



Introduction to the Federal Risk and Authorization Management Program (FedRAMP)

8/2/2015

Presented by: FedRAMP PMO

www.fedramp.gov



Today's Training

- Welcome! This training session is part one of the FedRAMP Training Series.

- 1. Introduction to the Federal Risk and Authorization Program (FedRAMP) – 100A**

2. FedRAMP System Security Plan (SSP) Required Documents
 3. FedRAMP Review and Approve Process
 4. Rev 3 to Rev 4 Transition
 5. Third Party Assessment Organization (3PAO) Specific Training
 6. Security Assessment Report (SAR) and Security Assessment Plan (SAP) Overview
 7. Significant Change Training for CSPs
- The goal of the FedRAMP Training Series is to provide a deeper understanding of the FedRAMP program and the level of effort required to satisfactorily complete a FedRAMP assessment.



Training Objectives

At the conclusion of this training session the participant should understand:

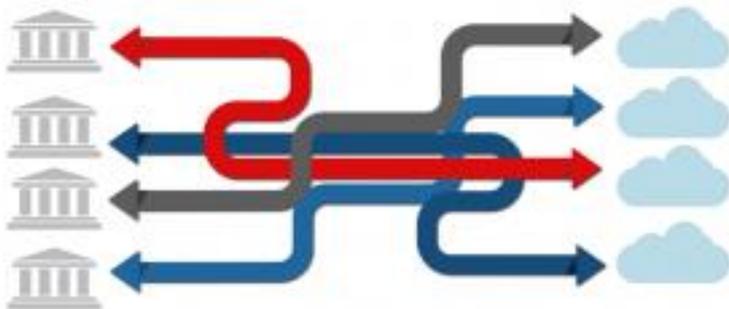
- FedRAMP U.S. Federal Government policy and legal framework
- FedRAMP Governance
- FedRAMP Partners
- Goals and benefits of FedRAMP
- Relationship between FedRAMP and the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)
- Options for Cloud Service Providers (CSPs) to achieve authorization
- Requirements for CSPs to become FedRAMP compliant



FedRAMP Overview

- FedRAMP was established via an OMB Memo in December 2012
- FedRAMP is the first government-wide security authorization program for FISMA – mandatory for all agencies and all cloud services
- FedRAMP’s framework is being modeled in other government security programs and by other countries (UK, EU, China)
- FedRAMP’s focus is to ensure the rigorous security standards of FISMA are applied while introducing efficiencies to the process for cloud systems (key of which is re-use)
- 700+ cloud systems that meet FedRAMP requirements
- \$70M in cost avoidance through reuse of FedRAMP authorizations

Before FedRAMP



With FedRAMP

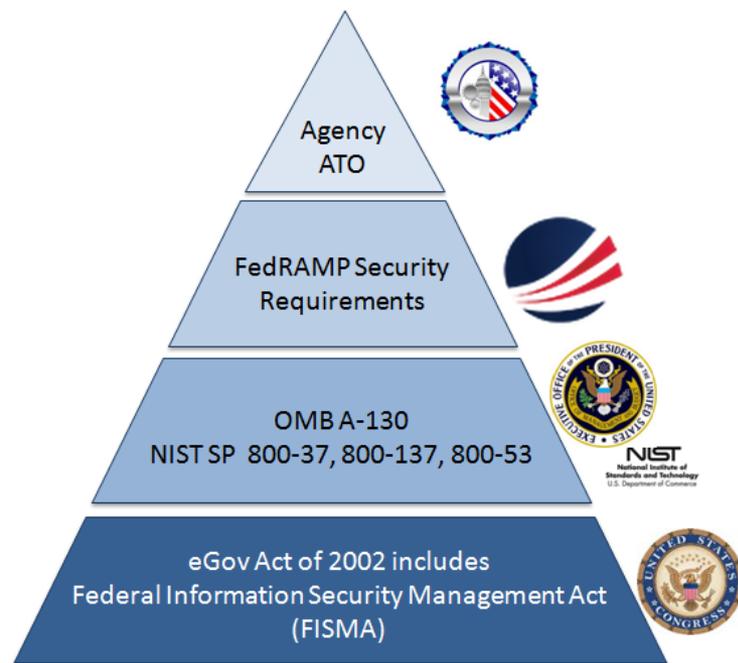




FedRAMP Federal Policy and Legal Framework

FedRAMP fits within the same framework agencies are using currently to provide security authorizations of IT services

- FedRAMP is how agencies implement FISMA for use of cloud based IT products and services
- Essentially, FedRAMP is a supplemental policy to OMB A-130 for security authorizations.
- Agencies are still required to grant individual authorizations





FedRAMP Governance

Joint Authorization Board (JAB):

- Has a team of Technical Representatives (TRs) similar to a Chief Information Security Officer (CISO)
- Under the TRs, there is a team of security staff that reviews security packages and recommends a Provisional Authorization to Operate (P-ATO)
- TRs also provide policy guidance

NIST:

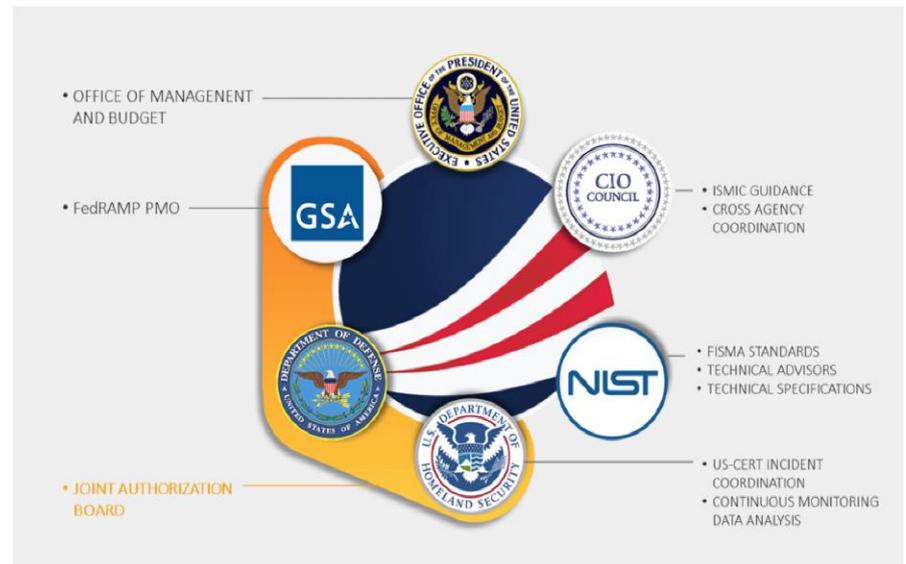
- Provides technical assistance to the Third Party Assessment Organizations (3PAO) process
- Maintains FISMA standards
- Establishes technical standards

Federal CIO Council:

- Coordinates cross agency communications

DHS:

- Monitors and reports on security incidents and provides monitoring
- Updates Federal standards for FISMA reporting





Success Depends on all Partners



FEDRAMP PMO:

- Provide a unified process for all agencies to follow
- Work with the JAB for prioritized vendors to achieve authorizations with an efficient review schedule
- Support CSPs and agencies through the process – regardless of which path they go
- Maintain secure repository of FedRAMP ATOs to enable reuse



AGENCIES:

- Conduct quality risk assessments that can be reused
- Integrate the FedRAMP requirements in to agency specific policies/procedures
- Deposit ATO documents in the FedRAMP secure repository



CSPs:

- Submit quality documentation in support of their FedRAMP application
- Encourage customers to reuse existing ATOs for their products



3PAOs:

- Maintain independence as part of the quality assurance process
- Provide quality assessments



FedRAMP Goals

The Goals of FedRAMP are:

Accelerate the adoption of secure cloud solutions through reuse of assessments and authorizations

Ensure consistent application of existing security practices

Improve real-time security visibility

Enhance transparency between the Government and CSPs



Increase consistency and confidence in the security of cloud solutions using NIST and FISMA defined standards

Increase automation and near real-time continuous monitoring

Provide a uniform approach to risk-based management

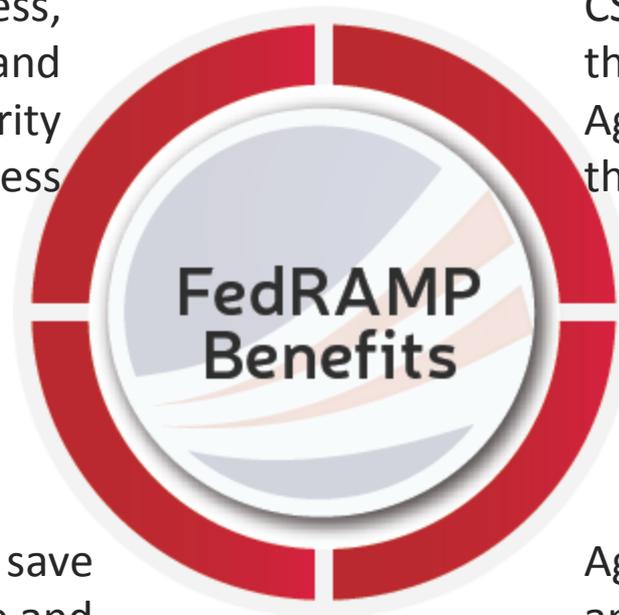


FedRAMP Benefits

The Benefits to Agencies and CSPs using FedRAMP are:

Improves the trustworthiness, reliability, consistency, and quality of the federal security authorization process

CSPs gain one authorization that is available to multiple Agencies, further increasing their federal footprint

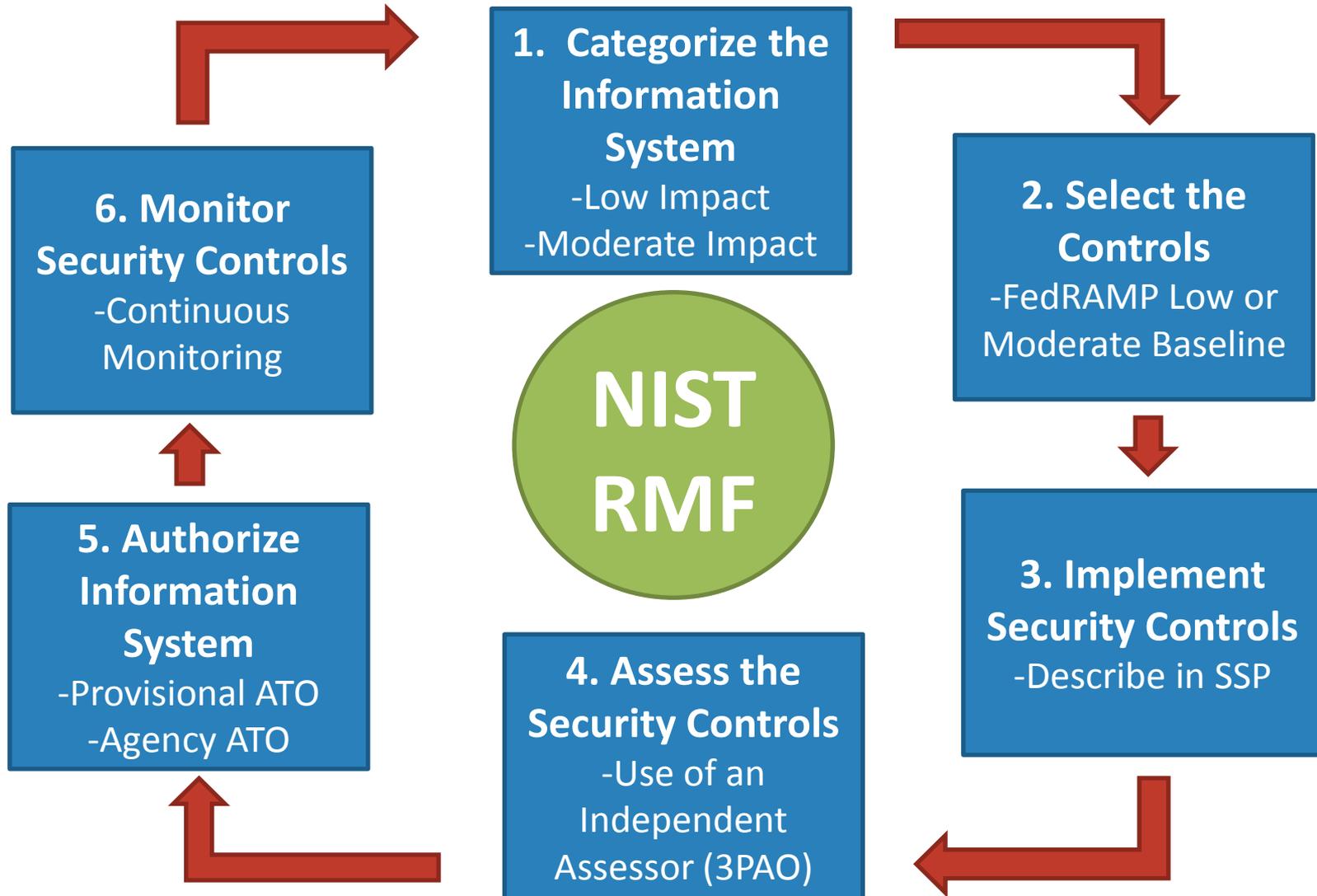


Agencies and CSPs save significant cost, time and resources – "do once, use many times"

Agencies are able to re-use and share existing security assessments



FedRAMP Relationship to the NIST Risk Management Framework (RMF)





FedRAMP SAF/NIST RMF Comparison

FedRAMP SAF Process	NIST SP 800-37 Step	FedRAMP Standard
Document	1. Categorize System	Low and Moderate Impact Levels
	2. Select Controls	Use FedRAMP 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
Monitor	6. Continuous Monitoring	Use Continuous Monitoring Strategy and Guide



FedRAMP Authorization Paths

JAB Provisional Authorization to Operate (P-ATO)

- DHS, DoD, and GSA CIOs rigorously review CSP packages for an acceptable risk posture using a standard baseline approach
- Provides provisional authorizations to operate for use across the federal government

Agency Authorization to Operate (ATO)

- A CSP may submit the appropriate documentation to the FedRAMP PMO and to an agency
- Agencies have varying levels of risk acceptance however, they may grant an ATO
- Packages are reviewed by at least one agency and determined to be FedRAMP compliant by the reviewing agency resulting in an Agency ATO

CSP Supplied

- CSPs may supply a security package to the FedRAMP PMO for prospective agency use
- CSPs complete the FedRAMP SAF independently, instead of through the JAB or through a federal agency
- CSPs will not have an authorization at the completion, but will have a FedRAMP compliant package available for leveraging



FedRAMP Compliance Requirements

A cloud system is compliant with FedRAMP if it meets the following requirements:

The system security package has been created using the required FedRAMP templates

A Provisional Authorization, and/or an Agency ATO, has been granted for the system

The system meets the FedRAMP security control requirements

An authorization letter for the system is on file with the FedRAMP Program Management Office

The system has been assessed by an independent assessor

The CSP maintains the continuous monitoring requirements of FedRAMP



Summary

- FedRAMP provides a standardized risk based approach for the Federal Government to leverage cloud services
- FedRAMP accelerates the adoption of secure cloud solutions through reuse of assessments and authorizations
- FedRAMP was built on the NIST RMF and compliance with FedRAMP ensures that the cloud service meets all FISMA requirements
- There are three paths to FedRAMP compliance: JAB P-ATO, Agency ATO, and CSP Supplied