DeMystifying FedRAMP

Jason Allen, Yello

Presented: 2019-03-06

DEMYSTIFING FEDRAMP

This is only the start of our FedRAMP journey

DEMYSTIFING FEDRAMP

What is FedRAMP?

“The Federal Risk and Authorization Management Program (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 saves cost, time, and staff required to conduct redundant Agency security assessments.”

When is FedRAMP required?

FedRAMP is mandatory for Federal Agency cloud deployments and service models at the low, moderate, and high risk impact levels.

NASA

Peace Corps

Department of Defense

Impact Levels

Cloud Service Offerings (CSOs) are categorized into one of three impact levels: Low, Moderate, and High; and across three security objectives: **Confidentiality, Integrity, and Availability.**

FedRAMP Low

127 Security Controls. Low Impact is most appropriate for CSOs where the loss of confidentiality, integrity, and availability would result in limited adverse effects on an agency's operations, assets, or individuals.

FedRAMP Moderate

327 Security Controls. Moderate Impact systems accounts for nearly 80% of CSP applications that receive FedRAMP authorization and is most appropriate for CSOs where the loss of confidentiality, integrity, and availability would result in serious adverse effects on an agency's operations, assets, or individuals.

FedRAMP High

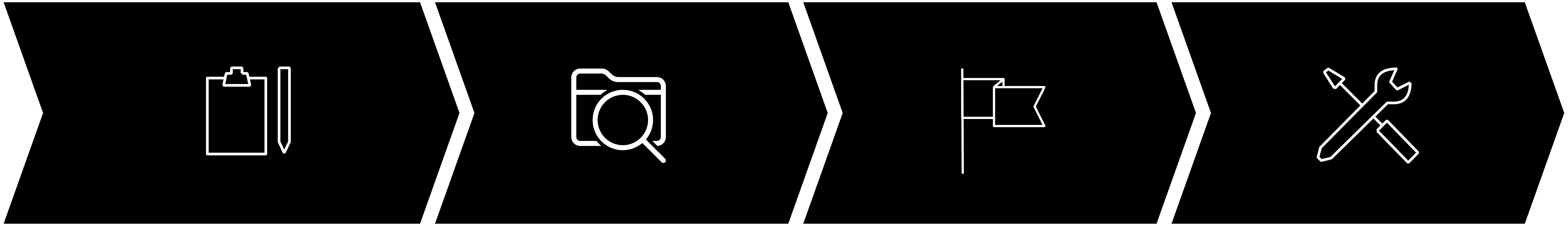
423 Security Controls. High impact usually in Law Enforcement and Emergency Services systems, Financial systems, Health systems, and any other system where loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Potentially a large investment

- Average cost of FEDRAMP based on Coalfire's (consulting firm) report $350K-$865K (excluding addtl headcount)
- FedRAMP takes approximately 12 months to achieve once in-process
- Annual assessment and recertification generally costs approx. 70% of the initial cost.
- Application and/or infrastructure engineering will be required

FedRAMP Authorization Process

Simplified flow of recommended steps for achieving FedRAMP authorization



Initial gap assessment

Which baseline controls aren't you meeting?

Full security assessment

After you've remediated any gaps another firm conducts a full assessment

Authorization process

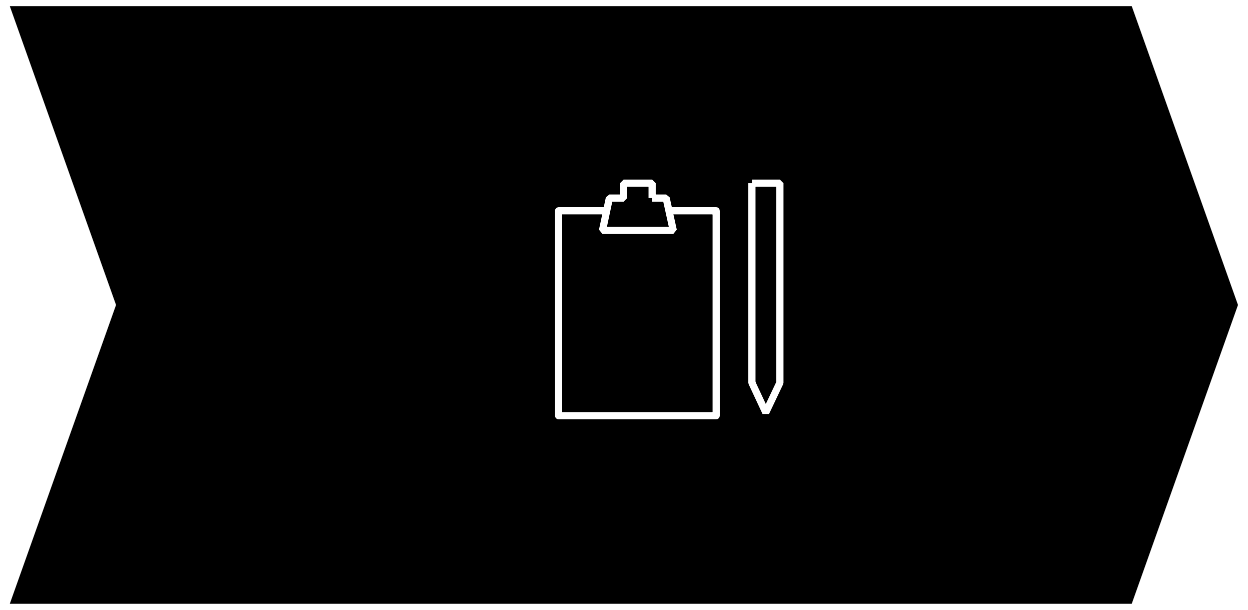
Packet is presented to the FedRAMP PMO and if everything goes well, you're authorized

Continuous Monitoring

Monthly reporting is required after authorization has been granted

Initial Gap Assessment

Simplified flow of recommended steps for achieving FedRAMP authorization



Initial gap assessment

Which baseline controls aren't you meeting?

Authorization Process

Simplified flow of recommended steps for achieving FedRAMP authorization

Initial gap assessment

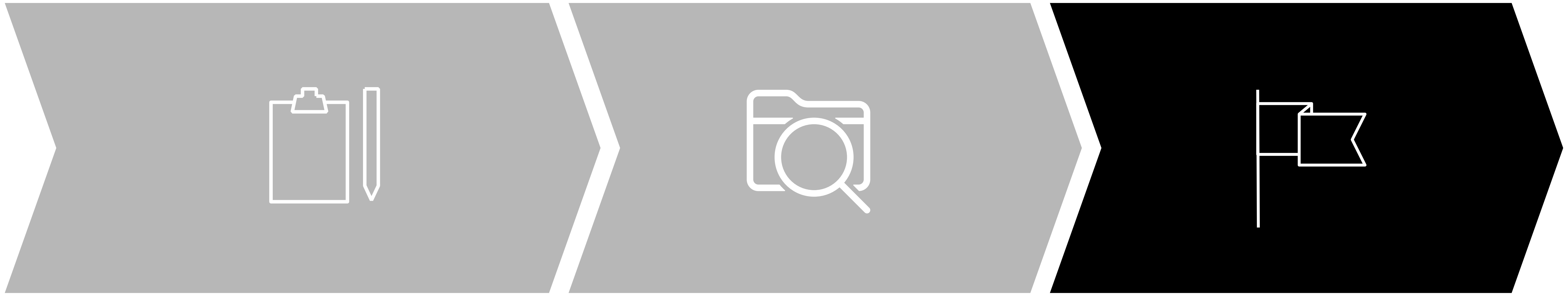
A company is an association or collection of individuals, whether

Full security assessment

After you’ve remediated any gaps another firm conducts a full assessment

Authorization Process

Simplified flow of recommended steps for achieving FedRAMP authorization



Initial gap assessment

A company is an association or collection of individuals, whether

Full security assessment

A company is an association or collection of individuals, whether

Authorization process

Packet is presented to the FedRAMP PMO and if everything goes well, you’re authorized

Continuous Monitoring

Simplified flow of recommended steps for achieving FedRAMP authorization

Initial gap assessment

Which baseline controls aren't you meeting?

Full security assessment

After you've remediated any gaps another firm conducts a full assessment

Authorization process

Packet is presented to the FedRAMP PMO and if everything goes well, you're authorized

Continuous Monitoring

Monthly reporting is required after authorization has been granted

DEMYSTIFING FEDRAMP

JAB or Agency?

Joint Authorization Board (JAB)

A cloud system that is multi-tenant in nature and has a broad use case of capabilities is exactly the kind of cloud that should pursue JAB authorization. The JAB reviews clouds that can and are being used government-wide. So if a CSP is considering JAB authorization, they should definitely take into consideration the amount of federal interest in their service and the depth of use cases across the government.

Agency

If only one or two agencies are interested in a CSP's cloud product or the cloud was designed specifically for a particular agency, then agency authorization is a better fit. Agency authorizations are targeted for niche cloud services that may only be used by a singular agency. Clouds that are unique to a particular agency provide a great benefit to that agency, but is not a good option for JAB authorization.

SRG IMPACT LEVELS

A company is an association or collection of individuals, whether natural persons, legal persons, or a mixture of both. Company members share a common purpose and unite in order to focus.

SRG Impact Level 2: Non-Controlled Unclassified Information

Level 2 includes all data cleared for public release, as well as some DoD private unclassified information not designated as CUI or critical mission data, but the information requires some minimal level of access control.

SRG Impact Level 4: Controlled Unclassified Information

Level 4 accommodates CUI which is the categorical designation that refers to unclassified information that under law or policy requires protection from unauthorized disclosure or other mission critical data.
(Requires AWS GovCloud)

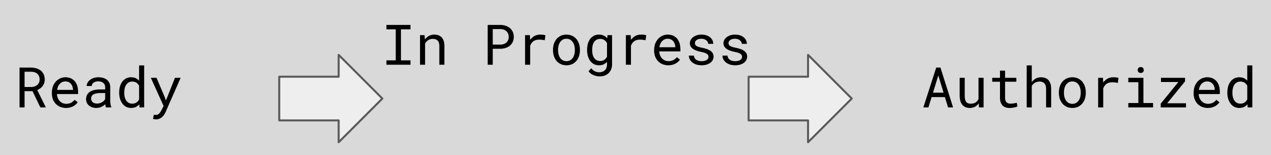
FedRAMP Cheat Sheet

The Federal Risk and Authorization Management Program (FedRAMP) is a United States government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

You should know:

- The average cost of FedRAMP authorization is $350K-$865K excluding engineering effort.
- FedRAMP is the way the government wants you to do security
- FedRAMP authorization can take 12-24 months

Phases:



Chicago DevSecops

Resources

NIST Publications

- 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
- 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

3PAOs

- A-LIGN
- Coalfire
- KRATOS
- Secure-IT

General

- FedRAMP Marketplace: Directory of all authorized CSPs
- FedRAMP CSPs: Starting point for service providers interested in FedRAMP
- Department of Defense Cloud Computing Security Guide

Common Terms

3PAO: Third Party Assessment Organization
AO: Authorizing Official
ATO: Authorization To Operate
CAP: Cloud Access Point
CSP: Cloud Service Provider
ConMon: Continuous Monitoring
FISMA: Federal Information Security Management Act
FedRAMP+: FedRAMP moderate and additional controls to meet IL4
FIPS: Federal Information Processing Standards
GovCloud: AWS FedRAMP High region
IAA: Inter-Agency Agreement
IL: Impact Level
JAB: Joint Authorization Board
P-ATO: Provisional Authorization to Operate
PA: Provisional Authorization
PMO: Program Management Office
POA&M: Plan of Action and Milestones
RAR: Readiness Assessment Report
SAP: Security Assessment Plan
SRG: Security Requirements Guide
SSP: System Security Plan