FedRAMP
Federal Risk and Authorization Management Program
Industry Day

Cloud SLA Workshop

Matt Goodrich

FedRAMP Program Manager

GSA

Overview

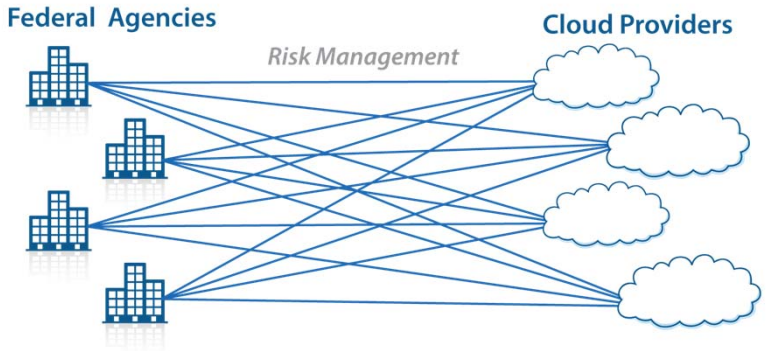
- What is FedRAMP?
- Relationship between NIST 800-53 FedRAMP controls and SLAs
- Opportunity areas for SLAs
- Considerations for SLAs from FedRAMP perspective

FedRAMP is FISMA for Cloud

Why is FedRAMP needed if FISMA has been in place since 2002?

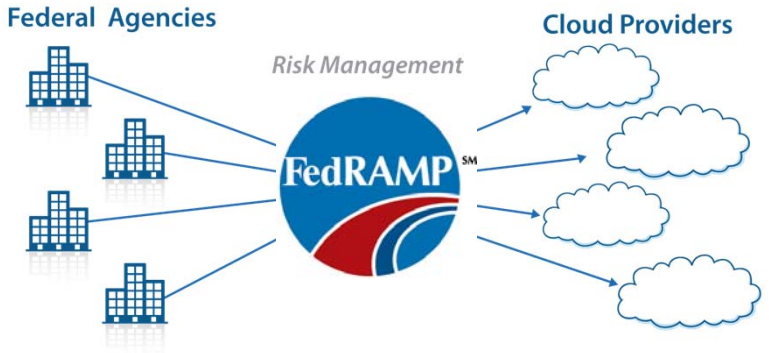
Problem:

- A duplicative, inconsistent, time consuming, costly, and inefficient cloud security risk management approach with little incentive to leverage existing Authorizations to Operate (ATOs) among agencies.

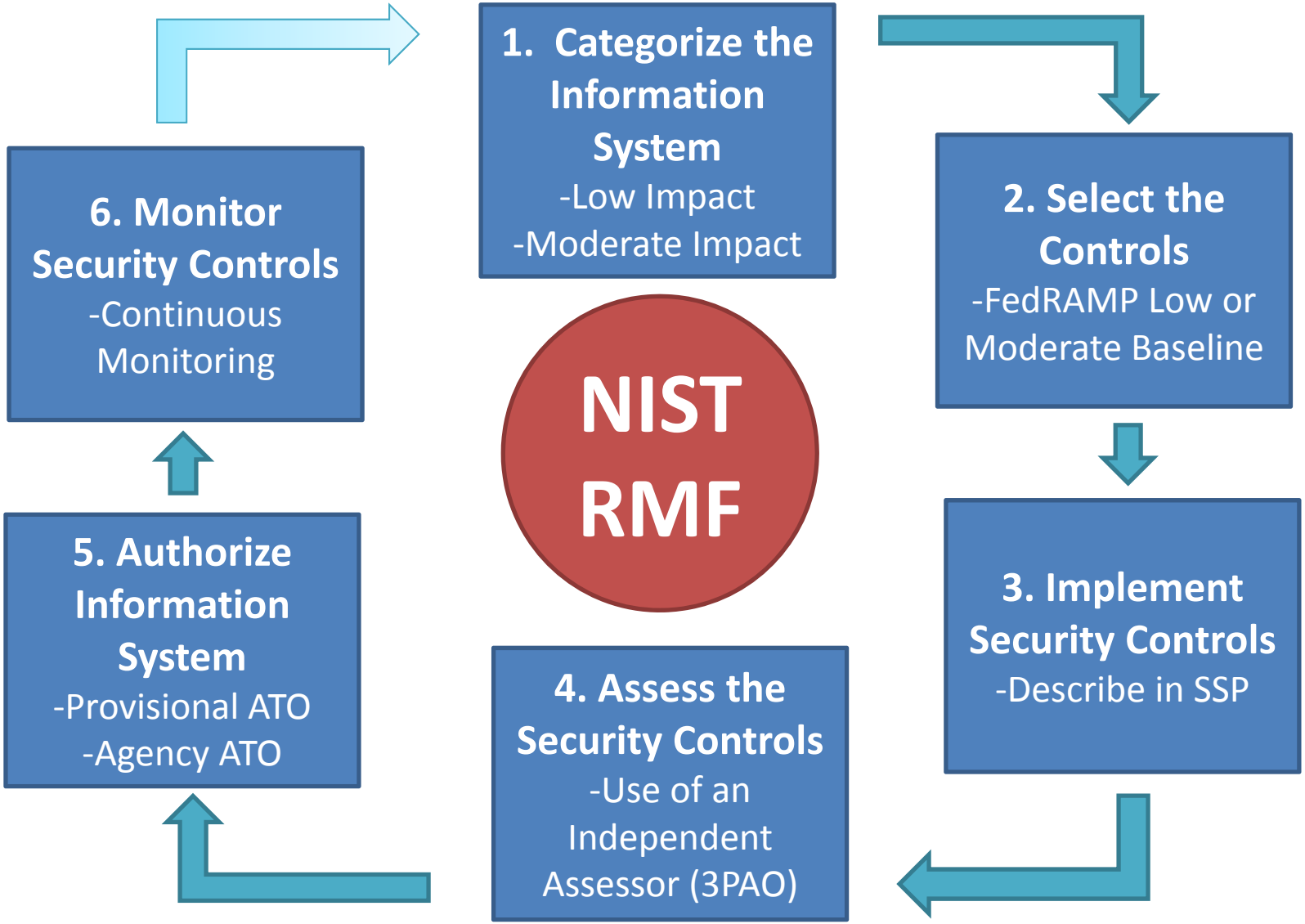


Solution: FedRAMP

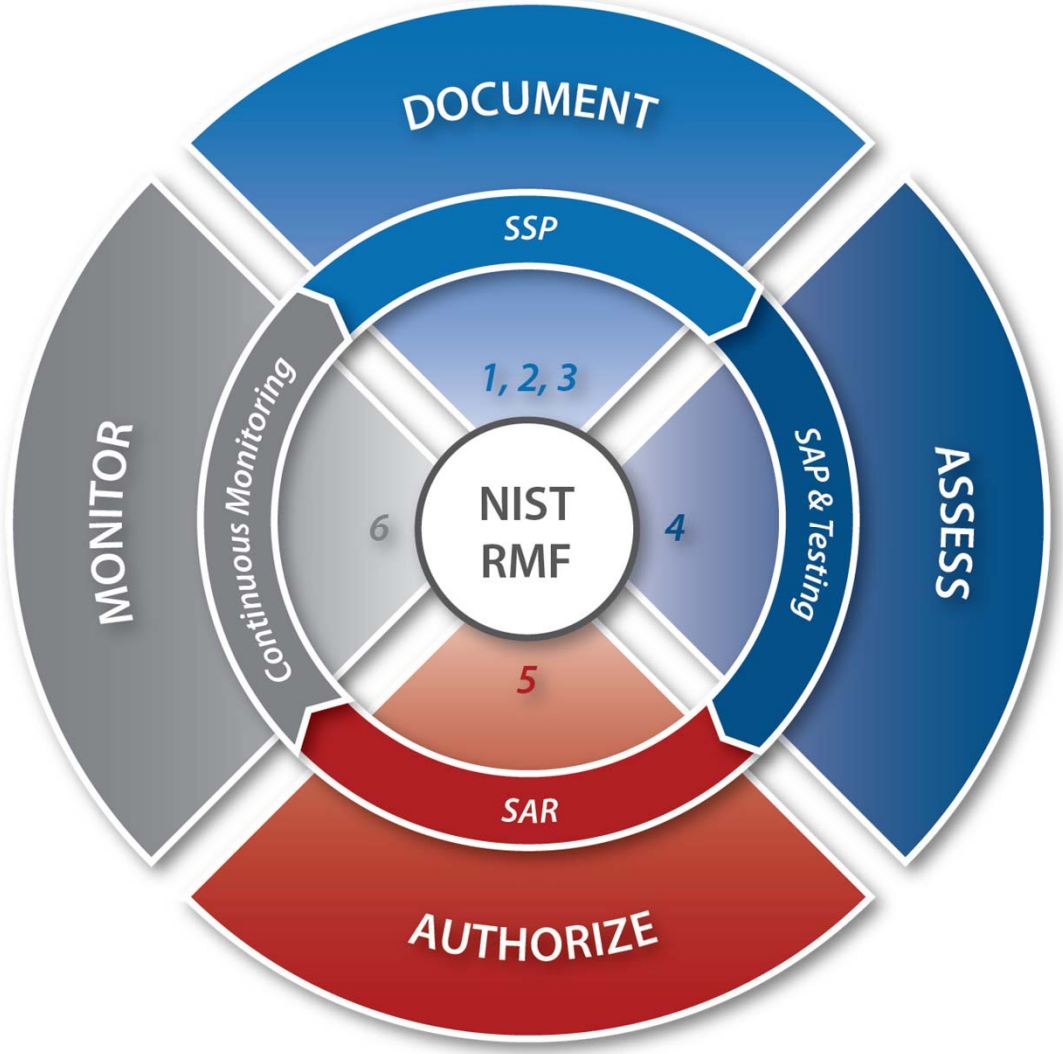
- Uniform risk management approach
- Standard set of approved, minimum security controls (FISMA Low and Moderate Impact)
- Consistent assessment process
- Provisional ATO



FedRAMP Relationship to the NIST Risk Management Framework



FedRAMP Security Assessment Framework (SAF) and NIST Risk Management Framework



Overview: FedRAMP SAF Standardizes RMF for Cloud

FedRAMP SAF Process	NIST SP 800-37 Step	FedRAMP Standard
Document	1. Categorize System	Low and Moderate Impact Levels
	2. Select Controls	Control Baselines for Low and Moderate Impact Levels
	3. Implement Security Controls	Use FedRAMP templates Implementation Guidance in "Guide to Understanding FedRAMP"
Assess	4. Assess the Security Controls	FedRAMP accredits 3PAOs 3PAOs use standard process and templates
Authorize	5. Authorize the System	ATOs with JAB P-ATO or Agency ATO CSP Supplied packages
Monitor	6. Continuous Monitoring	Use Continuous Monitoring Strategy and Guide

FedRAMP Controls and SLAs

FedRAMP Controls

- FedRAMP defines the security control implementations
- Based on the stated requirements within 800-53
- This is a view of ***capabilities*** of a provider in terms of security
- Cloud providers:
  - Document the implementation
  - Test the implementation
  - Review any risks associated with that implementation

SLAs

- SLA's really relate to the ***functionality*** of the security controls
- They define what service levels and deliverables customers should expect from the use of a cloud system

Opportunity Areas for SLAs

Functionality

- Focus on what you are getting out of the capabilities
- FedRAMP ensures the capabilities are there, SLAs determine what an agency can get out of that capability
- Capability also does not equal implemented functionality – sometimes agencies have to pay for this option

Examples

- Recovery time for disaster recovery
- Backup of systems
- Audit logs
- Uptime
- Bandwidth

Considerations for SLAs

Measurements / Metrics

- Clear definitions
  - e.g. what constitutes downtime
- How does customer have insight to performance?
  - e.g. dashboards, notifications, etc.

Outsourcing Risk

- SLA's essentially place risk from customer to provider
- Need to define consequences for failing to meet SLA
- Variability in SLAs results in higher cost
  - e.g. cloud providers are effective at providing due to economies of scale, getting higher performing SLAs likely result in higher cost

Inheritance

- SLAs can only be as good as the base service SLA
  - e.g. a SaaS cannot have a DR time of 4 hours if the IaaS it resides on has a DR time of 8 hours

Questions and Answers

For more information, please contact us or visit us the following website:

www.FedRAMP.gov
Email: info@fedramp.gov

Follow us on twitter @ FederalCloud