
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

WPS201-R

Dive deep on the FedRAMP authorization process

Brad Dispensa

Pr. Security and Compliance Specialist
AWS

Ted Steffan

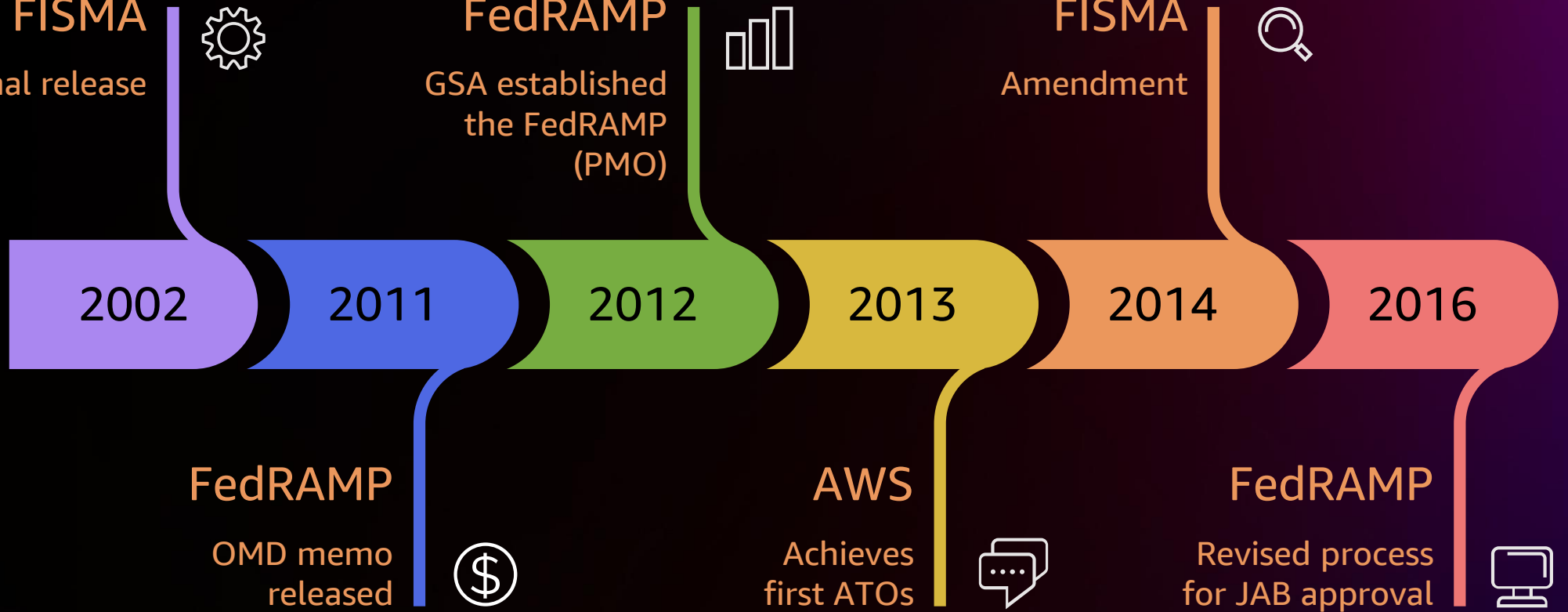
Head of Federal Compliance Acceleration
AWS

Session agenda

- Overview of FedRAMP and the process of getting your authorization
  - What is FedRAMP and how does it work?
  - Do I need Low, Moderate, or High?
- Hands-on table top of getting a company through the ATO process
  - Simulated table top exercise to help you walk through an actual process

FedRAMP/FISMA history

FedRAMP



FedRAMP

Federal Risk and Authorization Management Program (FedRAMP)

- US government program that provides a standard approach for security assessments authorization and continuous monitoring for cloud services
- PMO established by GSA in June of 2012
- Mission: To promote the adoption of secure cloud services
- Joint Authorization Board (JAB): Governance and decision-making body for FedRAMP
  - Made up of: CIOs from the DHS, GSA, and DoD
- Any cloud provider that holds federal data must be FedRAMP authorized
- Based on NIST SP 800-53 controls

3PAO – Third-party assessment organization

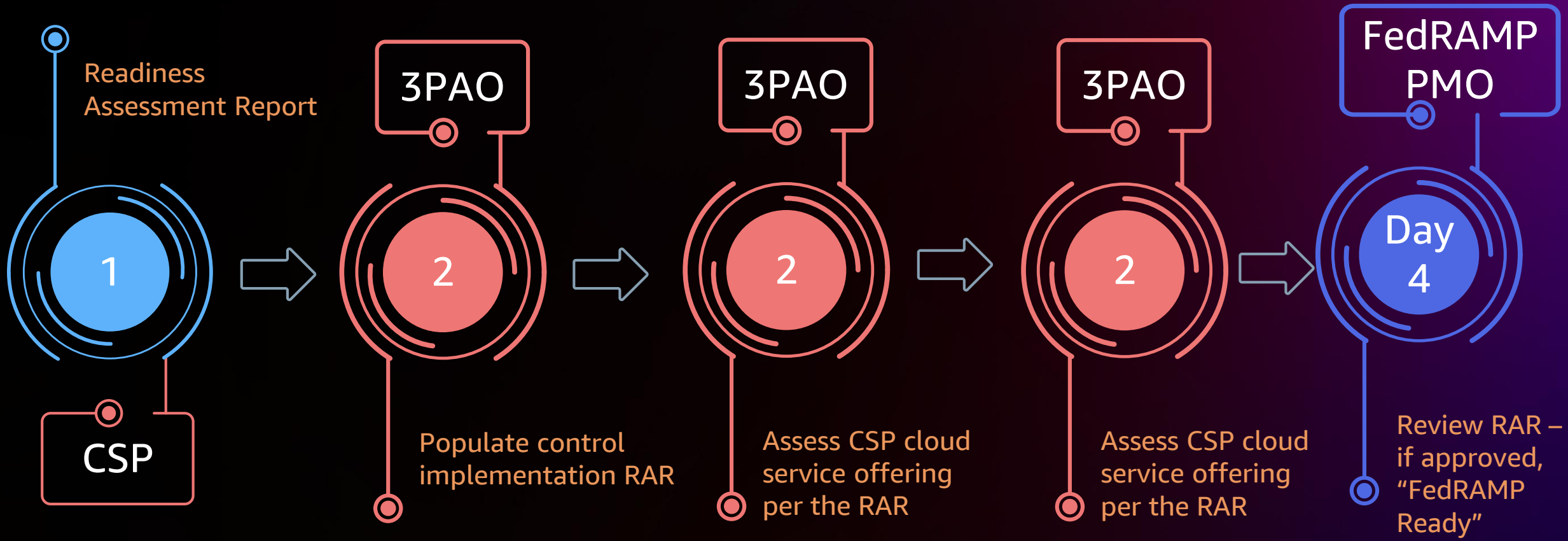
- An organization that has been certified to help CSPs and government agencies meet FedRAMP compliance regulations
- A 3PAO evaluates a CSP's systems to ensure transparency between government and CSP and consistency in data security strategies
- Certified 3PAOs use FedRAMP processes when performing security assessments
- GSA provides the following requirements for qualification as a 3PAO
  - Independence and quality management in accordance with ISO/IEC 17020:1998 standards
  - Information assurance competence that includes experience with FISMA and testing security controls
  - Competence in the security assessment of cloud-based information systems

FedRAMP Marketplace

FedRAMP Marketplace provides a searchable database of cloud service offerings that have achieved one of the following designations

- FedRAMP Ready
  - Indicates that a 3PAO attests to a CSO's security capabilities, a Readiness assessment report (RAR) has been reviewed and deemed acceptable by the FedRAMP PMO, and the CSP is highly likely to achieve FedRAMP Authorized designation
- FedRAMP In Process
  - Indicates a CSP/CSO is actively working towards FedRAMP authorization through the JAB or Agency authorization process, and is listed on the FedRAMP Marketplace
- FedRAMP Authorized
  - Provided to CSPs/CSOs that have successfully completed the FedRAMP authorization process with the JAB or a federal agency; FedRAMP Authorized indicates FedRAMP requirements have been met, and that a CSO's security package is available for agency reuse

Achieving FedRAMP Ready ((p)-ATO)



FedRAMP In Process

Indicates a CSP is actively working toward FedRAMP authorization through the JAB or Agency authorization process and is listed in the FedRAMP Marketplace

Prior to being listed as FedRAMP In Process in the Marketplace a CSP must

- Achieve FedRAMP Ready within 60 days of being prioritized by the JAB
- Finalize the CSO's System Security Plan (SSP)
- Engage a FedRAMP recognized 3PAO to develop a Security Assessment Plan (SAP), conduct a full security assessment, and produce a Security Assessment Report (SAR)
- Upload all required security package materials to MAX.gov for systems authorized at the Moderate baseline, or to their own repository if the system is authorized at the High baseline
- Participate in a formal kickoff meeting with the JAB, PMO, and partnering 3PAO

FedRAMP Authorized

Provided to CSOs that have successfully completed the FedRAMP authorization process with the JAB or a federal agency and indicates FedRAMP requirements have been met, and that a CSO’s security package is available for agency reuse

JAB Provisional Authorization

Cloud services that are FedRAMP In Process with the JAB can shift to FedRAMP Authorized

Agency Authorization

CSOs that are In Process with an agency can shift to FedRAMP Authorized

JAB provisional authorization

1. The JAB reviews the security package for the CSO

   CSPs and 3PAOs support JAB technical reviewers during their review, and participate in regular meetings with the PMO and JAB to address questions

2. The CSP submits accurate and complete monthly continuous monitoring (ConMon) deliverables such as scan files, Plan of Action & Milestones (POA&M), and up-to-date inventory to the JAB throughout the review

3. The CSP and 3PAO remediate system and documentation issues as needed following completion of the JAB review, ensuring all JAB comments are appropriately addressed

4. The JAB validates the CSP and 3PAO remediation efforts

5. The JAB issues a letter granting a P-ATO for the CSO to the CSP

   P-ATO letter is signed by the CIOs of the Department of Defense, the Department of Homeland Security, and the General Services Administration

Agency authorization

1. An agency grants an ATO for the CSO
2. CSP and 3PAO upload all security package materials to their secure FedRAMP repository (MAX.gov for packages authorized below the High baseline, their own repository for packages authorized at the High baseline)
3. The FedRAMP PMO reviews the package and releases an Agency Authorization Review Report

   If necessary, the FedRAMP PMO schedules a review meeting with the agency, CSP, and 3PAO to discuss questions and gain clarity on outstanding items reflected in the Agency Package Review Report

   Updates to the package may be requested by the FedRAMP PMO

How do I get a sponsor?

How do I know what level?

FedRAMP Connect

FedRAMP Ready

FedRAMP P-ATO

Choice of Impact

- Low impact SaaS
- Moderate
- High

IL4 versus IL5

Package prep

- System Security Plan (SSP) and engages an accredited 3PAO
- The 3PAO develops a Security Assessment Plan (SAP), conducts a full security assessment of the service offering, and produces a Security Assessment Report (SAR)
- The CSP develops a Plan of Action and Milestones (POA&M) to track and manage system security risks identified in the SAR

What are the rules?

NIST 800-53 (+ additional guidance)

		NIST 800-53 Security Controls Catalog Revision 4			FedRAMP Moderate Baseline			
Count	SORT ID	Family	ID	Control Name	NIST Control Description (From NIST SP 800-53r4 1/23/15)	Moderate FedRAMP-Defined Assignment / Selection Parameters (Numbering matches SSP)	M Additional FedRAMP Requirements and Guidance	Parameter
7	AC-02 (05)	ACCESS CONTROL	AC-2 (5)	ACCOUNT MANAGEMENT | INACTIVITY LOGOUT	The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out]. Supplemental Guidance: Related control: SC-23.		AC-2 (5) Guidance: Should use a shorter timeframe than AC-12.	

FIPS 199: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

FedRAMP baseline packages

https://www.fedramp.gov/baselines/

How does AWS Help?

GovCloud

Systems Manager conformance packs

ATO on AWS

CCGs

Artifacts

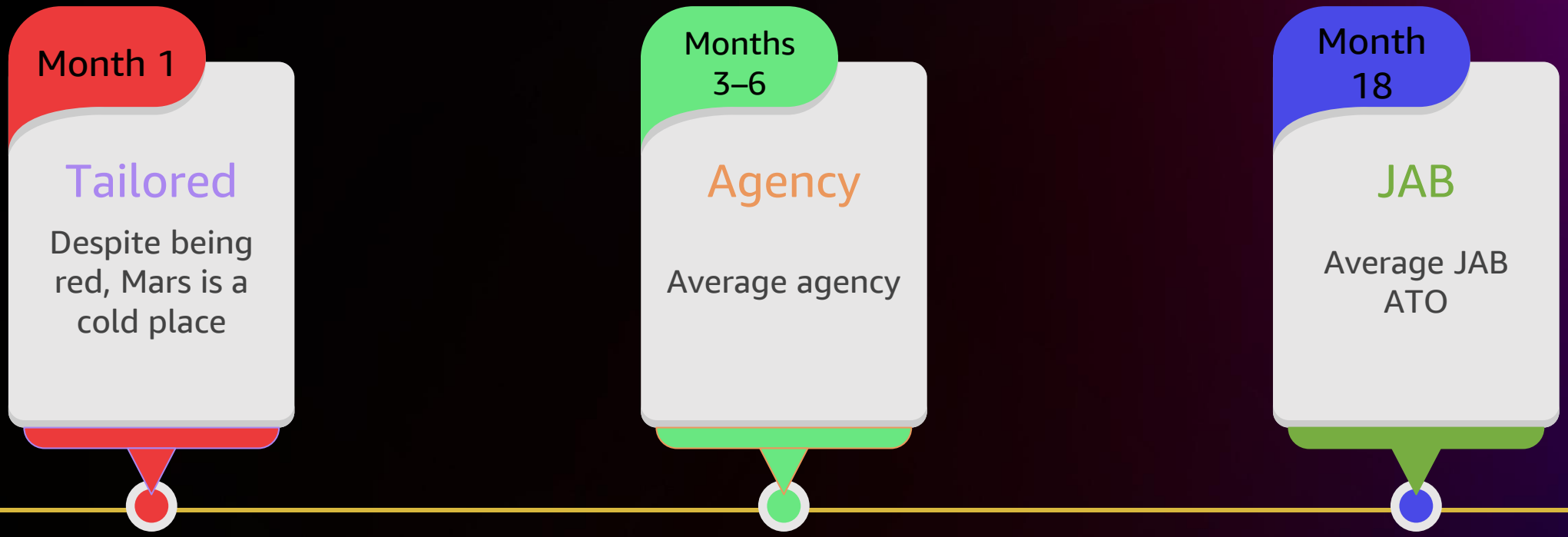
Caplinked ** .gov / .mil email

AWS Systems Manager

AWS Artifact

Caplinked™

Cost/time considerations



Avg. Cost
~$450k

Avg. Cost
$450k-$2M

Technical considerations

Let’s get hands on!

Thank you!

Please complete the session survey in the **mobile app**