FedRAMP Overview

Brian Conrad, FedRAMP Program Manager for Cybersecurity
Military Librarians Training Workshop
December 10, 2019

www.fedramp.gov
The Federal Risk and Authorization Management Program (FedRAMP) promotes the adoption of secure cloud services across the US Government by providing a standardized approach to security and risk assessment.
Federal law requires that Agencies authorize their information systems. FedRAMP is FISMA for cloud services and is required for all Executive Agencies.
FedRAMP Governance

- ISIMC Guidance
- Cross Agency Coordination
- FISMA Standards
- Technical Advisors
- Technical Specifications
- US-CERT Incident Coordination
- Continuous Monitoring Data Analysis
- Issuance of Binding Operational Directives
FedRAMP Authorized CSPs cover more than

5 MILLION assets available for Federal use & 1/3 of the world's internet traffic

4 security baselines to match government use to risk
- HIGH (421 controls)
- MODERATE (325 controls)
- LOW (125 controls)
- TAILORED (36 controls*)

165 Authorized Cloud Services
1,300+ Agency Reuses of Authorized Services
159 Participating Government Organizations
220+ Participating Industry Partners

POINTS OF CONNECTION

750+ Annual meetings with agencies and vendors
4,200+ Followers on Twitter
11,000+ Stakeholders on listserv
20,000+ Questions answered through info@fedramp.gov
FedRAMP Designations

FedRAMP READY

JAB

FedRAMP IN-PROCESS

AGENCY

FedRAMP AUTHORIZED

GSA
FedRAMP Baselines

FedRAMP provides 4 baselines for authorizing cloud services according to the security impact for the use of the service at Agencies

**Tailored for LI-SaaS**
- Specific to SaaS with low-risk use cases architected on FedRAMP-authorized infrastructure clouds
- Consolidated security documentation
- Enables agencies to *tailor* Low baseline to core, critical controls, commensurate with risk

**Low**
- 125 controls
- Limited adverse effect on Agency operations in the event of system breach
- Services do not store PII beyond that required for user login capability

**Moderate**
- 325 Controls
- 80% of federal use cases for cloud services
- Breach would result in serious adverse effects on Agency operations

**High**
- 421 controls
- Severe or catastrophic adverse effects on Agency operations in the event of system breach
- Common use cases include financial systems, health systems, and law enforcement or emergency services systems
FedRAMP baselines are organized according to 17 control families defined by NIST.

### NIST Control Families

- **AC** - Access Control
- **AU** - Audit & Accountability
- **AT** - Awareness & Training
- **CM** - Configuration Management
- **CP** - Contingency Planning
- **IA** - Identification & Authentication
- **IR** - Incident Response
- **MA** - Maintenance
- **MP** - Media Protection
- **PS** - Personnel Security
- **PE** - Physical & Environment Protection
- **PL** - Planning
- **RA** - Risk Assessment
- **CA** - Security Assessment & Authorization
- **SC** - System & Communications Protection
- **SI** - System & Information Integrity
- **SA** - System & Services Acquisition

### Example Control Areas

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SC-13</td>
<td>IA-2</td>
<td>RA-5</td>
<td>CA-3</td>
<td>CM-6</td>
</tr>
<tr>
<td>SC-8</td>
<td></td>
<td>SI-2</td>
<td>SC-7</td>
<td>SI-2</td>
</tr>
<tr>
<td>SC-28</td>
<td></td>
<td></td>
<td>AC-4</td>
<td></td>
</tr>
</tbody>
</table>

- **Encryption**
  - Helps ensure that only authorized parties can understand/decode the information.

- **Identification & Authentication**
  - Reduces the likelihood of account compromise and helps ensure that only the people who should have access to information do.

- **Vulnerability Scanning & Malicious Code**
  - Helps ensure vendors have what they need in place to continually respond to evolving threats.

- **Boundary Protection & System Interconnections**
  - Ensures federal data is protected from end to end and maintains a secure perimeter.

- **Configuration Management**
  - Provides visibility into what is changing and the impact of those changes.
Federal security policy requires all systems to be authorized based on risk.

FedRAMP standardizes the process for cloud, providing:

**DO ONCE, USE MANY TIMES**
Doing security authorizations right the first time allows Agencies to re-use work and eliminate duplicative efforts

**TRANSPARENCY**
Increased collaboration and creation of a community among the US Government and vendors that did not exist before, establishing the FIRST government-wide FISMA program

**VALIDATED WORK**
FedRAMP validates security authorizations to ensure that there is uniformity among security packages

**CENTRAL SHARING**
Centralized repository where Agencies can request access to security packages for expedient authorizations
- Provides a searchable database of all cloud services with a FedRAMP designation
- Enables researching of Authorized services and Third Party Assessment Organizations (3PAOs)
- Provides contact information and service descriptions for all cloud services
Questions?

Learn more at www.Fedramp.gov
Contact us at info@fedramp.gov

@FEDRAMP