FedRAMP: A Practical Approach

Katy Warren
Rock Sabetto

July 2018

Approved for Public Release;
Distribution Unlimited. Case Number 18-2368

MITRE

FedRAMP Agenda

- Introduction
- Process
- Considerations
- DoD FedRAMP+
- Closing Thoughts

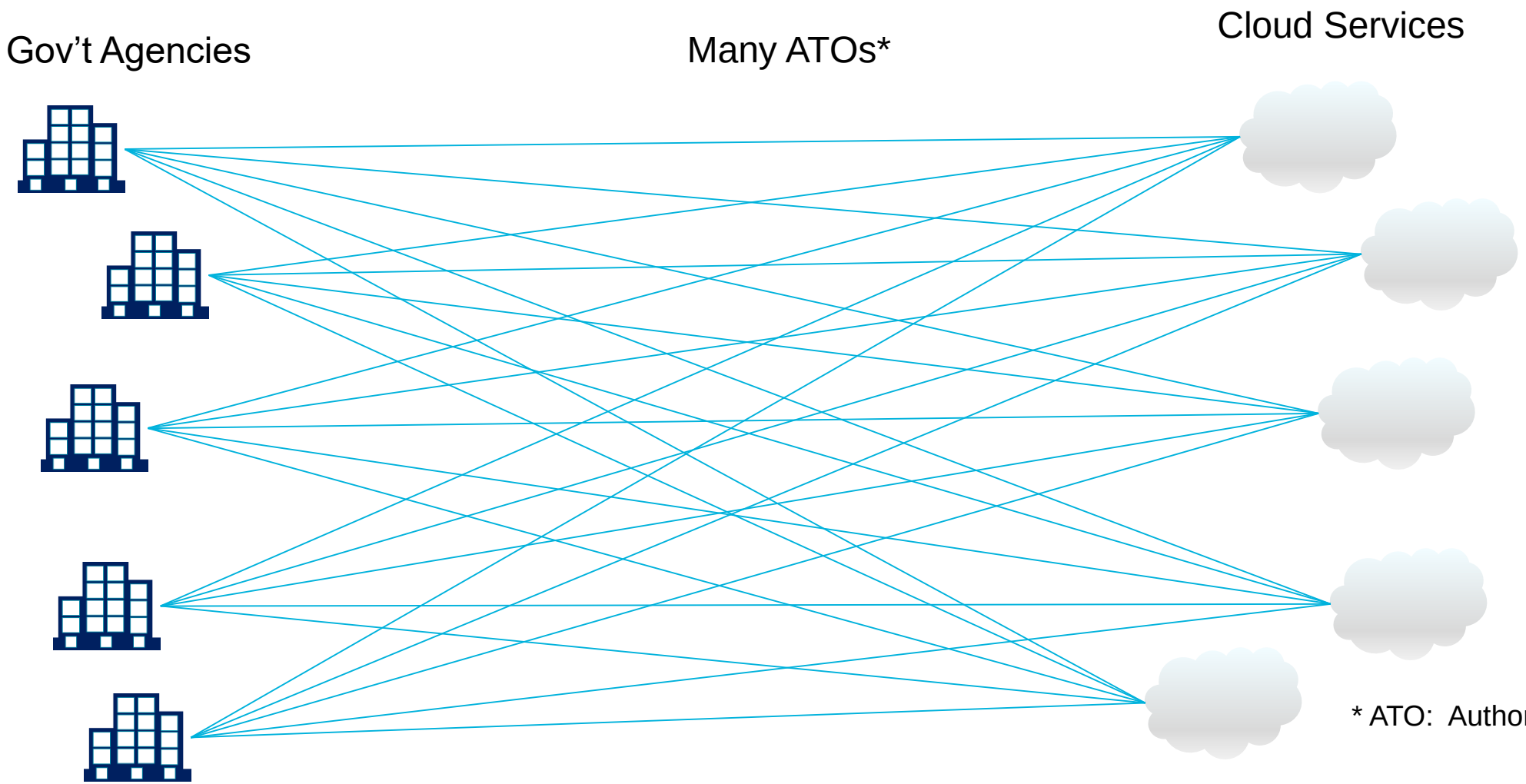
MITRE

Cloud Primer: 5, 4, 3

- **5 Essential Cloud Computing Characteristics**
  - *Resource Pooling*. Compute resources can be shared by multiple users
  - *On Demand*. Compute resources can be "spun up" as they are needed (and torn down, put back in the pool as they are no longer needed)
  - *Broadband Access*. The cloud environment is online (typically via the Internet / ISP) and is accessible from remote locations
  - *Metered Services*. Compute resource usage is measured for the purposes of billing, accounting, SLA measurement, etc.
  - *Rapid Elasticity*. Cloud environment can scale up (or down) quickly to accommodate new users and/or new compute requirements from existing users
- **4 Cloud Deployment Models**
  - *Private*. Solely for an organization
  - *Community*. Shared by multiple organizations from a community with shared concerns (e.g., mission, security requirements)
  - *Public*. Shared by many tenants, to include businesses and the general public. Owned by a cloud service provider
  - *Hybrid*. Some combination of the above, and potentially on premise IT as well
- **3 Cloud Service Models**
  - *IaaS* (infrastructure)
  - *PaaS* (platform)
  - *SaaS* (software)

FedRAMP Introduction

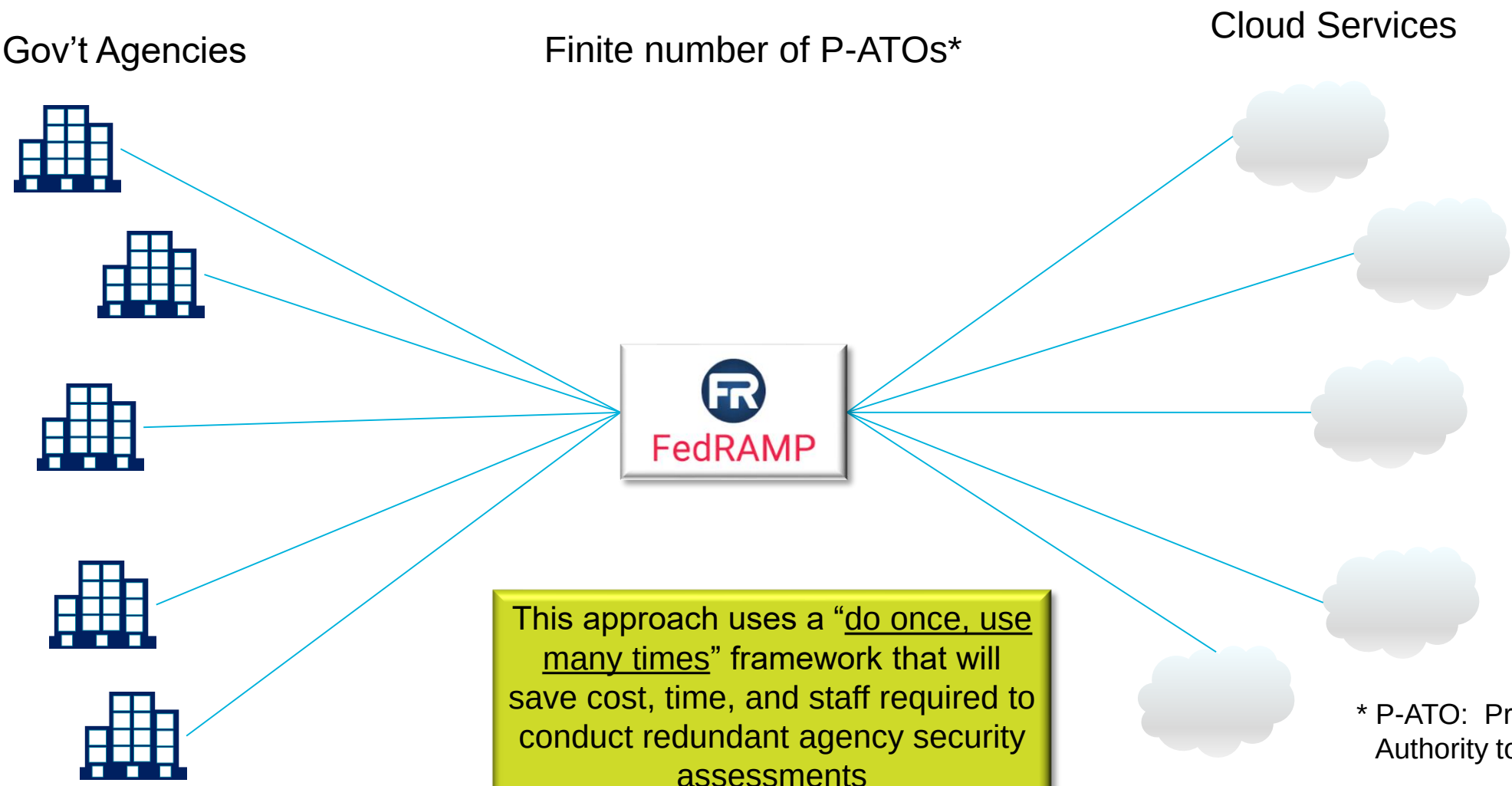
Before the creation of the *Federal Risk and Authorization Management Program* (FedRAMP)



* ATO: Authority to Operate

MITRE

After FedRAMP



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

* P-ATO: Provisional Authority to Operate

MITRE

Federal Risk and Authorization Management Program (FedRAMP)

- **FedRAMP is a Government-wide Cloud Program**
  - Provides standardized approach to security assessment and authorization
  - Ensures POA&M* remediation and continuous monitoring

- **Memo issued by 2nd CIO of the US, Steven VanRoekel**
  - Published to federal agency CIOs on December 8, 2011
  - Defining how federal agencies should use FedRAMP

- **Hosted by the Office of Management and Budget (OMB)**

- **Current FedRAMP Director - Matt Goodrich**

* POA&M: Plan of Actions and Milestones

FedRAMP Governing Bodies

- **FedRAMP PMO (GSA):** Administers FedRAMP, providing standard guidance and information
- **Joint Authorization Board (JAB):** Primary governance and decision-making body for FedRAMP. Members from CIO offices of DHS, GSA, and DOD. Grants P-ATOs, accredits 3PAOs, defines security requirements
- **CIO Council:** Disseminates FedRAMP information to Federal CIOs
- **DHS:** Manages FedRAMP continuous monitoring strategy including data feed criteria, reporting structure, threat notification coordination, and incident response
- **DOD:** Created FedRAMP+ model with Information Impact Levels for DOD programs
- **NIST:** Advises FedRAMP on FISMA compliance, assists in developing standards for 3PAOs accreditation
- **OMB:** Issued FedRAMP policy memo defining key FedRAMP requirements and capabilities

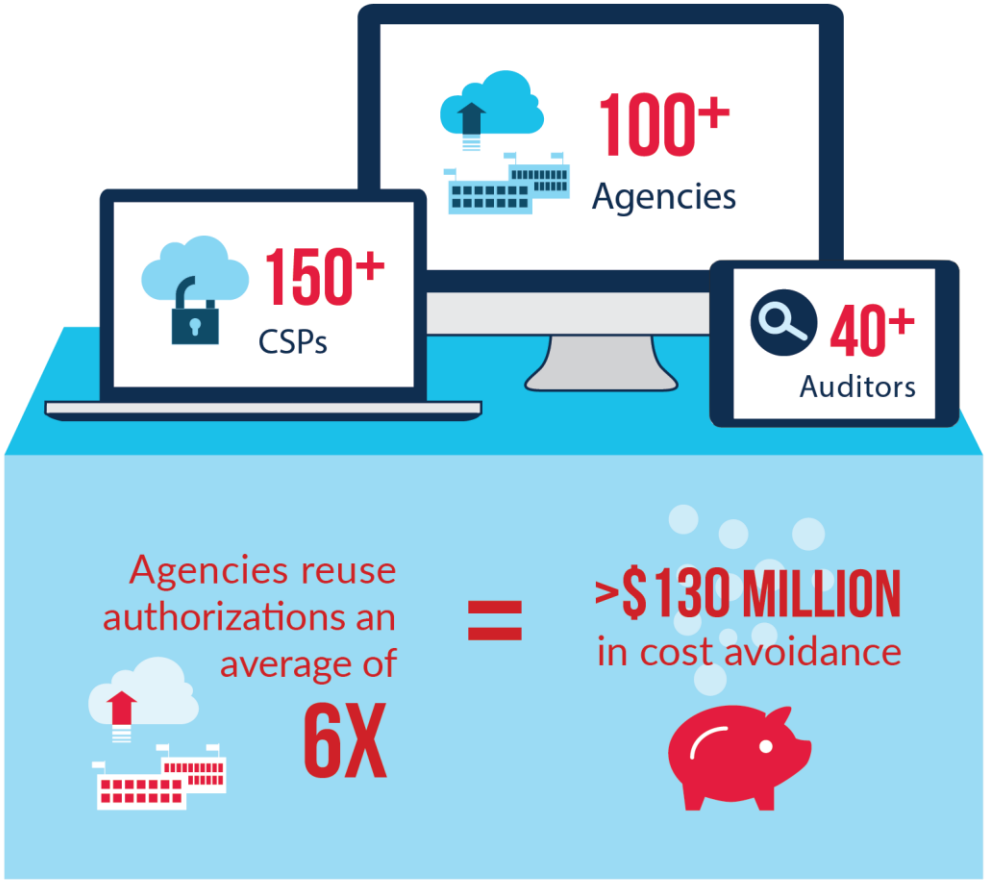
Image Source: https://www.fedramp.gov/governance/

MITRE

FedRAMP Today

We cover more than
5 MILLION ASSETS
of the world's largest cloud providers

and **1/3** of the world's internet traffic through our program



WE NOW OFFER

4 security baselines so government can match security to risk

- **HIGH** *(421 controls)*
- **MODERATE** *(325 controls)*
- **LOW** *(125 controls)*
- **LI SAAS** *(38 controls)*

Image Source: https://www.fedramp.gov/about/

MITRE

FedRAMP builds upon existing policy, frameworks

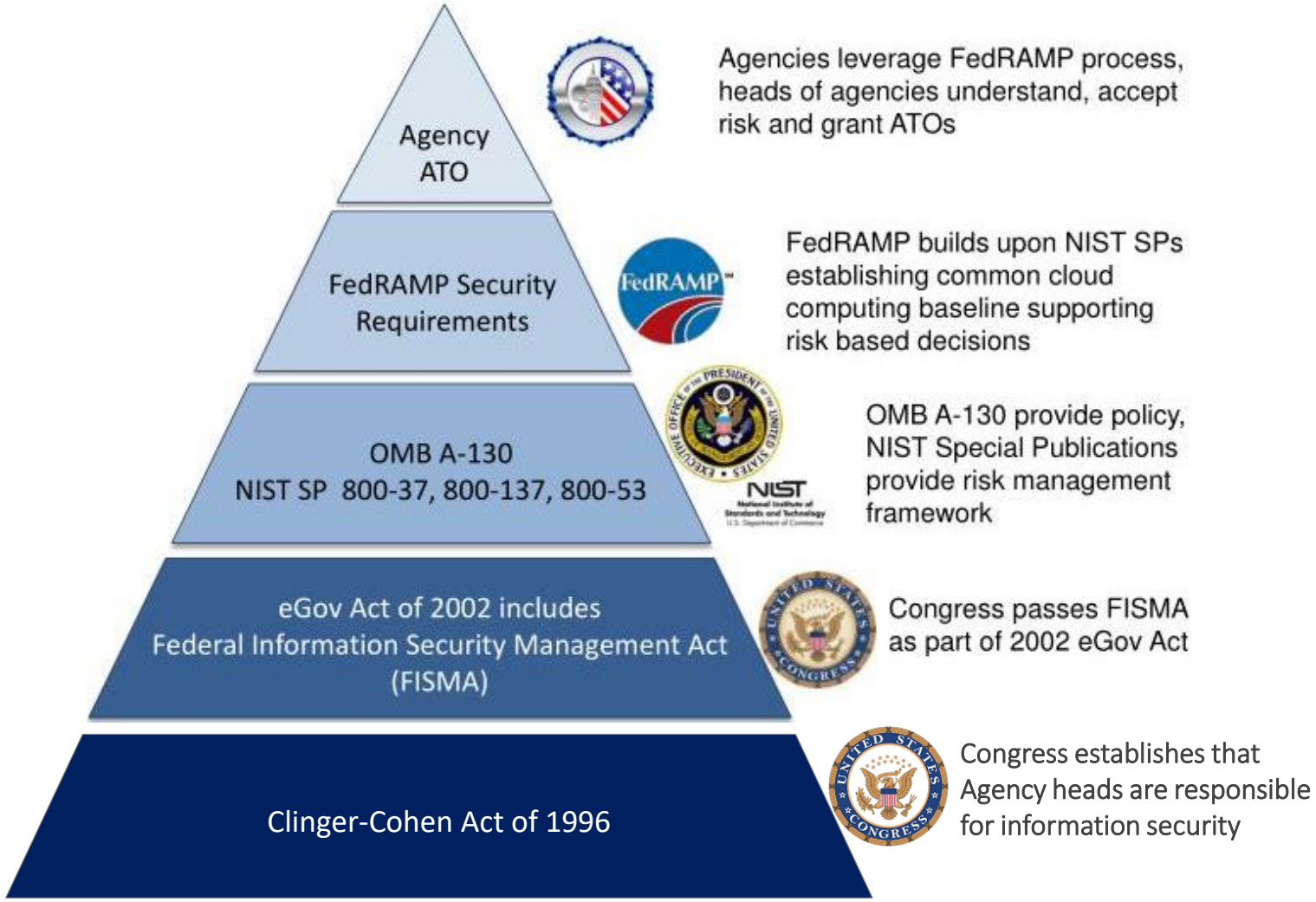


Image Source: *NIST FedRAMP overview, 7/10/2014*

Note: Image adapted by MITRE to include Clinger-Cohen

MITRE

FedRAMP Partners

- **Agency**
  - Owner of the operational systems and information
  - Accountable for security: owns the risk associated with moving to cloud. Grants the ATO
  - Over 100 Agencies have implemented FedRAMP-compliant cloud solutions*
- **CSP (Cloud Service Provider)**
  - Provides cloud service to the Agency
  - Responsible for obtaining P-ATO (provisional)
  - Current providers include: AWS, Microsoft (Azure), IBM, Google, Oracle, Salesforce
  - Currently there are 102 authorized CSPs*
- **3PAO (Third Party Assessment Organization)**
  - Accredited, independent CSP assessors
  - Perform initial and periodic assessments of CSPs against FedRAMP security requirements
  - Currently there are 43 authorized 3PAOs*

* www.fedramp.gov as of 6/4/2018

MITRE

FedRAMP Learning Paths for CSPs, 3PAOs, and Agencies

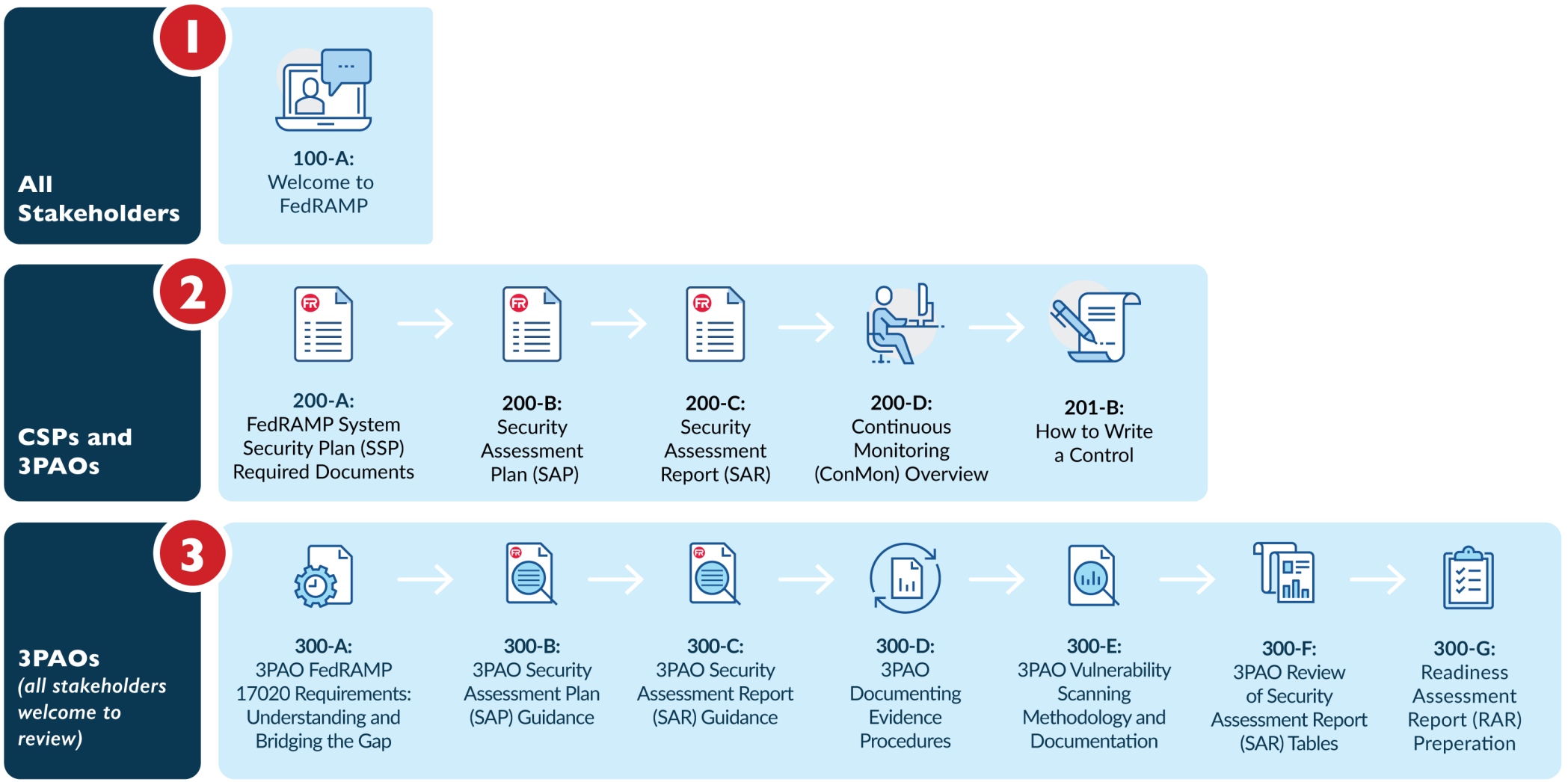
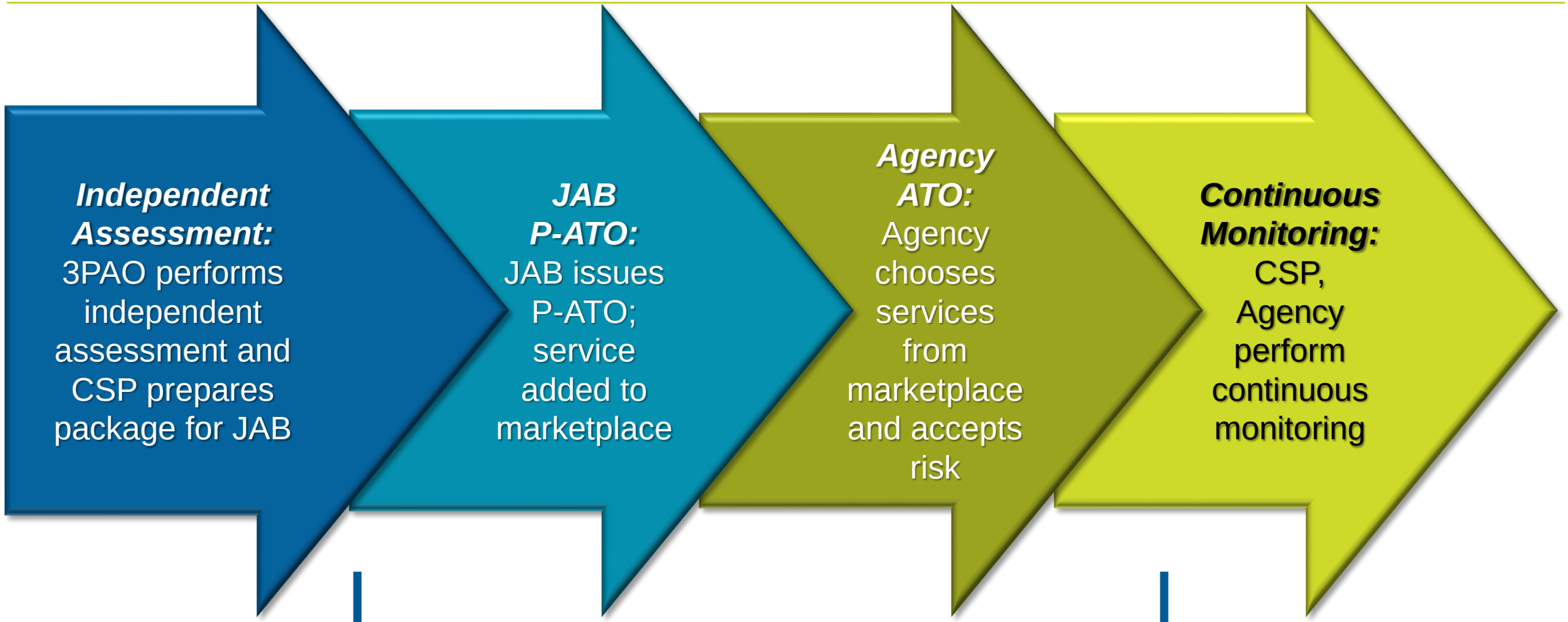


Image Source: https://www.fedramp.gov/training/

MITRE

FedRAMP Process

Overall FedRAMP Process

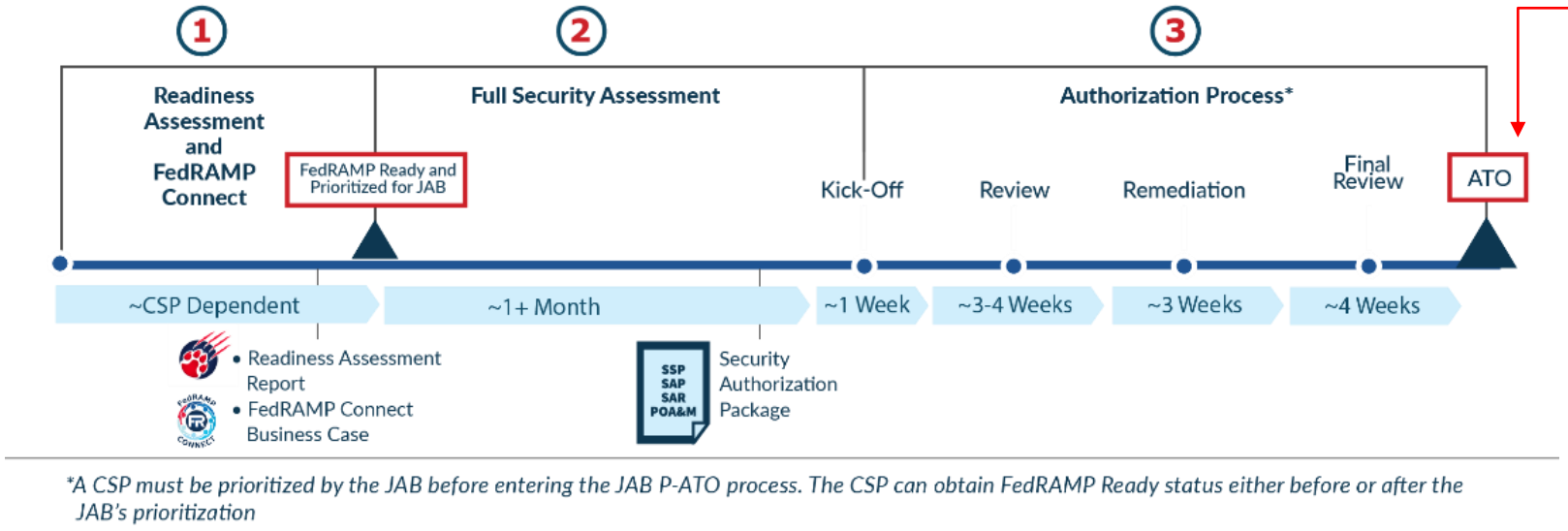


Next slides focus on JAB P-ATO and Agency ATO processes

MITRE

FedRAMP Process: JAB P-ATO

- CSPs obtain Provisional ATO (P-ATO) to provide service to Federal organizations via 3PAO companies
- P-ATO is granted by FedRAMP's Joint Authorization Board (JAB)
- Authorization Package minimally includes Security Plan (SSP), Security Assessment Plan and Report (SAP, SAR), POA&M, Continuous Monitoring Plan



A CSP must be prioritized by the JAB before entering the JAB P-ATO process. The CSP can obtain FedRAMP Ready status either before or after the JAB's prioritization

Note: image, copied from FedRAMP.gov, refers to the CSP P-ATO as "ATO".

Note: Agencies seeking services which have not obtained P-ATO may sponsor this process, and may be able to share cost with the CSP since the CSP will benefit from providing the service.

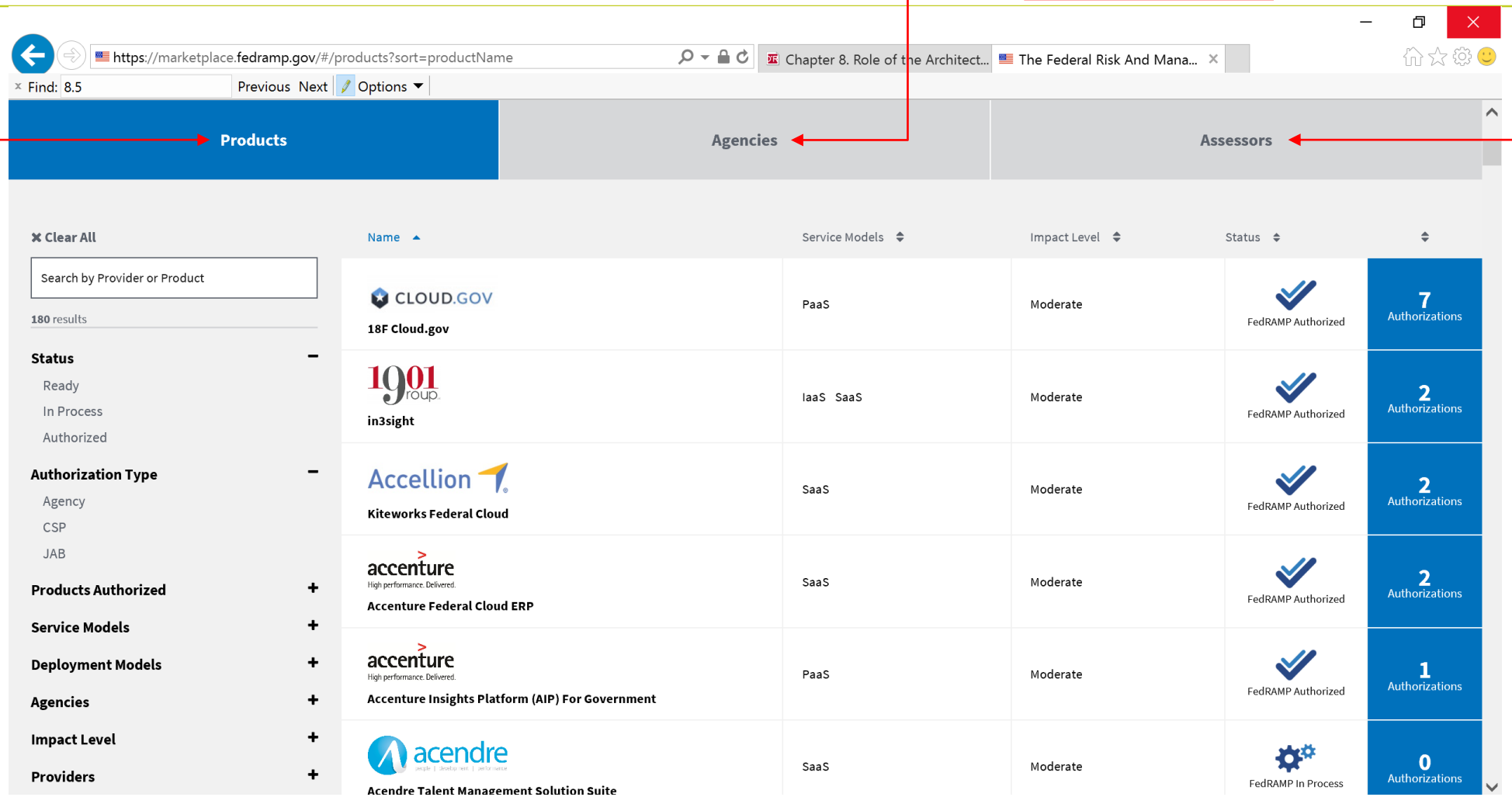
MITRE

FedRAMP Marketplace

Agency by Agency list of CSPs, CSP services in use

CSP offerings with JAB P-ATO or Agency ATO

3PAO companies with approval to "assess" CSPs

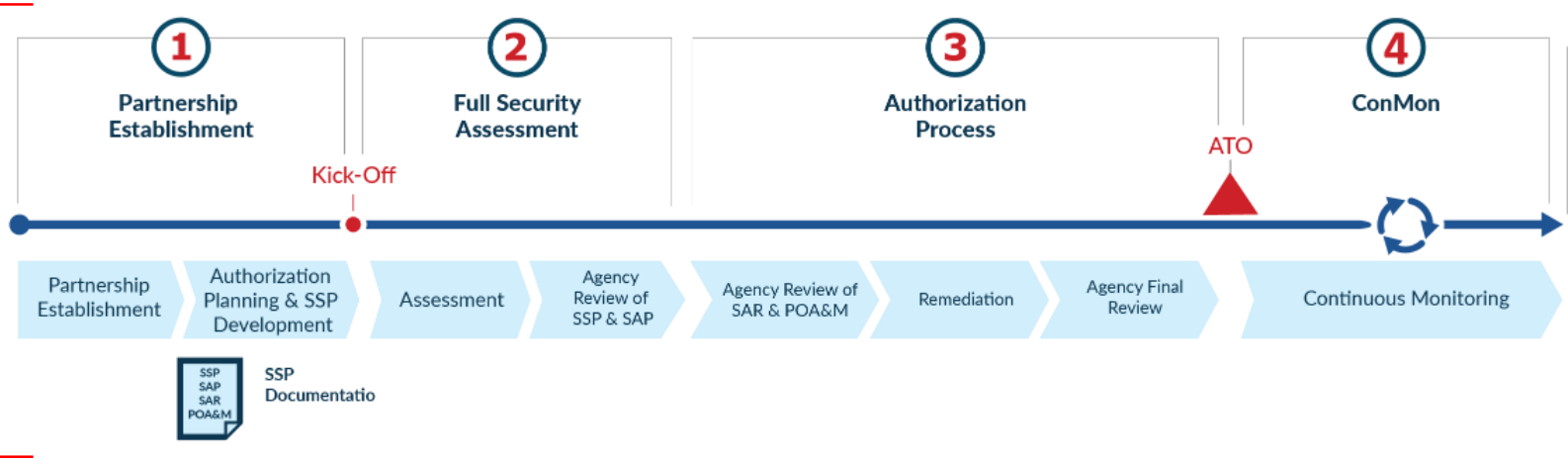


MITRE

FedRAMP Process: Agency Authorization

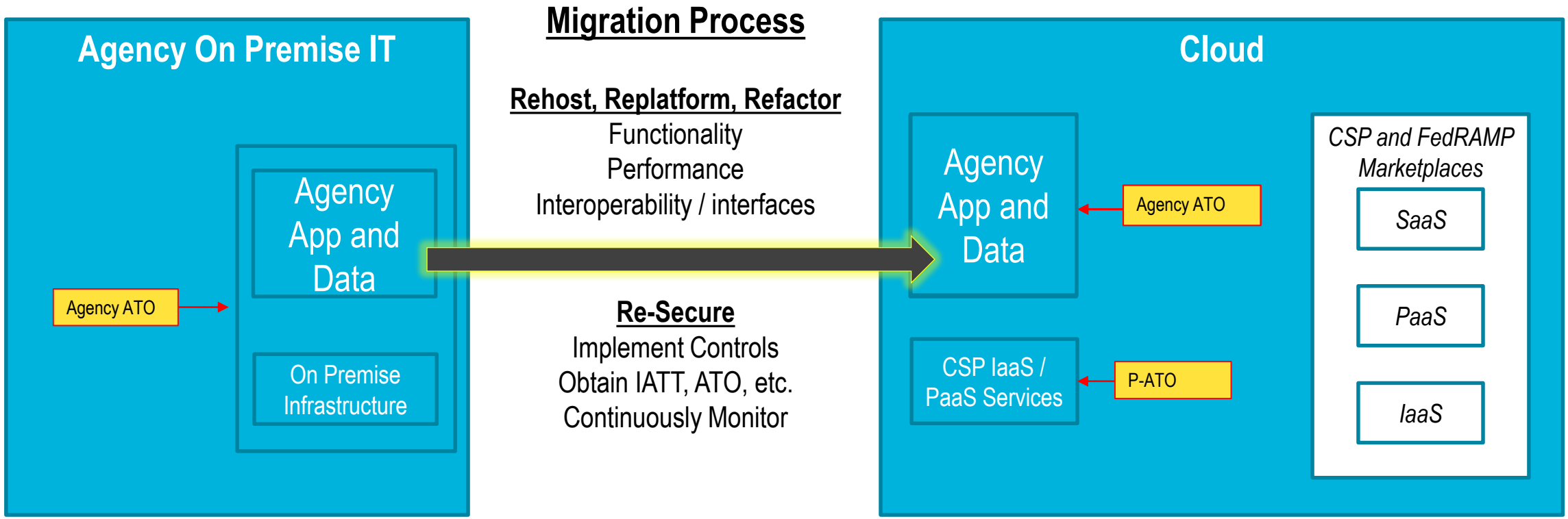
- Process used in cases where CSP service will serve one Agency or a small number of Agencies
- Agency grants ATO, using similar documentation package. Can be augmented with additional controls
- Other Agencies can leverage Agency ATO directly, but must accept risk
- Agency authorizations may include IATT, IATO, risk acceptance memorandum, etc.

Note: this process is described in detail in the *FedRAMP Agency Authorization Playbook* available on the FedRAMP public website



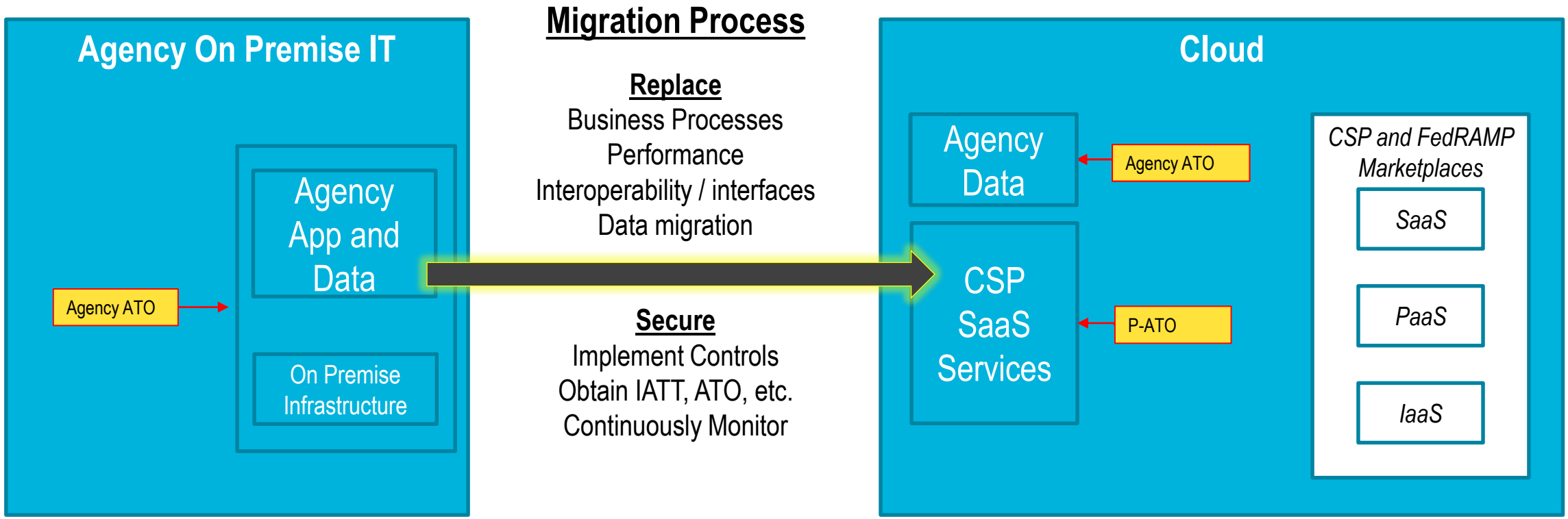
MITRE

Example: Legacy Application Migration and ATOs



MITRE

Example: Migration to SaaS and ATOs



MITRE

FedRAMP Considerations

Considerations (1 of 3)

- **FISMA compliance is mandatory.** Agencies comply with FISMA by applying NIST controls. For Federal Agency cloud deployments at low, moderate, and high risk impact levels, FedRAMP provides a proven, NIST-based path for FISMA compliance.
- **Median Cost** for CSP to Obtain FedRAMP P-ATO = $2.25M (50% engineering work, 50% process). Ongoing Cost = $1M to maintain Continuous Monitoring. Source: Continuum GRC site
- **Time to ATO**
  - 2014 – 16 months for JAB P-ATO, 13 months for Agency ATO; 2016 – 7 months for JAB P-ATO, 7 months for Agency ATO. Source: 2017 independent study by Coalfire 3PAO
  - Reduction in times have been driven by the "FedRAMP Accelerated" initiative. The processes described in this briefing are the result of this initiative. More details are available here: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Accelerated_A_Case_Study_For_Change_Within_Government.pdf

Considerations (2 of 3)

- **Data Ownership.** Government Agencies should carefully assess the data ownership portions of CSP contracts and SLAs. This is particularly important if the government wants to get the data out of the CSP (e.g., to move it on premise or to another CSP)
- **TIC Compliance.** TIC compliant architectures are required through the FedRAMP security controls baseline. TIC compliance is a hybrid responsibility with CSPs needing to have an architecture that supports TIC and Agencies enforcing TIC routing and compliance
- **POA&M Remediation.** A CSP has 30 days for remediating high POA&M items, 90 days for remediating moderate POA&M items, and 180 days to remediate low POA&M items
- **Change Management**
  - CSPs changing existing services (IaaS/PaaS/SaaS with JAB P-ATO) will document the change in the FedRAMP Significant Change Form and submit to FedRAMP for approval.
  - Agencies changing their cloud-hosted systems (i.e., systems they have installed on top of CSP services) will follow Agency-specific change control procedures

Considerations (3 of 3)

- **FedRAMP Security Baselines.** FedRAMP (like FISMA) uses (but is not limited to) NIST SP 800-53 r4 security controls:
  - HIGH = 421 Controls
  - MODERATE = 325 Controls
  - LOW = 125 Controls
  - LOW IMPACT (LI-SaaS) = 38 Controls (FedRAMP Tailored)
  - Controls are all downloadable via FedRAMP website
  - Notes:
    - Currently the only Approved FedRAMP HIGH CSPs are AWS, Azure, CSRA, Oracle, Workplace.Gov, Zscaler
    - FedRAMP Tailored LI-SaaS minimum requirements are described in the “FedRAMP Tailored Security Requirements for LI-SaaS” document, including restriction of PII to SaaS login information only
- **Automation.** FedRAMP is working with NIST to begin implementing OSCAL (Open Security Controls Assessment Language). OSCAL is an emerging control language for security authorization that seeks to introduce automation and reduce subjectivity in control assessments

DoD FedRAMP+

FedRAMP+

- **DoD established "FedRAMP+" (FedRAMP-Plus)** containing additional security controls beyond basic FedRAMP

- **FedRAMP+ P-ATO process**
  - Similar to, but separate from, the base FedRAMP process
  - Leverages NIST RMF (NIST SP 800-37R1)
  - Includes establishing "Impact Levels" that define specific requirements for Unclassified data that is not sensitive / somewhat sensitive / very sensitive / classified. Impact levels are 2, 4, 5, 6

- **Many non-DoD agencies accept FedRAMP+**
  - Agencies may leverage the added security requirements
  - Usually, DoD does not accept other agency ATOs

FedRAMP+ Information Impact Level Comparison
Source: DoD Cloud Computing Security Requirements Guide, 3/6/2017

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

MITRE

DoD Cloud Services: Assessment and Authorization Roles
Source: DoD Cloud Computing Security Requirements Guide, 3/6/2017

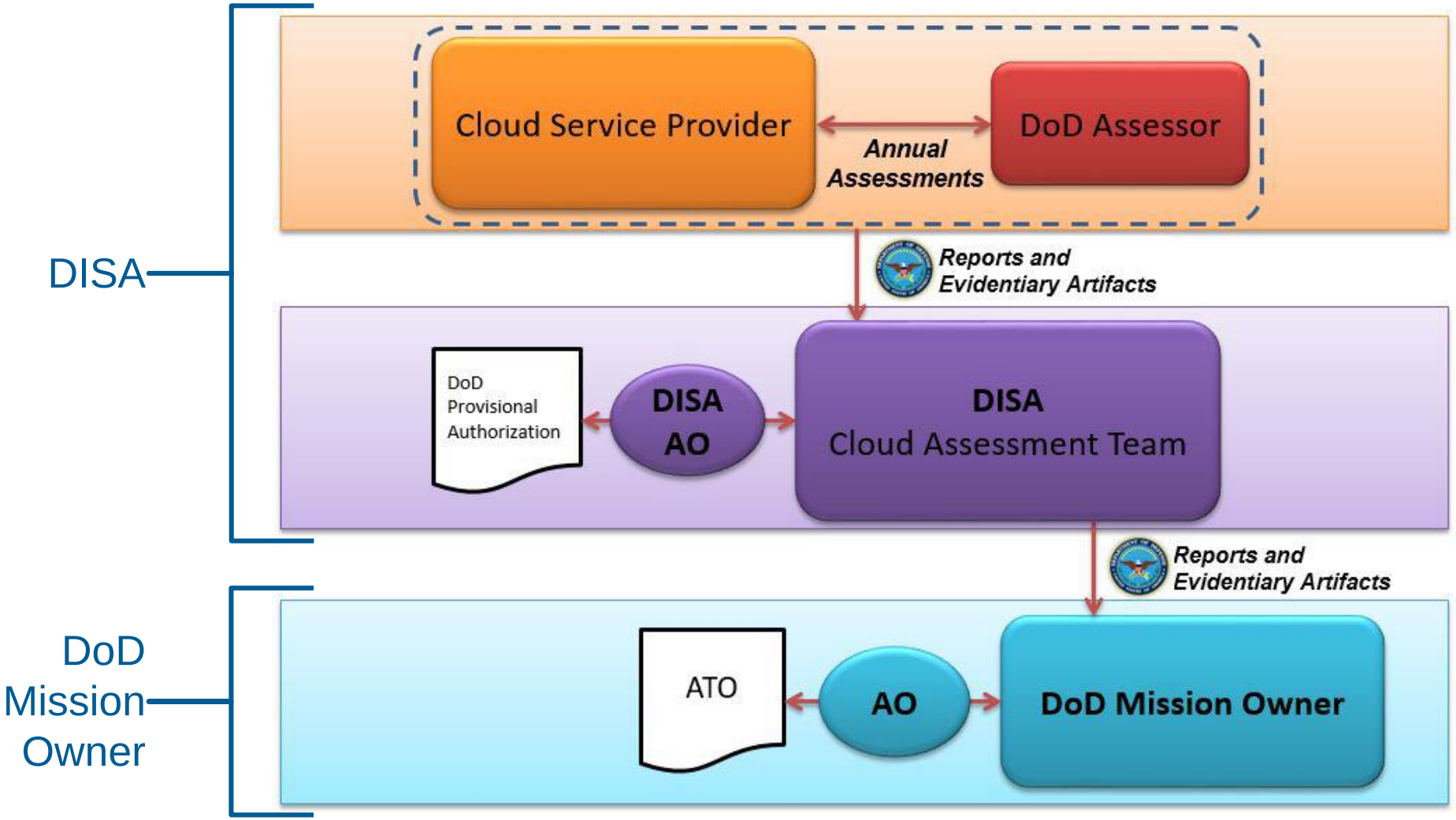


Image Source: DoD Cloud Computing SRG, *Figure 6 – DoD Continuous Monitoring for DoD Assessed CSOs*

MITRE

Closing Thoughts

Closing Thoughts

- **FedRAMP is achieving the objective to "do once, use many times"**
  - Effectively reducing time and expense required for Agencies to adopt cloud services
  - Over 100 Agencies, 150 CSPs, and 40 3PAO Assessors have successfully leveraged FedRAMP
- **Understanding FedRAMP is an important part of cloud adoption, but…**
  - FedRAMP addresses security, but does not cover funding, acquisition, engineering, operational, governance, or agency-specific security / change control requirements

Agencies are accountable for security

CSOs with JAB P-ATO still require Agency ATO

This is true even if the Agency is leveraging a SaaS solution: the Agency must still ensure data is protected

MITRE

Questions?

Sources

- FedRAMP.gov (accessed during May and June 2018)
- NIST FedRAMP Overview, NIST Technology Standards Coordination Office, 7/10/2014
- OMB Federal CIO Memo, “Security Authorization of Information Systems in Cloud Computing Environments”, 12/8/2011
- FedRAMP Wikipedia page (accessed 3/16/2018)
- Continuum GRC https://continuumgrc.com/fedramp/ (accessed 3/15/2018)
- FedRAMP Marketplace: https://marketplace.fedramp.gov/ (accessed during May and June 2018)
- DoD Cloud Computing Security Requirements Guide, DISA for DOD CIO, 3/6/2017
- Coalfire Report, “Securing Your Cloud Solutions: Research and Analysis on Meeting FedRAMP / Government Standards”, 2017
- FedRAMP Industry Day briefing, FedRAMP, 6/4/2014

MITRE