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.

Mandatory certification to offer cloud services to US Federal Government

FedRAMP can be resource intensive and expensive
FedRAMP Challenges

Building a compliant system for federal customers can be challenging, resource intensive, and time consuming.

Requires hiring additional resources for FedRAMP-related activities.*

Maintaining and managing the authorized environment is a significant investment.

FedRAMP Requirements

- **Infrastructure Stack**
- **Monitoring Stack**
- **Identity & Access Stack**
- **Process & Workflow**
- **Operational & Security Controls**
- **Engineering Controls**

* Dedicated resources should be considered due to work for teams supporting FedRAMP activities. Different sponsor agencies may have unique/stringent requirements (e.g., US-based resources).
Accelerate Product FedRAMP Timeline with Federal Ops Stack

**Product | Effort Analysis**

**Traditional Approach**
- Ready for Audit in ~24 Months +
- Solely maintain authorization (monthly and annual audits, documentation etc.)
- Sole responsibility to address all 325 controls

**Using Federal Ops Stack**
- Ready for Audit in ~12 Months
- Leverage FedRAMP-compliant Operational Security stack of services/tools
- Offload implementation of engineering-heavy technical controls
- Benefit from Ops stack offered heavy lifting for maintaining the certification post-authorization

**FedRAMP Controls**
- Operational & Security Controls
- Engineering Controls
  - Implement
  - Operate
- Monitor

**FedRAMP Control Stack**
- Operational & Security Controls
- Engineering Control Stack
  - Implement
  - Operate
- Monitor

**Total Effort Analysis**
- Total = 325 Controls (Rev4)

**Ops Stack inherited controls ~40-60%**
- Total = 325 Controls (Rev4)
Federal Ops Stack Services: Services and Key Features

Product 1
- Vulnerability Scanning
- Automated triage & attribution

Product 2
- Employee Identity Governance and Access
- Customer BYO-Idp (PIV/CAC)

Product 3
- 24x7 SOC
- Identify, Triage and coordinate
- Incident communication

Golden AMI w/ Compliance Drift Automation
- FIPS 140-2
- Compliance Drift
- Endpoint Protection

Continuous Monitoring (ConMon)

Federal Ops Stack VPC
- 24x7 SOC
- Identify, Triage and coordinate
- Incident communication
Federal Ops Stack: Services & Tools: IAM

Service Components

- Directory Services, SSO, MFA, Remote Access VPN
- Employee authentication and authorization
- Employee identity governance*
  - US persons validation
  - Employee access review (onboard, move, terminate, revalidation)
- Customer federated access (PIV/CAC)
- OAuth Clients
- Self-service APIs
Federal Ops Stack: Services & Tools: Vulnerability Management

Service Components

- Vulnerability Scanning (network, applications, databases, hosts, compliance)
- Container Vulnerability Scanning
- Automated Vulnerability Attribution and Triage
- Ticketing (vulnerability and product application)
- Dynamic Web Application testing (DAST)
Federal Ops Stack: Services & Tools: Golden AMI w/ Compliance Drift Monitoring and Remediation

Service Components

- FIPS enabled OS images
- CIS benchmark-hardened OS
- Image compliance drift monitoring and auto-remediation/ Automation as Compliance
- Pre-installed agents:
  - Incident monitoring
  - Application Whitelisting
  - File Integrity Monitoring
  - Host-based Intrusion Detection Systems
  - Signature based Anti-virus/Anti-malware
  - Patch Management
Federal Ops Stack: Services & Tools: Incident Monitoring

Service Components

- Cloud Security Incident Monitoring
- 24x7 SOC (US Person on US Soil)
- Identify, respond and triage incidents
- Co-ordination of IR activities with product team
- Ticketing
- Incident Communication process (policies and procedures)
Federal Ops Stack: Services & Tools: Continuous Monitoring

### Monthly ConMon Activities
- Vulnerability scans
- Plan of Actions and Milestones (POA&M) entries
- Deviation Requests
- Executive Summary for authorizing official
- FedRAMP Inventory update

### Annual Assessments
- Request for information/evidence
- Pen Test Assistance
- Interview preparations
- Remediation scans

### Baseline SSP creation
- Evidence collection
- Documentation

### Significant Change Requests
- Change control board advisory support

---

* Shared Responsibility