FedRAMP

WHAT'S NEW AT FEDRAMP?

John Hamilton, Program Manager - Operations

December 2017

FedRAMP Overview

FEDRAMP: HISTORICAL CONTEXT & OVERVIEW

FedRAMP was created out of the Federal Cloud Computing Initiative to remove the barriers to the adoption of cloud.

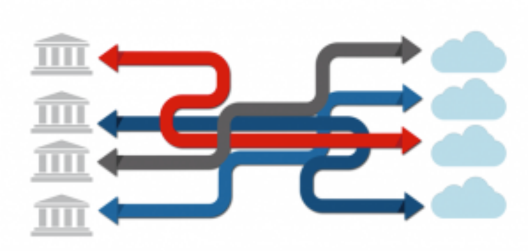
The #1 barrier Agencies identified was security.

Goals for FedRAMP

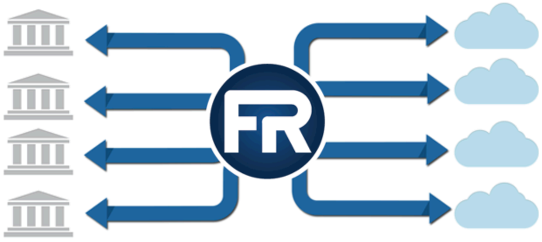
- Ensure the use of cloud services protects federal information
- Enable reuse across the federal government wherever possible to save money and time

FedRAMP provides a unified security framework (templates + control set) for how Agencies comply with FISMA for cloud technologies (SaaS, PaaS, IaaS) at the unclassified low, moderate, or high impact categories (FIPS 199).

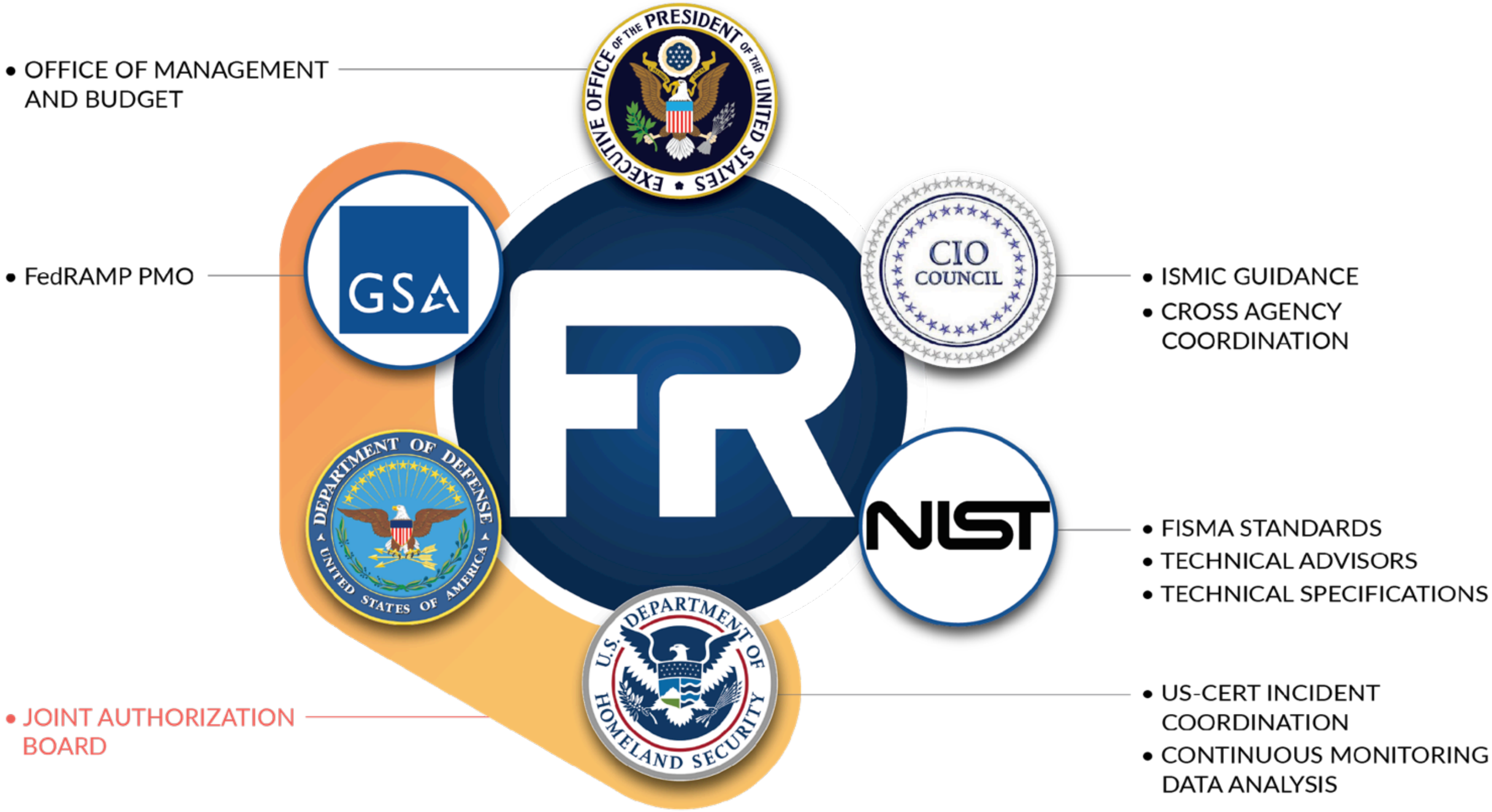
Before FedRAMP



With FedRAMP



FEDRAMP: GOVERNANCE



- OFFICE OF MANAGEMENT AND BUDGET
- FedRAMP PMO
- JOINT AUTHORIZATION BOARD

- ISMIC GUIDANCE
- CROSS AGENCY COORDINATION

- FISMA STANDARDS
- TECHNICAL ADVISORS
- TECHNICAL SPECIFICATIONS

- US-CERT INCIDENT COORDINATION
- CONTINUOUS MONITORING DATA ANALYSIS

FEDRAMP: STAKEHOLDERS

FedRAMP PMO

- Provide a unified process for all Agencies to follow
- Work with the JAB to prioritize vendors to achieve authorizations with an efficient review schedule
- Support CSPs and Agencies through the FedRAMP process
- Maintain secure repository of FedRAMP ATOs to enable reuse

AGENCIES

- Conduct quality risk assessments that can be reused
- Integrate the FedRAMP requirements into Agency specific policies/ procedures
- Deposit ATO documents in the FedRAMP secure repository

CSPs

- Submit quality documentation and testing in support of their FedRAMP application for the Cloud Service Offering (CSO)
- Encourage customers to reuse existing ATOs for their CSO

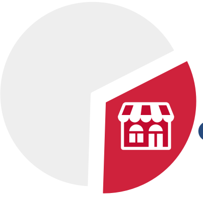
3PAOs

- Maintain independence as part of the quality assurance process
- Provide quality assessments

FEDRAMP
CONTINUES TO GROW THE MARKETPLACE

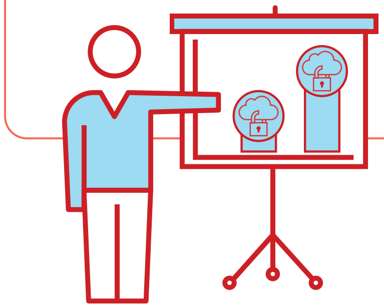
The program has been in existence for **5 years**

We currently have **91** authorized Cloud Service Providers



Of those that are authorized **31%** are **small business**

We have **DOUBLED** the number of cloud providers and authorizations each year since launch



113
Agencies authorizing a FedRAMP service

165
Cloud Service Providers pursuing or have achieved an authorization

45
Accredited **Auditors**

FEDRAMP IMPACTS

FEDRAMP HAS ENABLED GOVERNMENT TO AVOID >$138 MILLION IN COSTS

91 systems X **554** reuses @ **$250,000** per reuse = **>$138 MILLION** in cost avoidance

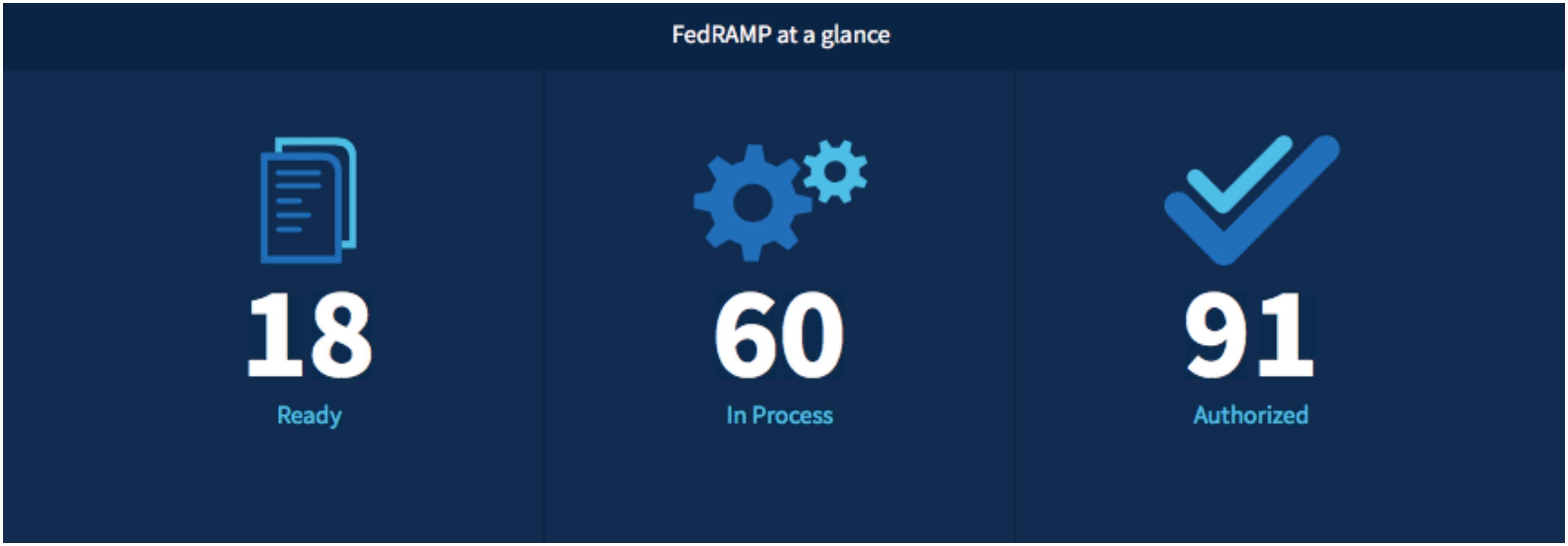
246% return on investment

One large provider has over **1 million assets**

Another covers almost **1/3 of the world's internet traffic**

FedRAMP Designations & The FedRAMP Authorization Process

FEDRAMP DESIGNATIONS



FedRAMP at a glance

18

Ready

60

In Process

91

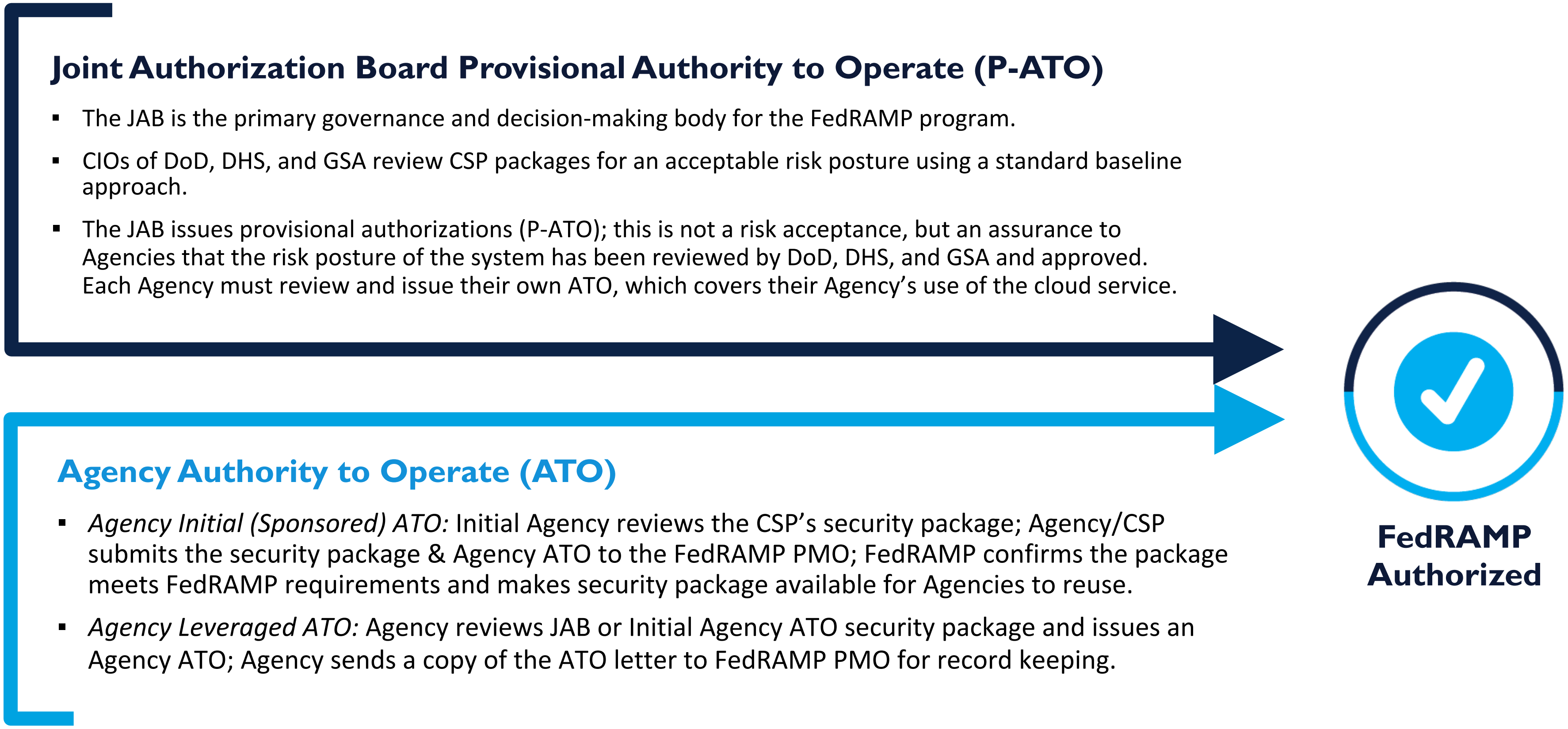
Authorized

There are three “official” FedRAMP designations: FedRAMP Ready, FedRAMP In Process, and FedRAMP Authorized. The FedRAMP PMO is the only entity that can classify CSOs as one of these three titles.

A listing of all CSOs that have achieved FedRAMP status can be found at https://marketplace.fedramp.gov/

FEDRAMP DESIGNATIONS: AUTHORIZED

There are two paths to an authorization: through the JAB or an Agency.



Joint Authorization Board Provisional Authority to Operate (P-ATO)

- The JAB is the primary governance and decision-making body for the FedRAMP program.
- CIOs of DoD, DHS, and GSA review CSP packages for an acceptable risk posture using a standard baseline approach.
- The JAB issues provisional authorizations (P-ATO); this is not a risk acceptance, but an assurance to Agencies that the risk posture of the system has been reviewed by DoD, DHS, and GSA and approved. Each Agency must review and issue their own ATO, which covers their Agency's use of the cloud service.

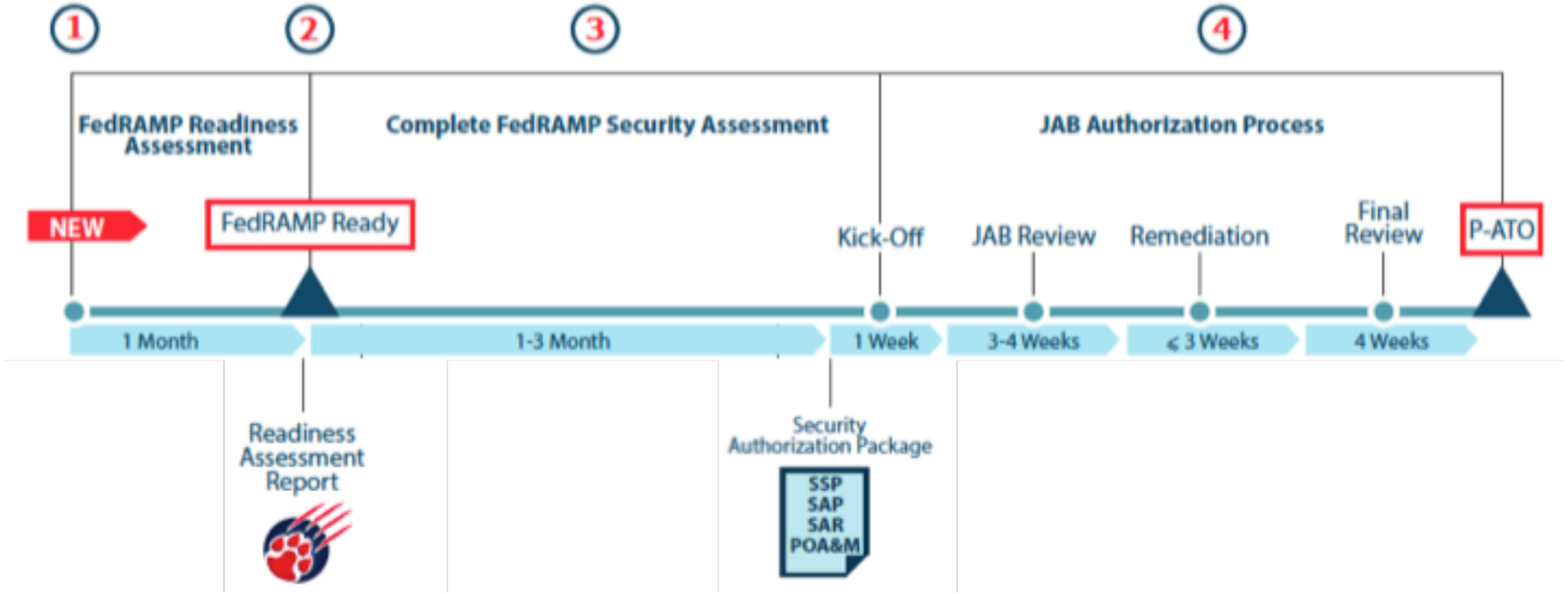
Agency Authority to Operate (ATO)

- *Agency Initial (Sponsored) ATO:* Initial Agency reviews the CSP's security package; Agency/CSP submits the security package & Agency ATO to the FedRAMP PMO; FedRAMP confirms the package meets FedRAMP requirements and makes security package available for Agencies to reuse.
- *Agency Leveraged ATO:* Agency reviews JAB or Initial Agency ATO security package and issues an Agency ATO; Agency sends a copy of the ATO letter to FedRAMP PMO for record keeping.

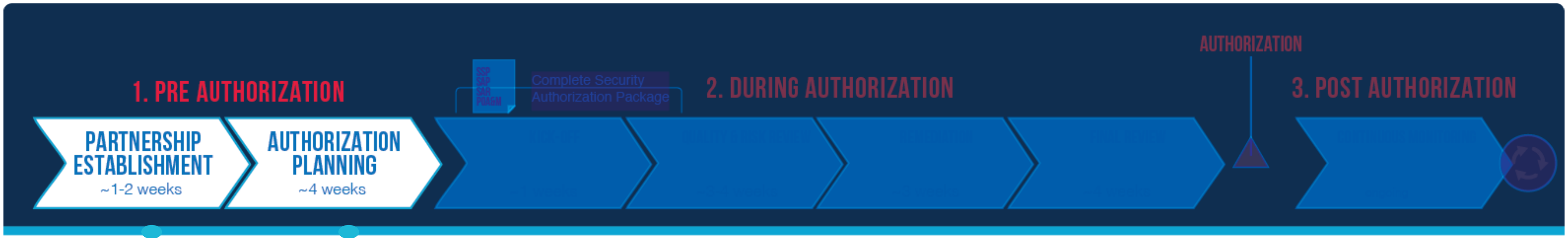
FedRAMP Authorized

THE JAB AUTHORIZATION PROCESS

FedRAMP Accelerated demonstrated the PMO's ability to reduce JAB authorization timelines by over 75%.


1
2
3
4
FedRAMP Readiness Assessment
Complete FedRAMP Security Assessment
JAB Authorization Process
NEW
FedRAMP Ready
Kick-Off
JAB Review
Remediation
Final Review
P-ATO
1 Month
1-3 Month
1 Week
3-4 Weeks
≤ 3 Weeks
4 Weeks
Readiness Assessment Report
Security Authorization Package
SSP
SAP
SAR
POA&M

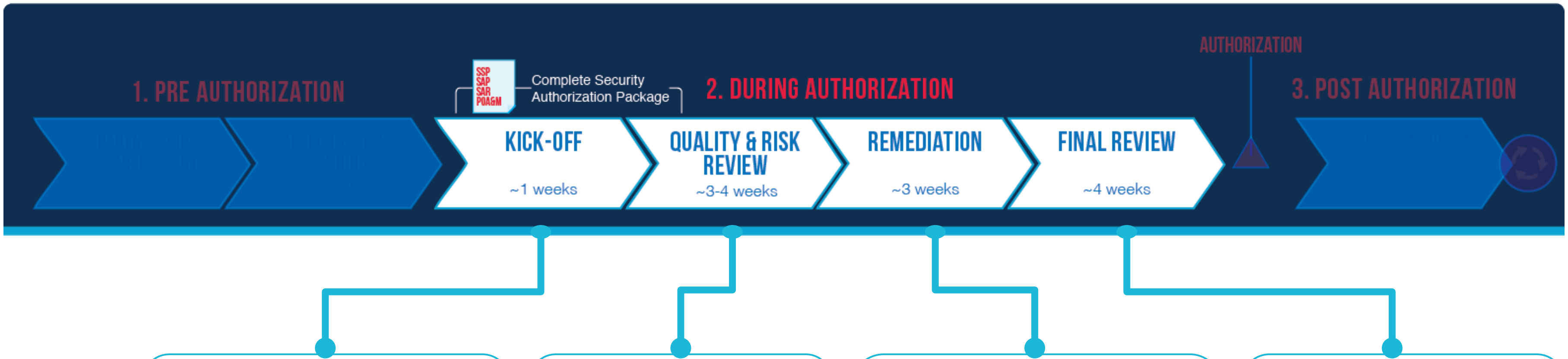
AGENCY AUTHORIZATION PROCESS:
1. PRE AUTHORIZATION



An Agency selects a CSO that meets their mission needs and establishes a working relationship in accordance with FedRAMP's ***In Process*** guidelines.

The Agency and CSP plan and set up their FedRAMP Agency authorization for success by confirming resources and determining a deliverable development and review approach.

AGENCY AUTHORIZATION PROCESS:
2. DURING AUTHORIZATION



All stakeholders obtain consensus on roles and responsibilities; agree on an overall process, project plan, milestones, deliverables, and schedule; and develop an understanding of the cloud offering architecture and high-level security configurations.

Agency reviews FedRAMP security authorization package (SSP + Attachments, SAP, SAR, PO&AM) for both quality and risk.

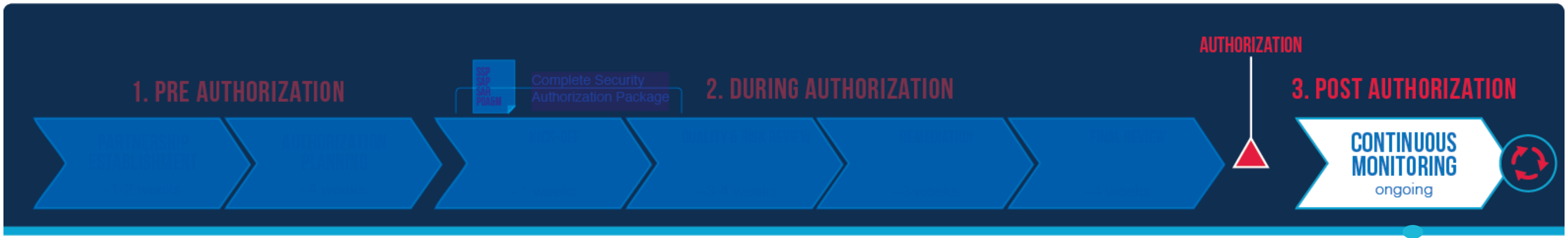
CSP addresses gaps identified by Agency reviewers to ensure the system is at an acceptable level of risk for the Agency.

Agency provides a defined timeframe to allow the CSP to make system updates and for the 3PAO to perform associated re-testing based on the Agency review (if applicable).

Agency provides their final approval for the CSP's authorization package.

Agency submits authorization package to FedRAMP for review.

AGENCY AUTHORIZATION PROCESS:
3. POST AUTHORIZATION



Agency establishes an ongoing continuous monitoring process.

CSP submits monthly continuous monitoring deliverables, major system change requests, and annual assessments to FedRAMP's secure repository.

FEDRAMP'S AGENCY REVIEW

FedRAMP makes the checklist we use to conduct our reviews available to the Agency community on our website.

Common Review Items

- Documentation review
  - SSP, SAP, SAR, POA&M, Continuous Monitoring Plan, ATO Letter
- Specific SSP checks
  - All critical controls are implemented
- Critical Control checks
  - Rules of Engagement are present
- SAP checks
- SAR checks
- Risks are documented
- POA&M checks
  - POA&M consistent with SAR Risk Exposure Summary Table

FedRAMP Program Updates

FedRAMP Connect

FEDRAMP CONNECT: OVERVIEW

The JAB selects 12 vendors per year to work with for a FedRAMP JAB P-ATO.

FedRAMP Connect – Evolving the Selection Process

- To evolve the program, the PMO worked with the JAB, OMB, and the CIO Council to develop clear, transparent criteria to prioritize CSPs for working with the JAB toward a P-ATO.
- Based on current resources and funding, the JAB has the capacity to authorize up to 12 CSPs a year.

Selection Criteria

- Demand is now the number one criterion for prioritization; it is also the only requirement for prioritization.
- There are also a range of preferential criteria if demand is all considered equal (government vs. commercial cloud, high impact vs. moderate impact, etc.).

Selection Process

- We received roughly 40 business cases for the inaugural FedRAMP Connect, held in early 2017.
- We selected 14 vendors to pitch their services to the JAB and 13 Agency CIOs and their representatives.
- The JAB prioritized 7 vendors and have kicked off the authorization process.
- Even if a vendor wasn’t selected for the JAB, we are working closely with them to identify an Agency match - 6 vendors have been matched to date.

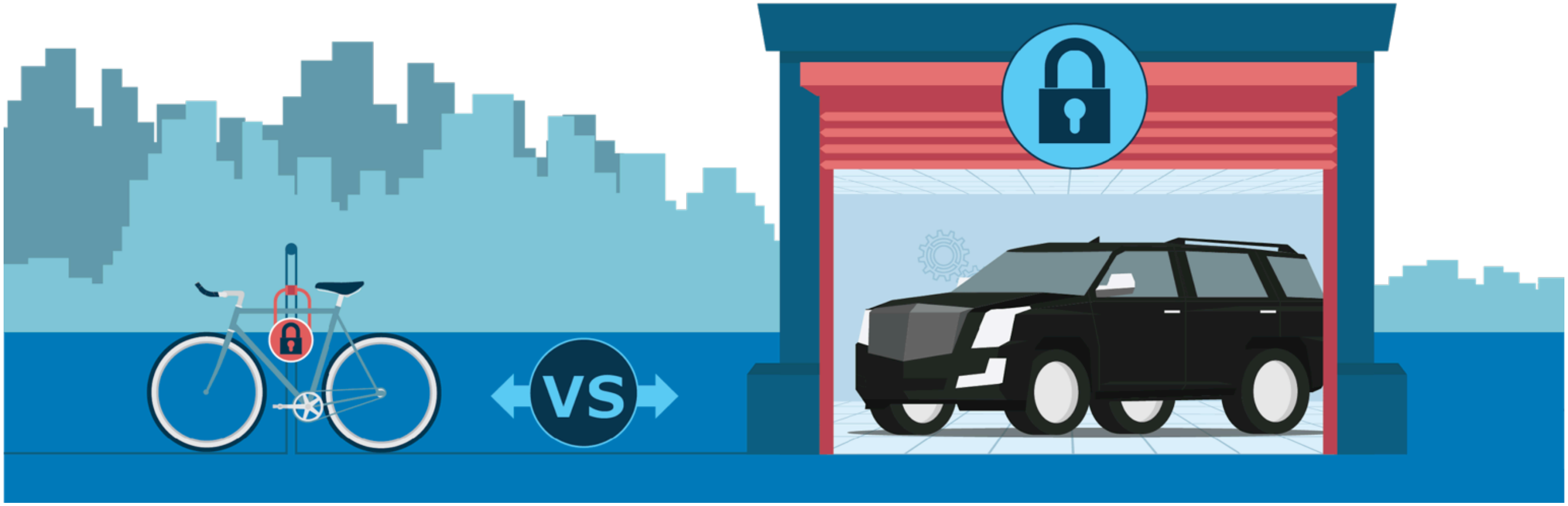
Upcoming Milestones

- We have received our second round of business cases and are currently conducting our analysis.
- We plan to prioritize vendors by early December.

FedRAMP Tailored

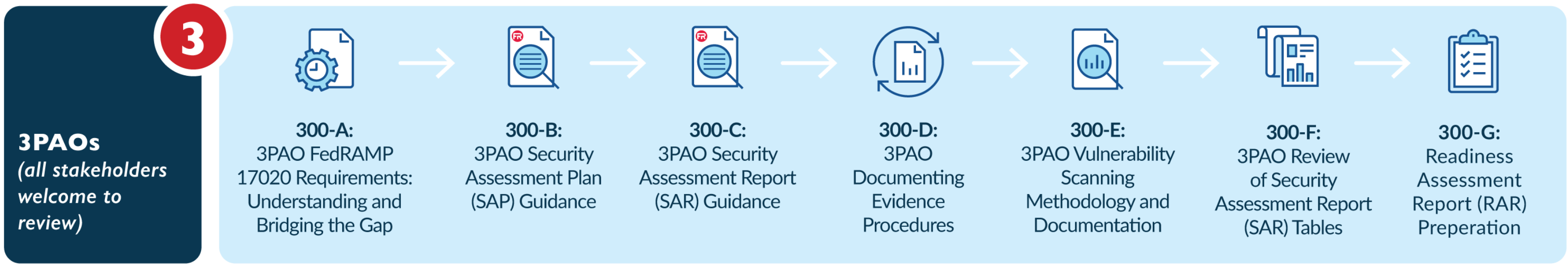
Not All SaaS are Created Equal

- FedRAMP was originally built around enterprise-wide solutions that would cover the **broadest range of data types** for cloud architectures and low, moderate, and high impact.
- **FedRAMP tailored addresses low risk use SaaS** — focusing on things like collaboration, project management, and open-source code development.
- You would not secure your 2017 Cadillac Escalade the same way you would secure your Huffy Bike – you need a more rigorous security mechanism for the SUV, while a U-lock device will suffice to secure your bicycle.



FedRAMP 3PAO Training Series

3PAO TRAINING SERIES: OVERVIEW



3

3PAOs
(all stakeholders welcome to review)

300-A: 3PAO FedRAMP 17020 Requirements: Understanding and Bridging the Gap

300-B: 3PAO Security Assessment Plan (SAP) Guidance

300-C: 3PAO Security Assessment Report (SAR) Guidance

300-D: 3PAO Documenting Evidence Procedures

300-E: 3PAO Vulnerability Scanning Methodology and Documentation

300-F: 3PAO Review of Security Assessment Report (SAR) Tables

300-G: Readiness Assessment Report (RAR) Preperation

300-Level Training Series

- Provides a deeper understanding of FedRAMP requirements and the LOE required to satisfactorily plan and perform a FedRAMP security assessment.
- Provides guidance to alleviate challenges 3PAOs face when:
  - Reviewing security package artifacts in accordance with FedRAMP requirements
  - Developing the Security Assessment Report (SAR)
  - Completing assessment documentation

Course Release Schedule

- **November 2nd**: 300-A FedRAMP ISO 17020 Requirements: Understanding and Bridging the Gap
- **December 5th**: 300-B 3PAO Security Assessment Plan (SAP) Guidance
- **December 5th**: 300-C 3PAO Security Assessment Report (SAR) Guidance
- **January 4th**: 300-D 3PAO Documenting Evidence Procedures
- **January 4th**: 300-E 3PAO Vulnerability Scanning Methodology and Documentation
- **February 1st:** 300-F 3PAO Review of Security Assessment Report (SAR) Tables

RFI For Cloud, FedRAMP, and Security Contract Language

CLOUD CONTRACT LANGUAGE RFI: OVERVIEW

FedRAMP is Seeking Input by December 15, 2017!

- FedRAMP has been identifying ways to create **standard contract language that agencies can use in their acquisition process** as they procure cloud-based products.
- FedRAMP, along with the GSA Secure Cloud Portfolio, is requesting industry feedback regarding the **acquisition process and how agencies include cloud, FedRAMP, and other security requirements in their contracts.**
- This feedback will allow us to continue to provide **improved guidance for government acquisition officials and contracting professionals**.
- The information gathered in this RFI will help identify **examples of preferred contract language** agencies should incorporate to convey FedRAMP requirements in their solicitations. These examples will be used to generate guidance and education for agencies.
- To provide your feedback, **please access the Request for Information (RFI) and provide comments on GitHub.**

Focus on FedRAMP

QUESTIONS?

info@fedramp.gov