AGENCY GUIDE FOR FEDRAMP AUTHORIZATIONS

HOW TO FUNCTIONALLY REUSE AN EXISTING AUTHORIZATION

Version 2.0

December 7, 2017

FedRAMP

REVISION HISTORY

Date	Version	Page(s)	Description	Author
08/05/2015	1.0	All	Initial Publication	FedRAMP PMO
06/06/2017	1.0	Cover	Updated logo	FedRAMP PMO
12/7/2017	2.0	All	Updated to the new template	FedRAMP PMO

HOW TO CONTACT US

Questions about FedRAMP or this document should be directed to info@fedramp.gov.

For more information about FedRAMP, visit the website at http://www.fedramp.gov.

TABLE OF CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

All U.S. federal information systems must comply with the Federal Information Security Management Act of 2002 (FISMA). The Federal Risk and Authorization Management Program (FedRAMP) applies FISMA to cloud computing systems. FedRAMP more easily allows agencies to reuse existing authorizations. This document describes the process by which agencies can reuse existing authorizations to reduce their overall time to grant an authorization and begin using a cloud service.

1. BACKGROUND AND INTRODUCTION

All cloud systems must comply with the Federal Information Security Management Act of 2002 (FISMA). There are certain complexities of cloud systems that create unique challenges for complying with FISMA. The Federal Risk and Authorization Management Program (FedRAMP) was designed to assist agencies in meeting FISMA requirements for cloud systems.

FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring based on cloud computing. Using a "do once, use many times" paradigm for FISMA compliance activities, FedRAMP reduces the cost of FISMA compliance and enables government entities to secure government data and detect cyber security vulnerabilities at unprecedented speeds.

This FedRAMP Agency Authorization to Operate (ATO) guide is specific to U.S. Federal Departments and Agencies and provides guidance and the understanding required to authorize an agency's application when reusing a FedRAMP-compliant cloud service provider. By reusing existing FedRAMP packages, agencies can reap significant financial savings and can implement new systems quickly and securely.

1.1. Assumptions

The design of this document guides government customers with their reuse of a FedRAMP security package to meet FISMA authorization requirements. It is NOT intended to assist with the creation of the initial Cloud Service Provider (CSP) authorization[1]. This document assumes the agency is relying on and reusing an existing FedRAMP security package. A listing of FedRAMP security packages can be found on the FedRAMP website, www.fedramp.gov.

Additionally, this document is written with the following assumptions:

- The reader understands FISMA.
- The reader understands cloud computing.
- The reader is an agency looking to reuse a CSP with an existing FedRAMP authorization.
- The reader understands the intended use and responsibilities associated with the cloud service they are authorizing.

This guide is NOT designed to address certain related topics as noted below:

- This guide is not an instruction manual on FISMA.
- This guide is not an educational resource on the complexities of cloud computing.
- This guide does not advise agencies on the technical implementation of security controls.

[1] For assisting with completing an initial CSP authorization, agencies should review the *FedRAMP Security Assessment Framework* available on www.FedRAMP.gov.

- This guide does not advise agencies on how to build a cloud.

Additional information on the above topics can be found elsewhere, including www.fedramp.gov and the National Institute of Standards and Technology (NIST) websites. Section 6 contains references to some of the applicable standards and guidance.

1.2. Authorities

On December 9, 2010, the Office of Management and Budget (OMB) released *25 Point Implementation Plan to Reform Federal Information Technology Management*. Point 3 under this plan created the Cloud First Policy, which requires Agencies to use cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. In follow-up to the 25 Point Plan, on February 8, 2011, OMB released the *Federal Cloud Computing Strategy,* giving agencies practical guidance on considerations and practical methodologies for moving to the cloud. Finally, on December 8, 2011, OMB released the *Security Authorization of Information Systems in Cloud Computing Environments* – also known also as the FedRAMP Policy Memo – mandating that for all agency use of cloud services, the agencies use FedRAMP for their risk assessments, security authorizations, and granting of ATOs, and ensure applicable contracts require CSPs to comply with FedRAMP requirements.

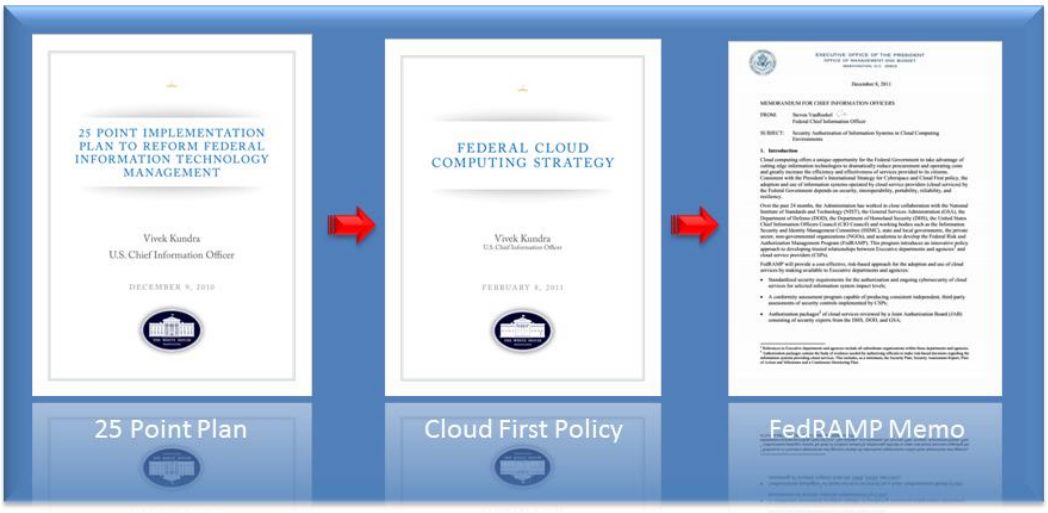

Figure 1: Evolution of Government Cloud Policy

2. OVERVIEW OF SECURITY AUTHORIZATION RESPONSIBILITIES

Any system an agency uses must comply with FISMA. FedRAMP ensures that any use of cloud services makes meeting FISMA more transparent and enables easier reuse of the base cloud services across

agencies. Agencies need to think of cloud services as the building block upon which their end service exists. This building block offers varying degrees of completeness depending on if an agency is using an Infrastructure, Platform or Software as a Service. Regardless of the service being used, an Agency's ATO must include the entire application –and there will always be responsibility differences between CSPs and agencies as shown below in Figure 2.

Figure 2 shows how an agency instance completes the overall security responsibilities, depicting the overall authorization boundary when using a cloud service. The agency instance represents the agency's responsibility when completing a security authorization – whether it is unique application needs, customization, or required integration with agency back ends. An example of this would be multi-factor authentication. The CSP would address the capabilities for multi-factor authentication, but the agency instance would have to fully implement this for each agency user.

Figure 2: Security Authorization Boundary

A FedRAMP system can be reused from agency to agency. The CSP block in Figure 2 represents those services that each agency customer uses and leverages from a FedRAMP authorization. In this view, if another customer purchases the same services, then the next agency would require to complete the agency instance, but would not have to do anything in the CSP block.

When granting an authorization at an agency for specific services, an agency must authorize both the CSP and the agency instance portions of the stack. In this case, the CSP stack already meets the FedRAMP requirements, so an agency instance must meet the agency's organizational policies for FISMA[2] authorizations.

FedRAMP recognizes that agencies have their own programs for complying with FISMA based on specific agency requirements. Agency's use of cloud aligns with FISMA processes since FedRAMP is based on the NIST Special Publication (SP) 800 series documents. The remainder of this Agency Guide walks agency users through reuse of a FedRAMP package within each of the NIST Risk Management Framework (RMF) steps to complete the security authorization requirements and boundary.

[2] It is important to note that the implementation of the agency instance is not necessarily required to meet FedRAMP requirements. FedRAMP is required for cloud services. If the agency implementation is not a cloud service itself, then the agency need not use the FedRAMP process or templates when documenting and assessing the agency instance portion of the application stack.

3. APPLYING FEDRAMP TO THE NIST RMF

The FedRAMP Security Assessment Framework process is based on NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. The NIST RMF, shown below in Figure 3, describes the six risk management steps required of U.S. government systems, including cloud systems. The following sections discuss the RMF-compliant FedRAMP steps an agency must take when leveraging a compliant CSP package for the authorization of the agency instance portion of the authorization boundary.

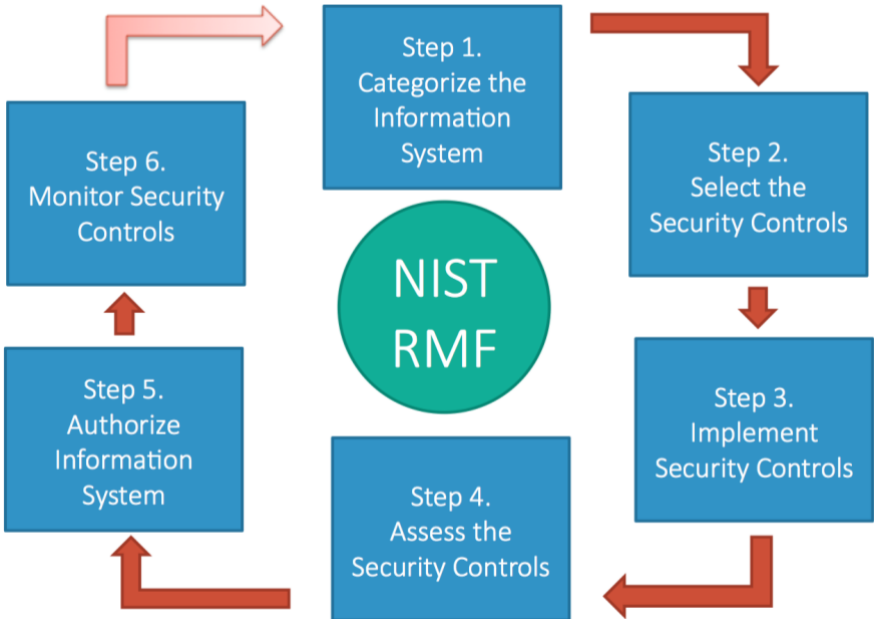

Figure 3: NIST SP 800-37, Rev 1 - RMF

3.1. Step 1: Categorize

The first step in Figure 3, the RMF, is to categorize the information system. This categorization is based on the NIST Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199). Cloud systems require the same categorization determination that agencies use for traditional on-premises systems. The categorization methodology is described in detail in FIPS 199.

To determine a system's categorization, agencies first determine what information types they plan on storing, processing, or transmitting on the cloud system. After determining information types, agencies determine the FIPS 199 Low, Moderate, or High sensitivity categorization of the information system. The agency is required to document their FIPS 199 categorization using their respective agency processes and procedures.

Determining the FIPS 199 categorization of the proposed system allows agencies to appropriately select a CSP that will best fit their security requirements. For example, if the proposed system will process FIPS 199 Moderate data, the cloud service the agency selects also must be categorized at Moderate to meet the designated system requirements. With an understanding of the categorization of the data, agencies can determine a system categorization (Low, Moderate, or High) and proceed with the selection of security controls.

3.2. Step 2: Select

The second step of Figure 3, the RMF, is to select the security controls. FedRAMP has a pre-determined baseline of controls that CSPs must meet. Agencies should do an analysis of the FedRAMP baseline to adequately understand what controls a CSP will be required to implement.

Based on agency policies, standards, and guidelines, agencies then select the security controls required for the system based on the categorization level determined in Step 1. The agency selection of security controls should be performed based on the organizational risk tolerance and system data/mission. Agencies then must analyze agency-specific controls compared to the FedRAMP baseline. Agencies must address any delta of controls outside the FedRAMP baseline.

3.3. Step 3: Implement

RMF Figure 3, Step 3 is where cloud computing intersects the standard FISMA process. In Step 2, the agency identified the required security controls for the desired information system. When reusing a FedRAMP compliant system, the cloud system has already implemented a large portion of these. However, there is a delta of controls that an agency will have to implement either fully or partially – or that may not be applicable.

The first step in the implementation phase is to identify what controls the agency needs to implement, and what the cloud provider already implements. The easiest way to begin this is to review the CSP's FedRAMP Control Implementation Summary (CIS) document. This document provides a listing of all the controls the CSP implements as well as the controls that are the customer's responsibility, and any shared responsibilities. This will allow an agency to quickly identify and list the controls that are the agency's responsibility to implement[3].

[3] It may be possible for the agency to negotiate with the CSP to implement some of the agency-specific controls. Regardless, these controls are still agency-specific controls.

After identifying the controls which are an agency's responsibility to implement, an agency must actually implement the security controls for which it is responsible. This process is faster than fully implementing controls from a new system as a majority of the controls are covered by the CSP.

As a note, not all controls have a clean delineation of who is responsible; some require both an agency and a CSP to have some sort of action to fully implement. These controls are "shared controls" and have two types of requirements for agencies:

- Independent shared controls:
  - These controls are provided by both the CSP and the agency.
  - An example of a shared independent control is Security Awareness Training. Both entities, the agency and the CSP, need to ensure that their users take Security Awareness Training.
- Dependent shared controls:
  - These controls are shared between the agency and CSP and are dependent on each other.
  - An example of a dependent shared control is two-factor authentication where the CSP implements two-factor authentication and makes hard tokens available to the agency customer. It is up to the agency to distribute the tokens to its users and also to require their users to use the tokens.

3.4. Step 4: Assess

Step 4 of Figure 3, the RMF, is to assess the implementation of the security controls to identify any potential risks associated with the control implementations. This is often referred to as security control assessment or testing. To make an authorization decision, all security controls must be assessed. Using the list of CSP and agency-specific controls identified in Step 3, Figure 3, the agency now needs to assess the agency-specific controls – inclusive of any agency specific shared controls.

The CSP controls, listed in the CSP CIS, are independently assessed and the results are part of the FedRAMP security package. The agency must augment that assessment with the assessment of the agency-specific controls. Agency-specific controls are assessed in accordance with agency policy by an independent assessor.

The combination of security assessment results from the FedRAMP package and the agency-specific control assessment constitutes a comprehensive assessment of the Authorization Boundary as represented in Figure 2. The combined assessment results are sufficient to make an authorization decision.

3.5. Step 5: Authorize

Agencies reusing FedRAMP CSPs are required to authorize the entire cloud stack before processing, storing, or transmitting government data. Agencies should review the security assessment information

for the combined agency-specific controls along with the CSP controls within the FedRAMP security package.

Combining the agency-specific assessment of controls and risk review with the FedRAMP security package does introduce some complexities. When reusing a FedRAMP security package, the assessment that was completed could have the potential of being completed months or in some cases years ago. When this is the case agencies must use continuous monitoring reports and data to detail he most recent security posture. FedRAMP recommends that agencies review the CSPs most recent Security Assessment Report and at least the last 90 days of Continuous Monitoring (ConMon) deliverables to have a full understanding of the CSPs current risk posture. This allows an agency to better understand the risk posture of the CSP-implemented security controls.

Agencies must combine the security risks associated with the CSP security controls with the agency-specific assessment risks. By combining these two assessments and associated risks, it presents a complete picture of the risks associated with the security authorization boundary portrayed in Figure 2. This combination provides the basis for the authorizing official to determine the risk and grant an ATO.

Once an ATO is granted, the agency is required to provide the FedRAMP Program Management Office (PMO) with a copy of the ATO memo[4]. The ATO memo enables the FedRAMP office to contact the appropriate agency organization in the event that FedRAMP obtains relevant security information related to the CSP responsibilities that should be disseminated to the CSP customers.

3.6. Step 6: Monitor

ConMon keeps the security authorization package timely and provides information to authorizing officials about the current risk posture of an environment. ConMon includes operational visibility related to the continued implementation of the security controls, change control for any changes to the system, and incident response for how to handle any potential incidents or breaches of a system's security.

FedRAMP dictates how CSPs maintain the security of their system through ConMon using the *FedRAMP Continuous Monitoring Strategy and Guide.* CSPs upload these results to the FedRAMP secure repository for agencies to review. Agencies are encouraged to use the *FedRAMP Guide to Multi-Agency Continuous Monitoring* to jointly review and analyze the CSP portion and responsibilities of ConMon.

Agencies are required to meet their organizational policies and procedures for ConMon on the agency-specific security controls. Similar to the authorization step above, the agency uses the combined results of the ConMon – CSP ConMon and agency-specific controls – to ensure the security risk posture of the

[4] There is an ATO letter template agencies can use available on www.FedRAMP.gov. If agencies do not use the template letter, agencies must include the unique elements within that template ATO letter to be accepted by the FedRAMP PMO.

system is acceptable. Performance of ConMon activities occurs on a monthly basis. At a minimum, this includes monthly reviews of vulnerability scan data and Plan of Action and Milestones (POA&M) updates. The agency must follow their agency's policies for reporting and monitoring information systems when evaluating and reporting the risk posture. Obtaining Security Packages for Review

After reviewing the list of available FedRAMP-compliant CSP packages on the FedRAMP Marketplace, agencies may contact FedRAMP PMO to request access to specific CSP Security Packages available in the FedRAMP secure repository.

3.7. Requesting Access

The FedRAMP Marketplace at www.fedramp.gov provides a listing and a description of the CSPs that have FedRAMP-compliant packages. The FedRAMP PMO has a prescribed process for allowing access to Security Packages and the FedRAMP secure repository. All package reviewers must have a .gov or a .mil email address.

4. OBTAINING APPROVALS FOR ACCESS

Once a prospective Security Package reviewer determines which package they would like to review, the next step is to download the FedRAMP Package Access Request Form (available on www.fedramp.gov) and fill the requisite fields. The form needs to be reviewed and signed internally at the reviewer's home agency by the reviewer and the reviewer's Chief Information Security Officer, or Authorizing Officer before submitting the request to the FedRAMP PMO.

Once the authority within the requesting agency signs the form, prospective package reviewers can scan the signed access request form and email it to info@fedramp.gov. The FedRAMP PMO will review the form for correctness and completeness. All information on the form is subject to verification.

The prospective Security Package reviewer is notified when the reviewer's request is approved or denied. After notification of access approval, Security Package reviewers will receive instructions regarding how to access the FedRAMP Package. Completion and submittal of a new FedRAMP Package Access Request Form is required for each package.

5. RESOURCES

Below are some FedRAMP resources that may be helpful throughout this FedRAMP Agency ATO process.

- Creating Effective Cloud Computing Contracts for the Federal Government
  https://www.fedramp.gov/files/2015/03/Cloud-Best-Practices.pdf

- FedRAMP Standard Contract Clauses
  https://www.fedramp.gov/files/2015/03/FedRAMP_Standard_Contractual_Clauses_062712_0.pdf

- FedRAMP Control Specific Contract Clauses
  https://www.fedramp.gov/files/2015/03/FedRAMP-Control-Specific-Contract-Clauses-v2.1.docx

- FedRAMP Policy Memo
  https://www.fedramp.gov/files/2015/03/fedrampmemo.pdf

- FedRAMP Program Documents (including the FedRAMP Security Assessment Framework)
  http://www.fedramp.gov/resources/documents/

- Guide to Understanding FedRAMP
  https://www.fedramp.gov/files/2015/03/Guide-to-Understanding-FedRAMP-v2.0-4.docx

6. APPLICABLE REQUIREMENTS, STANDARDS, AND GUIDANCE

The most current approved version of the following requirements, standards, and guidance are applicable to the FedRAMP program, regardless of the version noted in this section:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*
- NIST SP 800-27, Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-53, Revision 4, as amended, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*

- NIST SP 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*
- NIST SP 800-145, *The NIST Definition of Cloud Computing*
- NIST SP 800-46, *Cloud Computing Synopsis and Recommendations*

APPENDIX A FedRAMP ACRONYMS

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website Documents page under Program Overview Documents.

(https://www.fedramp.gov/resources/documents-2016/)

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.