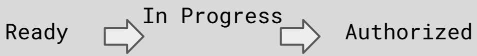
FedRAMP Cheat Sheet

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:



Ready ⇨ In Progress ⇨ Authorized

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