Federal Risk and Authorization Management Program (FedRAMP)

Concept of Operations Press Briefing

February 8, 2012

GSA

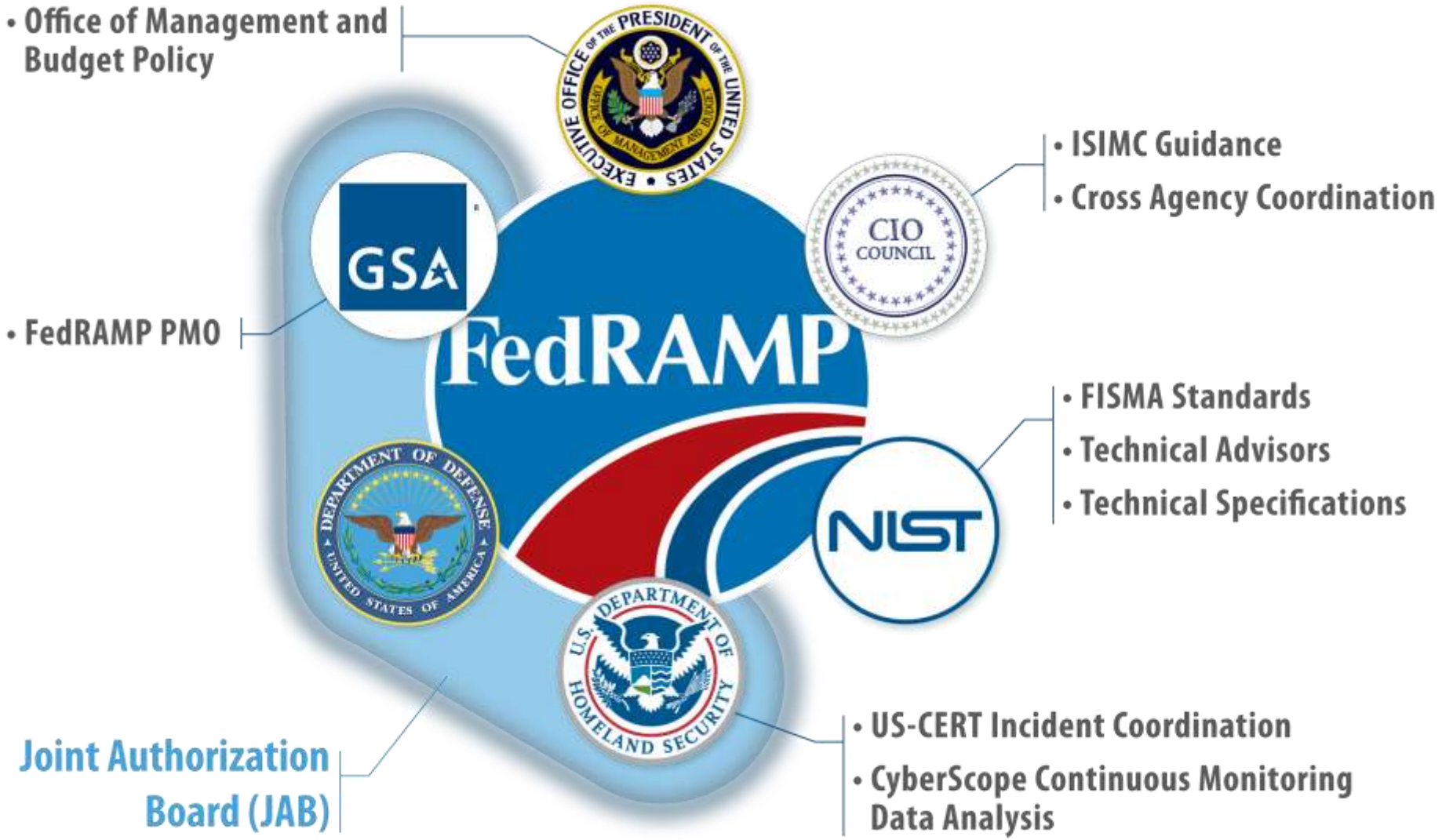
FedRAMP℠

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.

Executive Sponsors



FedRAMP Phases and Timeline

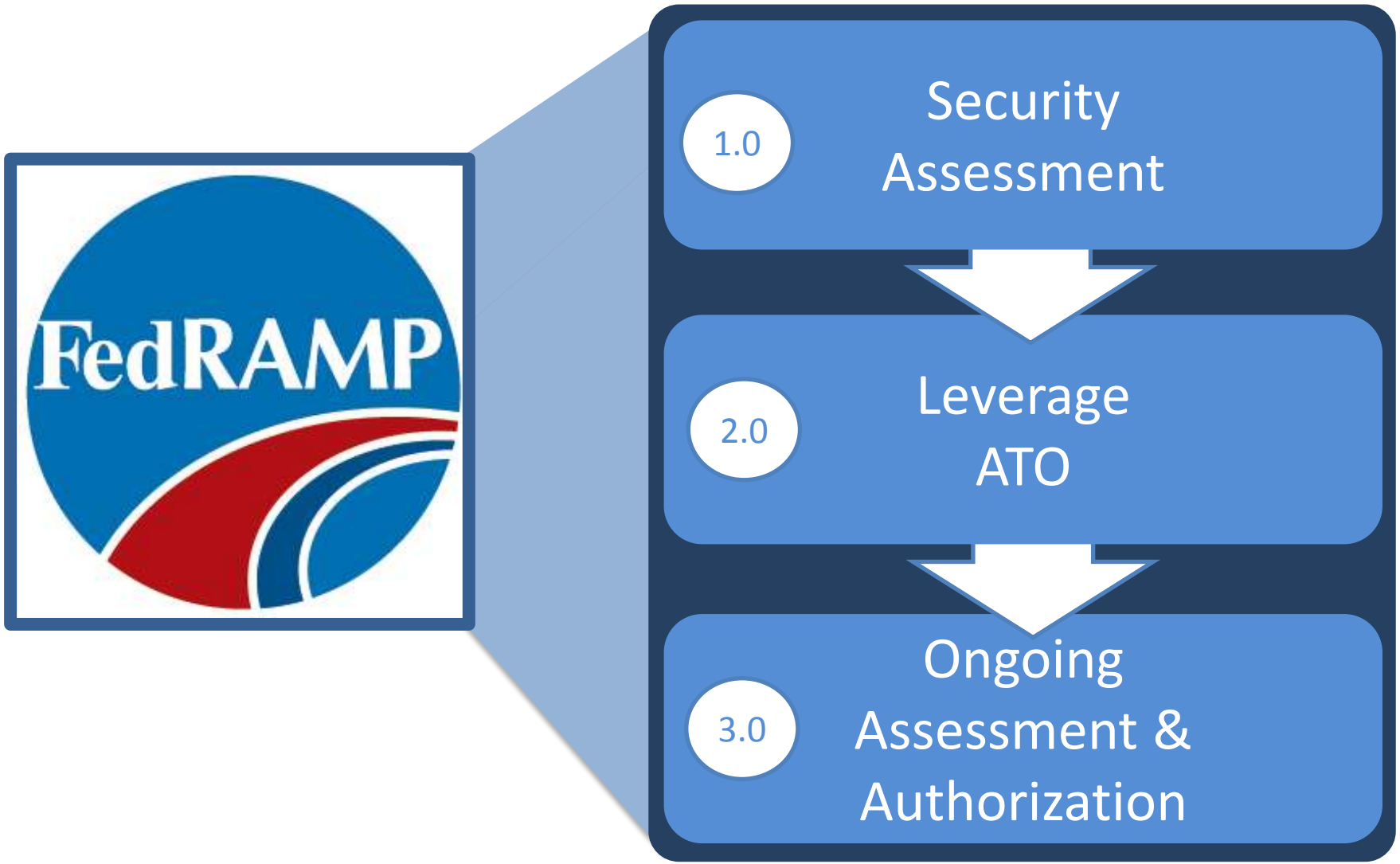
Phased evolution towards sustainable operations allows for the management of risks, capture of lessons learned, and incremental rollout of capabilities

	FY12	FY12	FY13 Q2	FY14
	Pre-Launch Activities	**Initial Operational Capabilities (IOC)**	**Full Operations**	**Sustaining Operations**
	Finalize Requirements and Documentation in Preparation of Launch	*Launch IOC with Limited Scope and Cloud Service Provider (CSP)s*	*Execute Full Operational Capabilities with Manual Processes*	*Move to Full Implementation with On-Demand Scalability*
Key Activities	• Publish FedRAMP Requirements (Security Controls, Templates, Guidance) • Publish Agency Compliance Guidance • Accredit 3PAOs • Establish Priority Queue	• Authorize CSPs • Update CONOPS, Continuous Monitoring Requirements and CSP Guidance	• Conduct Assessments & Authorizations • Scale Operations to Authorize More CSPs	• Implement Electronic Authorization Repository • Scale to Steady State Operations
		Gather Feedback and Incorporate Lessons Learned		
Outcomes	• Initial List of Accredited 3PAOs • Launch FedRAMP into Initial Operating Capabilities	• Initial CSP Authorizations • Established Performance Benchmark	• Multiple CSP Authorizations • Defined Business Model • Measure Benchmarks	• Authorizations Scale by Demand • Implement Business Model • Self-Sustaining Funding Model Covering Operations • Privatized Accreditation Board

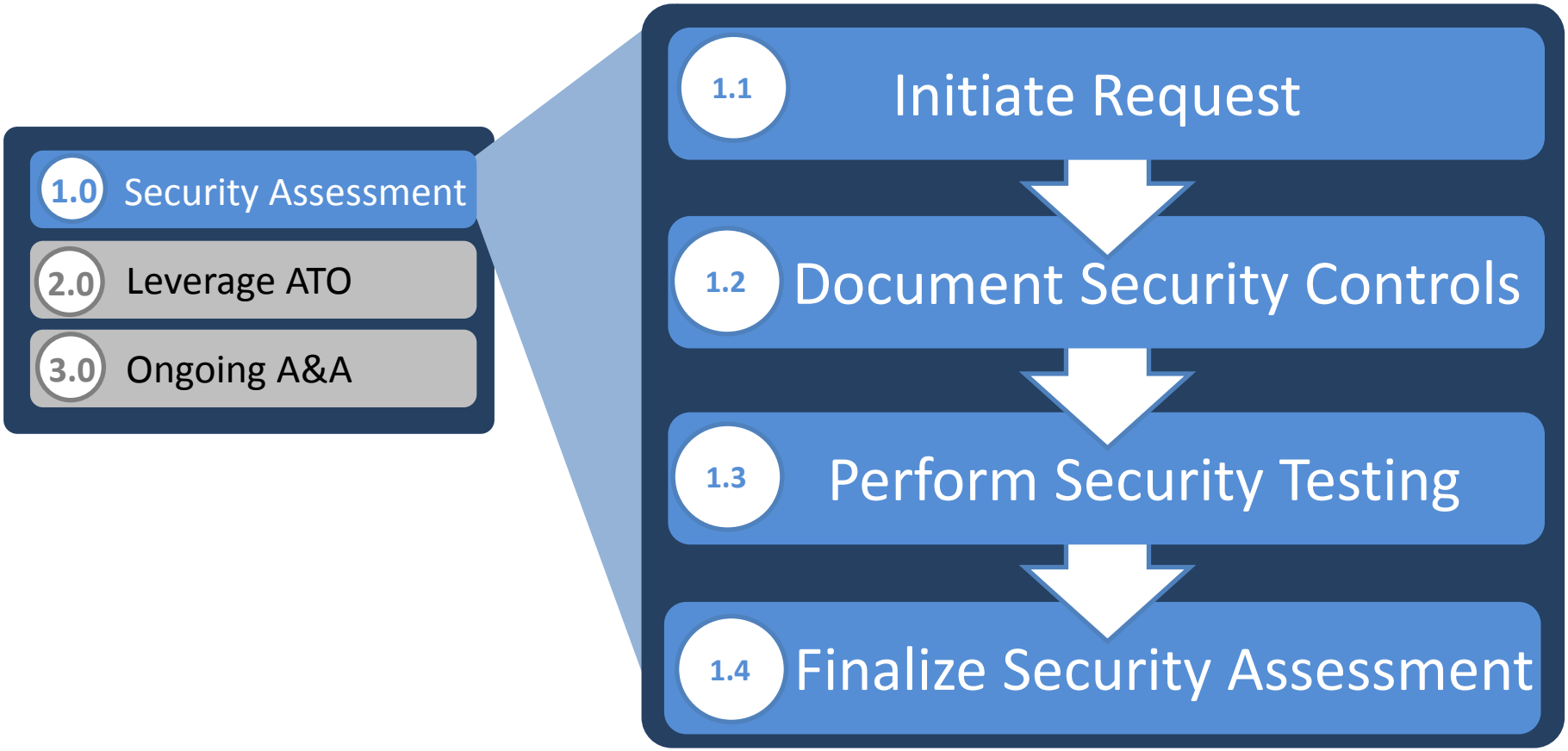
FedRAMP Pre-Launch Activities

- [x] Policy Memo
- [x] FedRAMP Baseline Security Controls
- [x] 3PAO Accreditation
- [x] FedRAMP.gov
- [ ] FedRAMP CONOPS
- [ ] Publish Agency Compliance Guidance
- [ ] Accredit 3PAOs
- [ ] JAB Charter
- [ ] Initial Operating Capability (IOC)

FedRAMP CONOPS: Process Areas



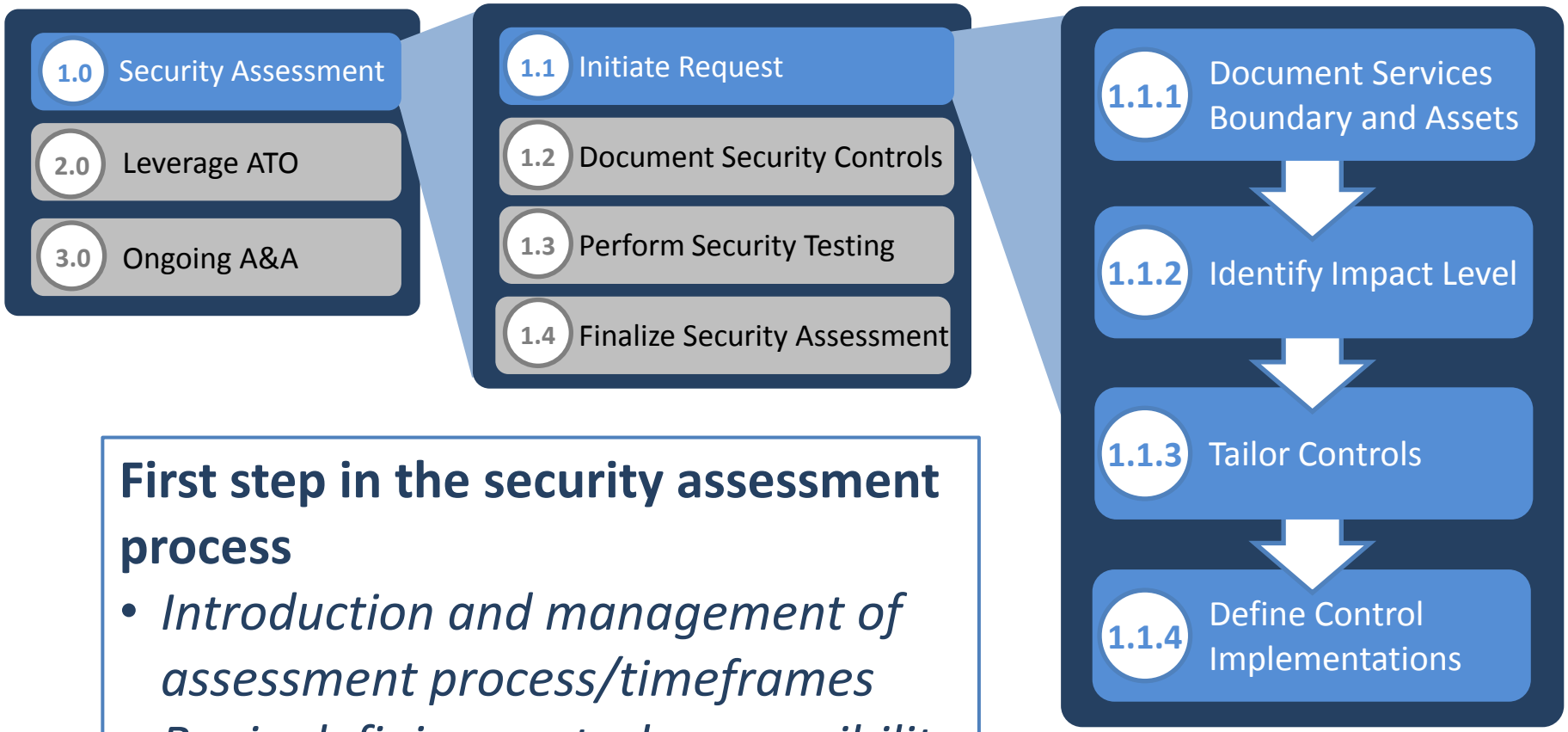
FedRAMP CONOPS: Security Assessment Process



Security Assessment Process aligns with NIST 800-37

FedRAMP CONOPS: Security Assessment Process

Initiate Request



First step in the security assessment process

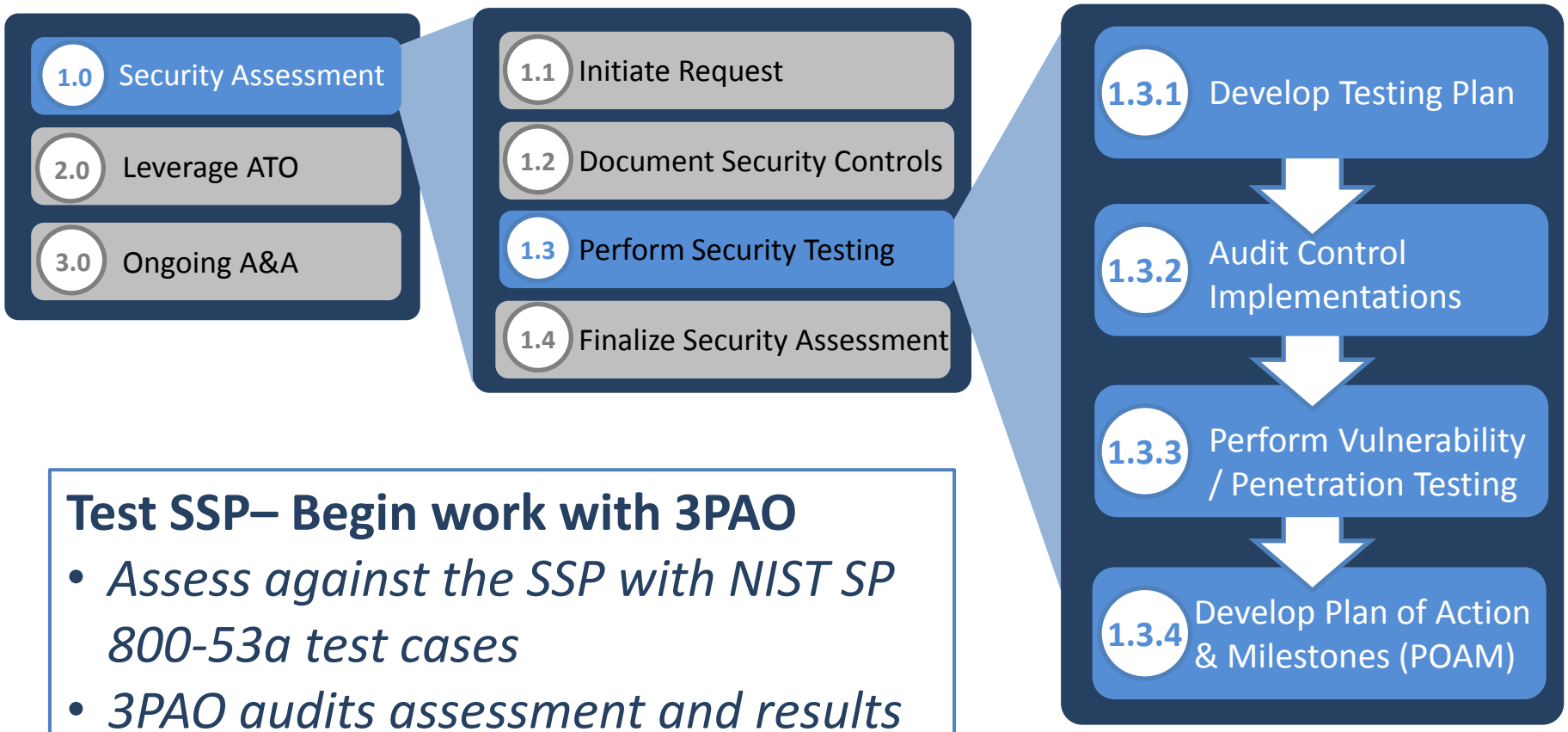
- *Introduction and management of assessment process/timeframes*
- *Begin defining control responsibility*
- *Identify any alternate implementations of controls*

FedRAMP CONOPS: Security Assessment Process
Document Security Controls

Document the System Security Plan (SSP)

- *Address how the CSP implements each FedRAMP security control*
  - *Control responsibility*
  - *What solution is being used for the control*
  - *How the solution meets the control requirement*

FedRAMP CONOPS: Security Assessment Process
Perform Security Testing

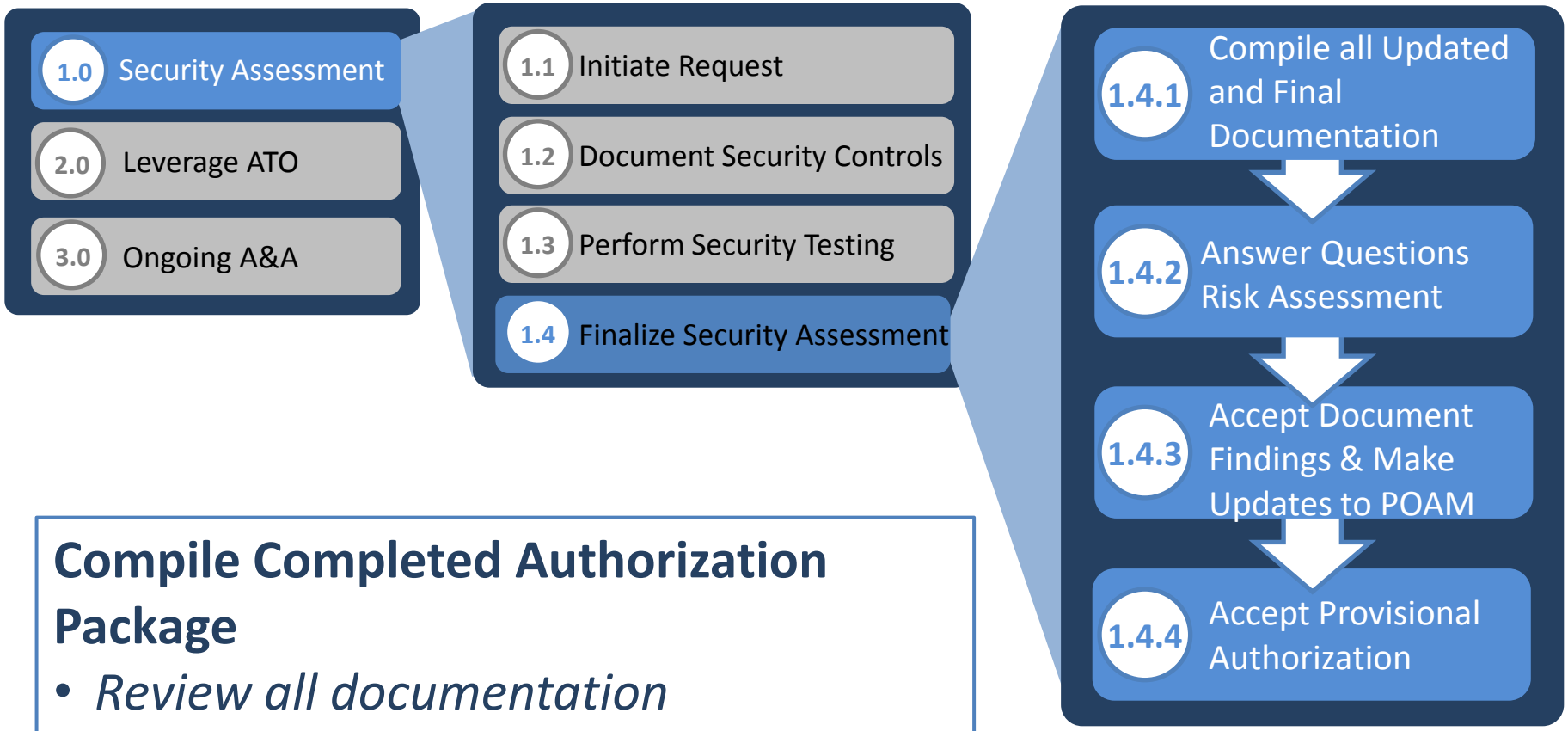


Test SSP– Begin work with 3PAO

- *Assess against the SSP with NIST SP 800-53a test cases*
- *3PAO audits assessment and results*
- *3PAO generates security assessment report*

FedRAMP CONOPS: Security Assessment Process

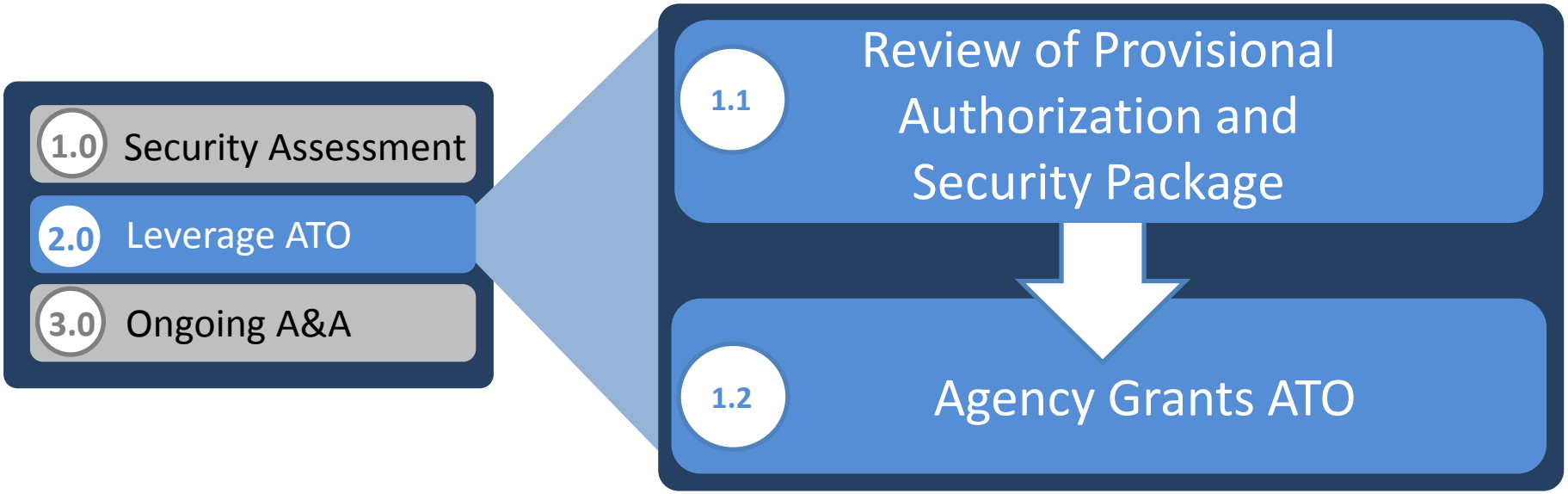
Finalize Security Assessment



Compile Completed Authorization Package

- *Review all documentation*
- *Review risk posture of CSP system*
- *Grant / deny provisional authorization*

FedRAMP CONOPS: Leverage ATO Process



Federal Agencies Leverage ATO's from the FedRAMP Repository

Leverage ATO: FedRAMP Repository

FedRAMP will maintain a repository of standardized security assessment packages Federal Agencies can leverage to make their own risk-based decisions to grant an Authority to Operate for a cloud solution for their Agency.

This repository is key to the "do once, use many times" approach.

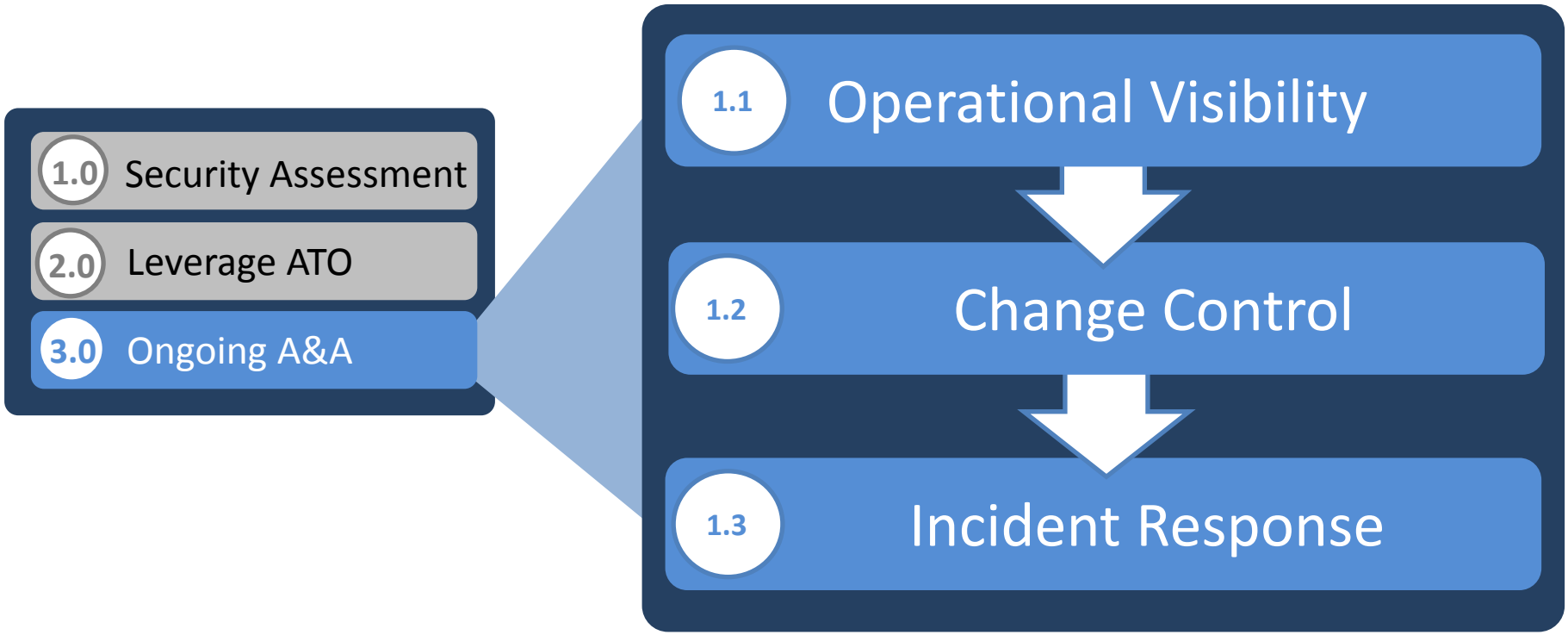
Per OMB policy memo, all assessment packages must use the FedRAMP security requirements – which includes the FedRAMP baseline set of controls as well as all FedRAMP templates

Category	FedRAMP 3PAO	ATO Status
JAB Provisional ATO	✓	n/a
Agency ATO with FedRAMP 3PAO	✓	Agency
Agency ATO**	✗	Agency
CSP Supplied	✓	JAB (+Agency)

Level of Gov't Review

*** A&A packages without a FedRAMP 3PAO do not meet the independence requirements created by the JAB and are not eligible for JAB review*

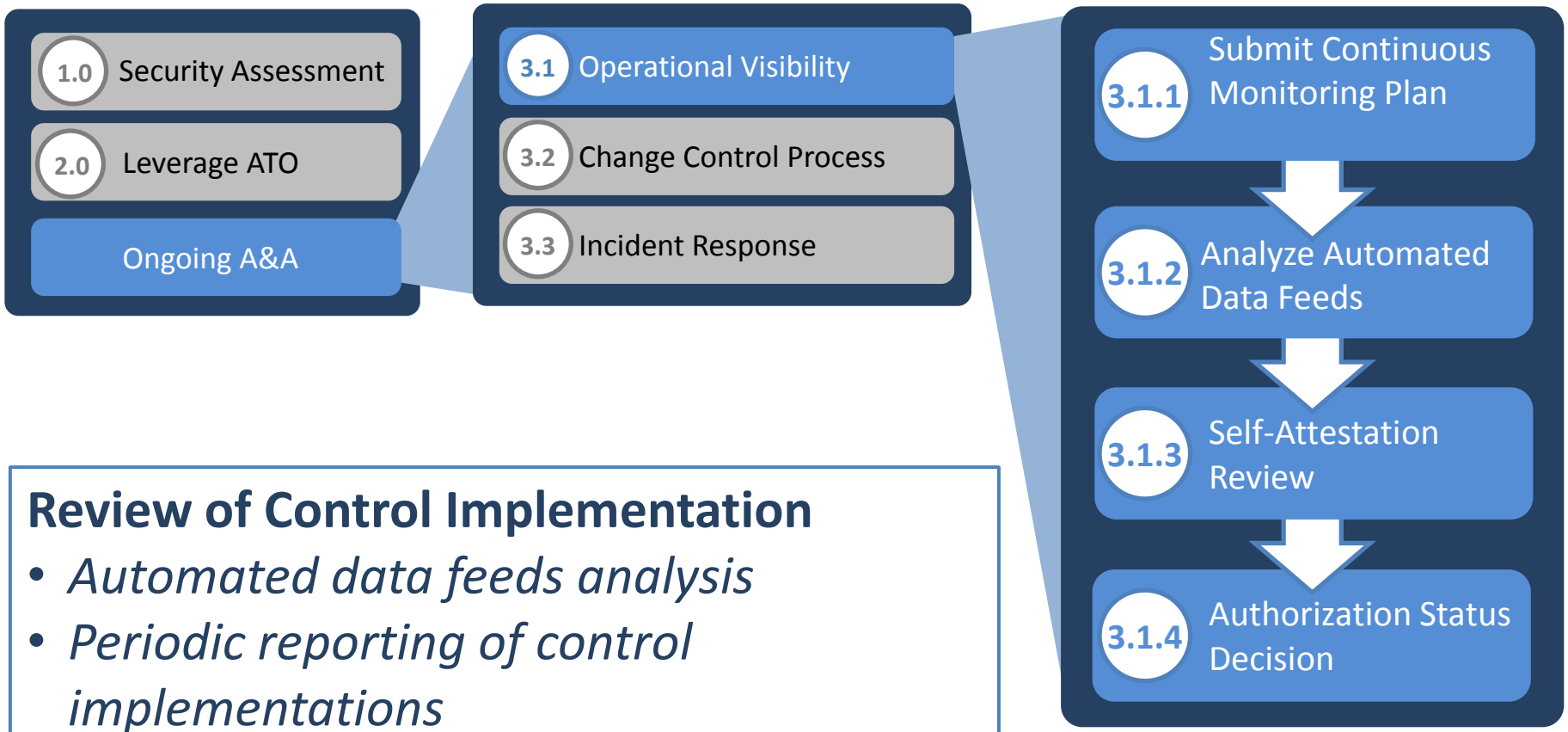
FedRAMP CONOPS: Ongoing Assessment & Authorization (Continuous Monitoring)



Security Assessment Process aligns with NIST 800-137

Shift from compliance based decision to risk management framework

FedRAMP CONOPS: Ongoing A&A Process
Operational Visibility



Review of Control Implementation

- *Automated data feeds analysis*
- *Periodic reporting of control implementations*
- *Review of CSP's annual self attestation and Supplier's Declaration of Conformity*

FedRAMP CONOPS: Ongoing A&A Process
Change Control Process

Review of Changes to CSP System

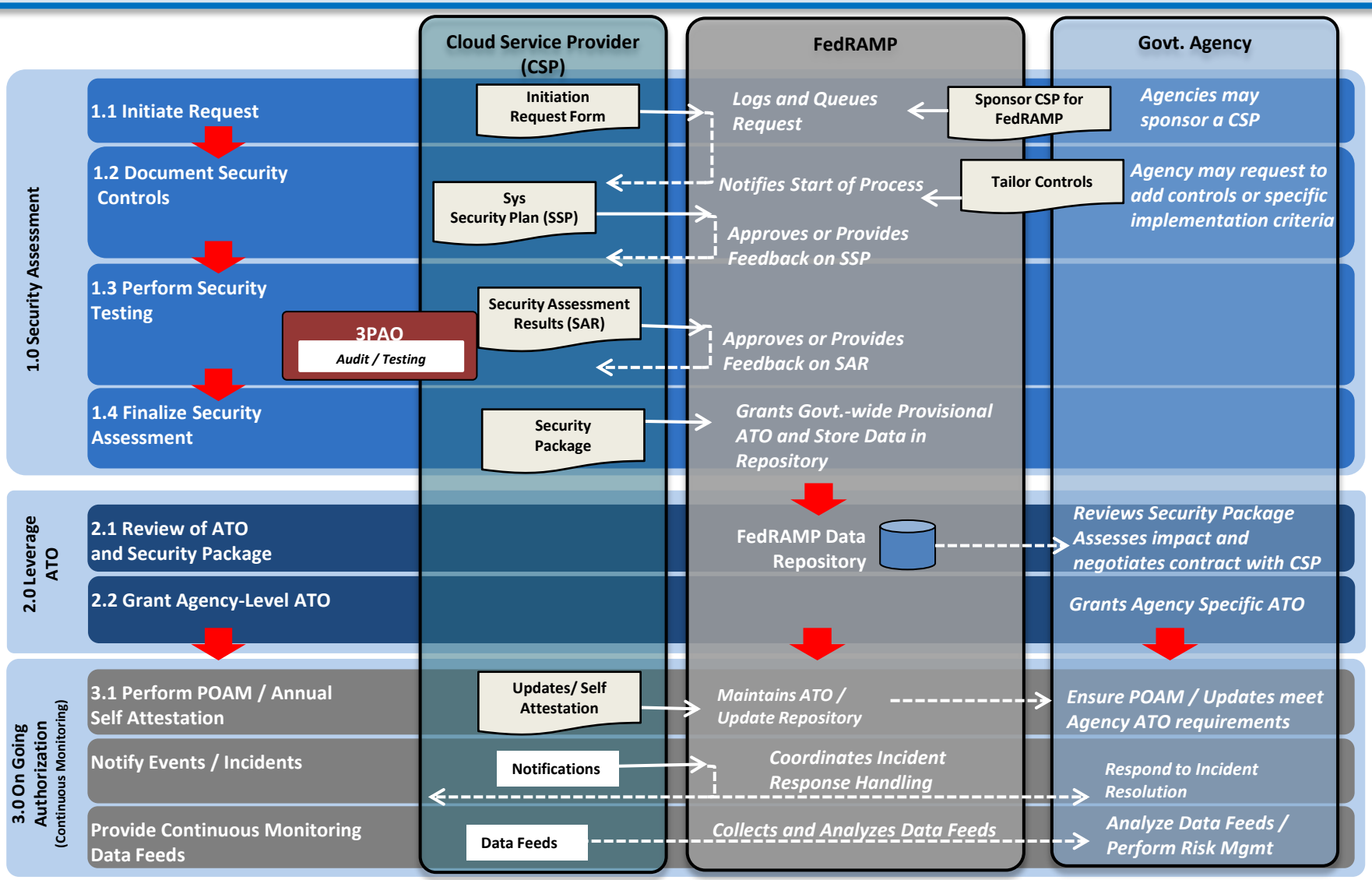
- *Monitoring of POAMs*
- *Review of changes to CSP system in accordance with CSP configuration management plan*

FedRAMP CONOPS: Ongoing A&A Process
Incident Response

Monitoring of Incidents and New Vulnerabilities

- *Coordination with US-CERT and Agency Security Operations Centers*
- *Coordination of remediation and mitigation activities across Agencies*

FedRAMP Concept of Operations – Overview



GSA

For more information, please contact us or visit us at any of the following websites:

http://FedRAMP.gov
http://gsa.gov/FedRAMP
Follow us on twitter @ FederalCloud

Background Slides

FedRAMP Policy Memo

December 8, 2011 OMB Policy Memo

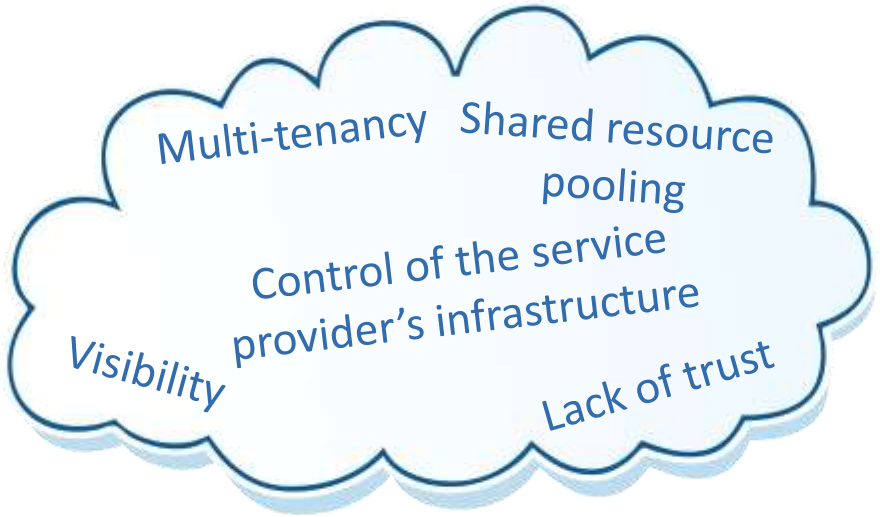
- Establishes Federal policy for the protection of Federal information in cloud services
- Describes the key components of FedRAMP and its operational capabilities
- Defines Executive department and agency responsibilities in developing, implementing, operating and maintaining FedRAMP
- Defines the requirements for Executive departments and agencies using FedRAMP in the acquisition of cloud services

FedRAMP Baseline Security Controls

Controls are selected from the NIST SP 800-53 R3 catalog of controls for low and moderate impact systems

Impact level	NIST Baseline Controls	Additional FedRAMP Controls	Total Controls Agreed to By JAB for FedRAMP
Low	115	1	116
Moderate	252	45	297

Additional FedRAMP controls selected to address unique elements of cloud computing



FedRAMP Security Controls Baseline Available on FedRAMP.gov

FedRAMP 3PAO Accreditation

FedRAMP requires CSPs to use Third Party Assessment Organizations (3PAOs) to independently validate and verify that they meet FedRAMP security requirements

Conformity assessment process to accredit 3PAOs based on NIST program

(1) Independence and quality management in accordance with ISO standards; and

(2) Technical competence through FISMA knowledge testing.

Benefits of leveraging a formal 3PAO approval process:

- **Consistency in performing security assessments**
- **Ensures 3PAO independence from Cloud Service Providers**
- **Establishes an approved list of 3PAOs for CSPs and Agencies to use**

Projected Date for initial list is mid-April 2012. Rolling accreditation afterwards.

FedRAMP.gov

The Authoritative Source for Information and Documentation on FedRAMP

- All content and documentation need by 3PAOs, CSPs, and interested agencies
- Contact and feedback mechanisms
- Frequently Asked Questions (FAQ) received from website, Industry & Agency Days, and other sources
- Will continue to grow and evolve with FedRAMP program