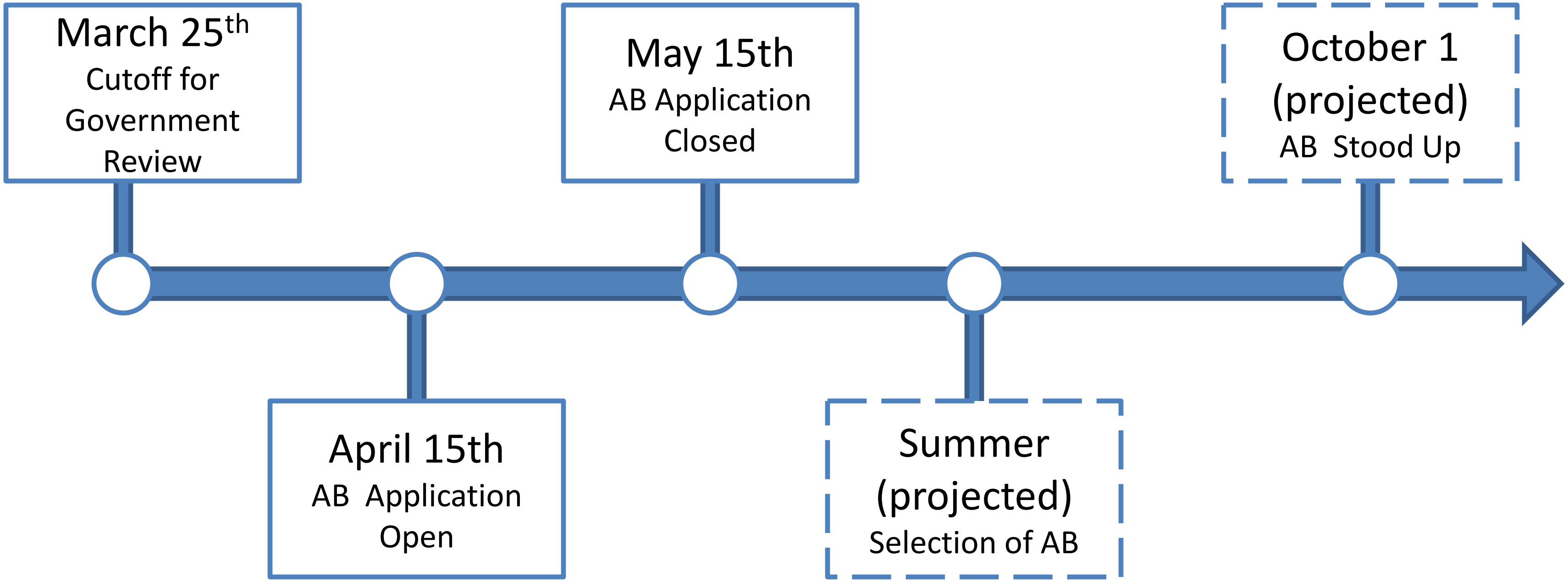
- Controls have been combined, removed, clarified, scope expanded, additional guidance given, etc.
- Management, Operational, Technical labels removed.
- Privacy controls added in appendix J

3PAO Privatization

3PAO Privatization is designed to keep rigor of 3PAO program and free government resources

- Same process that was done for Health IT, NAVLAP, UL, etc.
- FedRAMP will maintain ownership of accreditation list and is final source of accreditation decision
- Privatization is for accreditation reviews of applicants ONLY
- Privatization will also allow for increased surveillance post accreditation

Privatization Timeframe



March 25th
Cutoff for Government Review

April 15th
AB Application Open

May 15th
AB Application Closed

Summer (projected)
Selection of AB

October 1 (projected)
AB Stood Up

Tentative Timeline for 3PAO Privatization

- Currently reviewing AB applications
- We are evaluating all possibilities and approaches for transition of currently accredited 3PAOs to privatized accreditation review
- CSPs and Federal agencies will not be impacted due to privatization efforts – SARs will be accepted from anyone who is on the accredited list

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

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

Follow us on twitter @ FederalCloud