Chapter Three: Potential Assessment & Authorization Approach

3. Potential Assessment & Authorization Approach

3.1. Introduction

Cloud computing presents a unique opportunity to increase the effectiveness and efficiency of the A&A and Continuous Monitoring process for Federal Agencies. The nature of cloud computing systems does not allow Federal Agencies to enforce their own unique security requirements and policies on a shared infrastructure – as many of these unique requirements are incompatible. Hence, cloud computing provides an opportunity for the Federal Agencies to work together to create a common security baseline for authorizing these shared systems.

The implementation of a common security baseline requires a joint approach for the A&A and Continuous Monitoring process. Any joint approach to this process requires a coordinated effort of many operational components working together. These operations need to interact/interplay with each other to successfully authorize and monitor cloud systems for government-wide use.

FedRAMP operations could potentially be executed by different entities and in many different models. However, the end goal is to establish an on-going A&A approach that all Federal Agencies can leverage. To accomplish that goal, the following benefits are desired regardless of the operating approach:

- Inter-Agency vetted Cloud Computing Security Requirement baseline that is used across the Federal Government;
- Consistent interpretation and application of security requirement baseline in a cloud computing environment;
- Consistent interpretation of cloud service provider authorization packages using a standard set of processes and evaluation criteria;
- More consistent and efficient continuous monitoring of cloud computing environment/systems fostering cross-agency communication in best practices and shared knowledge; and
- Cost savings/avoidance realized due to the “Approve once, use often” concept for security authorization of cloud systems.

FedRAMP operations could be conducted under many delivery models. The Federal Cloud Computing Initiative (FCCI) has focused on exploring three models in particular. The three models for assessment that have been vetted within Government and Industry are:

- A centralized approach working through a FedRAMP program office;
- A federated model using capabilities of multiple approved agency centers; and
- Some combination of the above that combines public and private sector partners.

Preliminary vetting of the three models focused on finding a model that best met the goals of this endeavor as mentioned above. As a result of vetting the models with government and industry stakeholders, this chapter presents FedRAMP operations through a centralized program office context. However, the government is seeking your input, knowledge, and experience as to the best model for FedRAMP operations that deliver upon the described benefits and encourage you to actively engage and contribute with substantive comments.

3.2. Overview

Background

The Federal Government is increasingly using large shared and outsourced systems by moving to cloud computing, virtualization, and datacenter/application consolidation. The current method of conducting risk management of shared, outsourced, cloud computing systems on an agency-by-agency basis causes duplication of efforts, inefficiencies in sharing knowledge, best practices and lessons learned in authorizing and ongoing monitoring of such systems, and the unnecessary cost from repetitive work and relearning.

In order to address these concerns, the U.S. Chief Information Officer (U.S. CIO) established a government-wide Federal Risk and Authorization Management Program (FedRAMP) to provide joint security assessment, authorizations and continuous monitoring of cloud computing services for all Federal Agencies to leverage.

Purpose

The objective of FedRAMP is threefold:

- Ensure that information systems/services used government-wide have adequate information security;
- Eliminate duplication of effort and reduce risk management costs; and
- Enable rapid and cost-effective procurement of information systems/services for Federal agencies.

Benefits

Joint authorization of cloud computing services provides a common security risk model that can be leveraged across the Federal Government. The use of a common security risk model provides a consistent baseline for Cloud based technologies across government. This common baseline will ensure that the benefits and challenges of cloud based technologies are effectively integrated across the various cloud computing solutions currently proposed within the government. The risk model will also enable the government to "approve once and use often" by ensuring other agencies gain the benefit and insight of the FedRAMP's Authorization and access to service provider's authorization packages.

By providing a unified government-wide risk management for enterprise level IT systems, FedRAMP will enable Agencies to either use or leverage authorizations with:

- An interagency vetted approach;
- Consistent application of Federal security requirements;
- Consolidated risk management; and
- Increased effectiveness and management cost savings.

3.3. Governance

The following sections describe the FedRAMP governance model and define the roles and responsibilities of key stakeholders of the FedRAMP process.

3.3.1. Governance Model

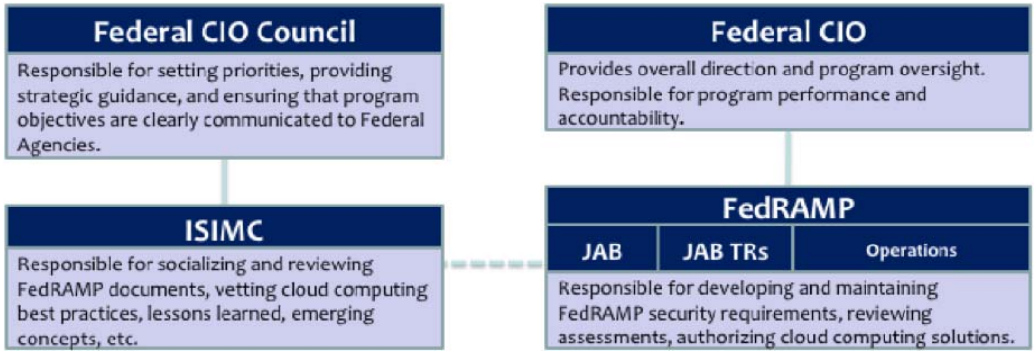


Figure 3: FedRAMP Governance Model

FedRAMP is an interagency effort under the authority of the U.S. Chief Information Officer (U.S. CIO) and managed out of the General Services Administration (GSA) as depicted in Figure 3 and detailed below.

The initiation of FedRAMP and the Joint Authorization Board (JAB) has been via the U.S. CIO in coordination with the Federal CIO Council. The U.S. CIO has tasked the Joint Authorization Board (JAB) with jointly authorizing cloud computing systems. The General Service Administration has been tasked with the actual day-to-day operation of FedRAMP in supports this effort.

The three permanent members of JAB include the Department of Homeland Security (DHS), Department of Defense (DOD), and the General Services Administration (GSA). The sponsoring government agency for each cloud computing system will be represented as the rotating JAB member. The JAB also performs risk determination and acceptance of FedRAMP authorized systems.

The JAB also has the final decision making authority on FedRAMP security controls, policies, procedures and templates.

JAB technical representatives are appointed by their respective JAB authorizing official (both permanent and rotating) for the implementation of the FedRAMP process. JAB technical representatives provide subject matter expertise and advice to the JAB authorizing officials.

The JAB technical representatives review the vetted authorization packages provided by FedRAMP. The JAB technical representatives make authorization recommendations to the JAB authorizing officials and advise the JAB of all residual risks.

FedRAMP is an administrative support team provided by the U.S. CIO under the guidance of GSA. FedRAMP operations are responsible for the day-to-day administration and project management of FedRAMP. FedRAMP performs an initial review of submitted authorization packages and has the authority to work with cloud computing system owners to refine each

submission until it satisfies FedRAMP and JAB requirements. FedRAMP also oversees continuous monitoring of authorized systems.

The ISIMC under the Federal CIO Council is responsible for socializing and reviewing FedRAMP processes and documents. They provide recommendations on the FedRAMP documents directly to the JAB. Their recommendations are based on vetting the cloud computing best practices, lessons learned and emerging concepts within the Federal CIO Council community. However, the final approval on changes to FedRAMP processes and documents is made by the JAB.

3.3.2. Roles and Responsibilities

Table 3: Stakeholder Roles and Responsibilities defines the responsibilities/tasks for FedRAMP stakeholders.

Role	Duties and Responsibilities
JAB Chair (U.S. CIO)	• Selects the JAB Authorizing Officials • Coordinates FedRAMP activities with the CIO Council • Tasks and funds FedRAMP, for technical support as necessary
JAB Authorizing Officials	• Designate a JAB Technical Representative • Ensure the Technical Representative considers current threats and evaluation criteria based on evolving cloud computing best practices in their review of joint authorizations. • Issue joint authorization decisions • Resolve issues as needed
JAB Rotating Authorizing Officials (Sponsoring Agency Authorizing Official)	• Same duties as JAB Authorizing Officials only for their sponsored cloud solution.

Role	Duties and Responsibilities

FedRAMP Operations	• Communicate FedRAMP security requirements to service providers or prospective providers.
	• Review CSP security authorization packages
	• Work with JAB Technical Representatives to clarify questions and concerns regarding authorization packages
	• Maintain a repository of Authorizations in two categories:
	  o Authorizations granted by the JAB.
	  o Authorizations granted by individual agencies.
	• Perform continuous monitoring oversight of FedRAMP authorized systems.
	• Collect FISMA data from FedRAMP authorized systems for quarterly and annually reporting of data to OMB through GSA.
	• Facilitate the leveraging of authorized systems for other federal entities.
	• Maintain knowledge of the FedRAMP capabilities and process throughout industry and the federal government.

JAB Technical Representatives (including the technical representative from the sponsoring Agency)	• Provide subject matter expertise to implement the direction of the JAB Authorizing Official. • Support FedRAMP in defining and implementing the joint authorization process. • Recommend authorization decisions to the JAB Authorizing Official. • Escalate issues to the JAB Authorizing Official as appropriate.
Sponsoring Agency	• Cloud system selection and submission to FedRAMP • Ensures a contractual agreement with a provider is in place using FedRAMP requirements. • Designate Federal personnel to facilitate the receipt and delivery of deliverables between the cloud computing provider (CSP) and FedRAMP. • Assessment, Authorization and continuous monitoring and FISMA reporting of controls that are Agency's (customer's) responsibility.
Leveraging Agency	• Review FedRAMP authorization packages. • Determine if the stated risk determination and acceptance is consistent with its agency's needs. • Authorize cloud system for their Agency use. • Assessment, Authorization and continuous monitoring and FISMA reporting of controls that are Agency's (customer's) responsibility.

Role	Duties and Responsibilities
Cloud Service Provider (CSP)	• The service provider is a government or commercial entity that has a cloud offering/service (IaaS, PaaS or SaaS) and requires FedRAMP authorization of their offering/service for Government use. • Work with the sponsoring Agency to submit their offering for FedRAMP authorization. • Hire independent third party assessor to perform initial system assessment and on-going monitoring of controls. • Create and submit authorization packages. • Provide Continuous Monitoring reports and updates to FedRAMP.

532 **Table 3: Stakeholder Roles and Responsibilities**

3.4. Assessment and Authorization Processes

3.4.1. High-Level Overview

The following figure depicts the high-level process for getting on the FedRAMP authorization request log. Once the Cloud Service Provider (CSP) system is officially on the FedRAMP authorization log, FedRAMP begins processing the cloud system for JAB authorization. The subsequent sections detail the steps involved in the FedRAMP Assessment and Authorization process.

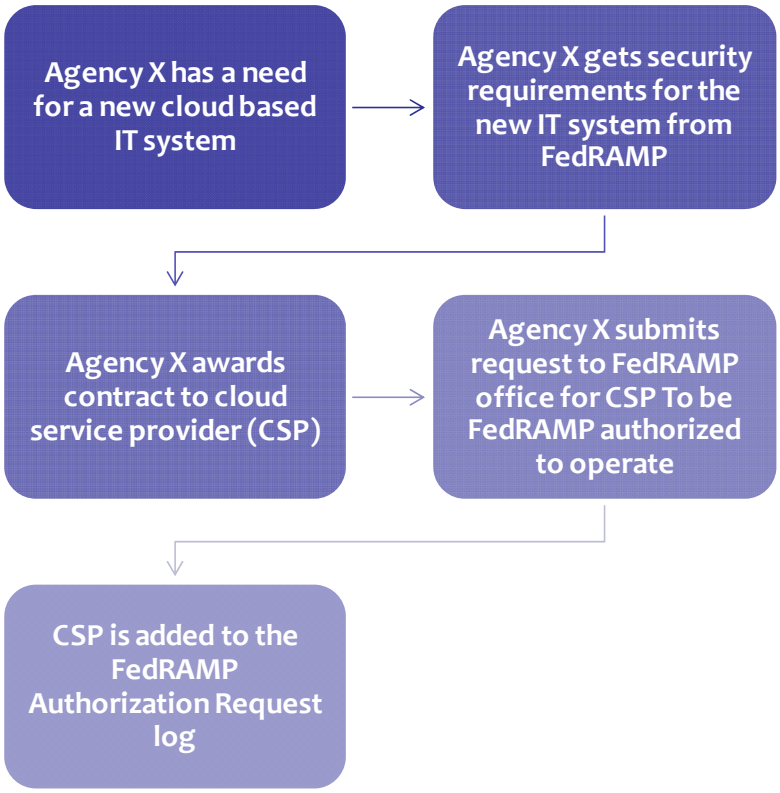
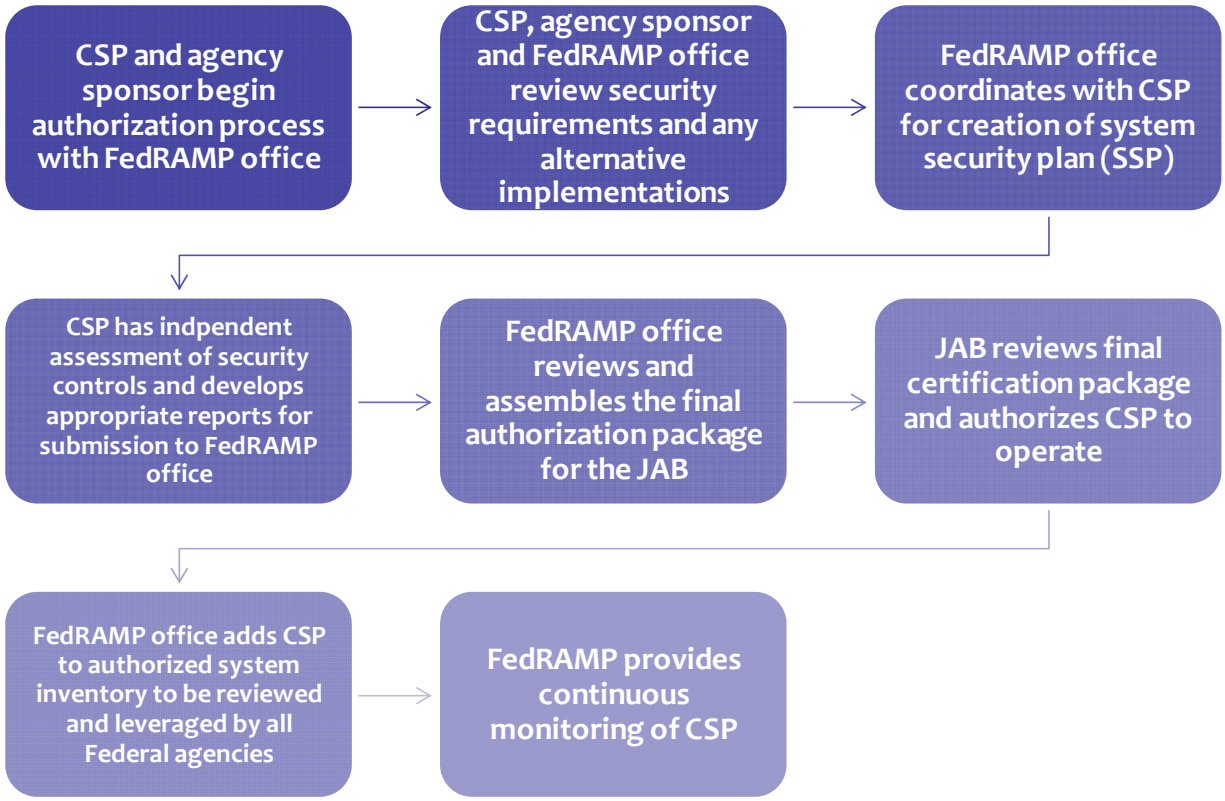


Figure 4: FedRAMP authorization request process



542
543 **Figure 5: FedRAMP authorization process**

3.4.2. Detailed Assessment & Authorization Process

3.4.2.1. Purpose

This section defines FedRAMP assessment and authorization process for Cloud Service Providers (CSP). It also provides guidelines and procedures for applying the NIST 800-37 R1 Risk Management Framework to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and continuous monitoring. CCS Service Providers should use this process and the noted references prior to initiating/performing the Security Authorization process.

3.4.2.2. Policy

Security Authorization Process:

a. The FedRAMP Authorizing Officials (AO) must authorize, in writing, all cloud computing systems before they go into operational service for government interest.

b. A service provider's cloud computing systems must be authorized/reauthorized at least every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST SP 800-37 R1.

Authorization termination dates are influenced by FedRAMP policies that may establish maximum authorization periods. For example, if the maximum authorization period for an information system is three years, then the service provider establishes a continuous monitoring strategy for assessing a subset of the security controls employed within and inherited by the system during the authorization period. This strategy allows all security controls designated in the respective security plans to be assessed at least one time by the end of the three-year period. This also includes any common controls deployed external to service provider cloud computing systems. If the security control assessments are conducted by qualified assessors with the required degree of *independence* based on policies, appropriate security standards and guidelines, and the needs of the FedRAMP authorizing officials, the assessment results can be cumulatively applied to the reauthorization, thus supporting the concept of ongoing authorization. FedRAMP policies regarding ongoing authorization and formal reauthorization, if/when required, are consistent with federal directives, regulations, and/or policies.

3.4.2.3. Required Artifacts

All Service Providers' CCS must complete *and* deliver *the following artifacts* as part of the authorization process. Templates for these artifacts can be found in FedRAMP templates as described in reference materials:

- Privacy Impact Assessment (PIA)
- FedRAMP Test Procedures and Results
- Security Assessment Report (SAR)
- System Security Plan (SSP)
- IT System Contingency Plan (CP)
- IT System Contingency Plan (CP) Test Results
- Plan of Action and Milestones (POA&M)

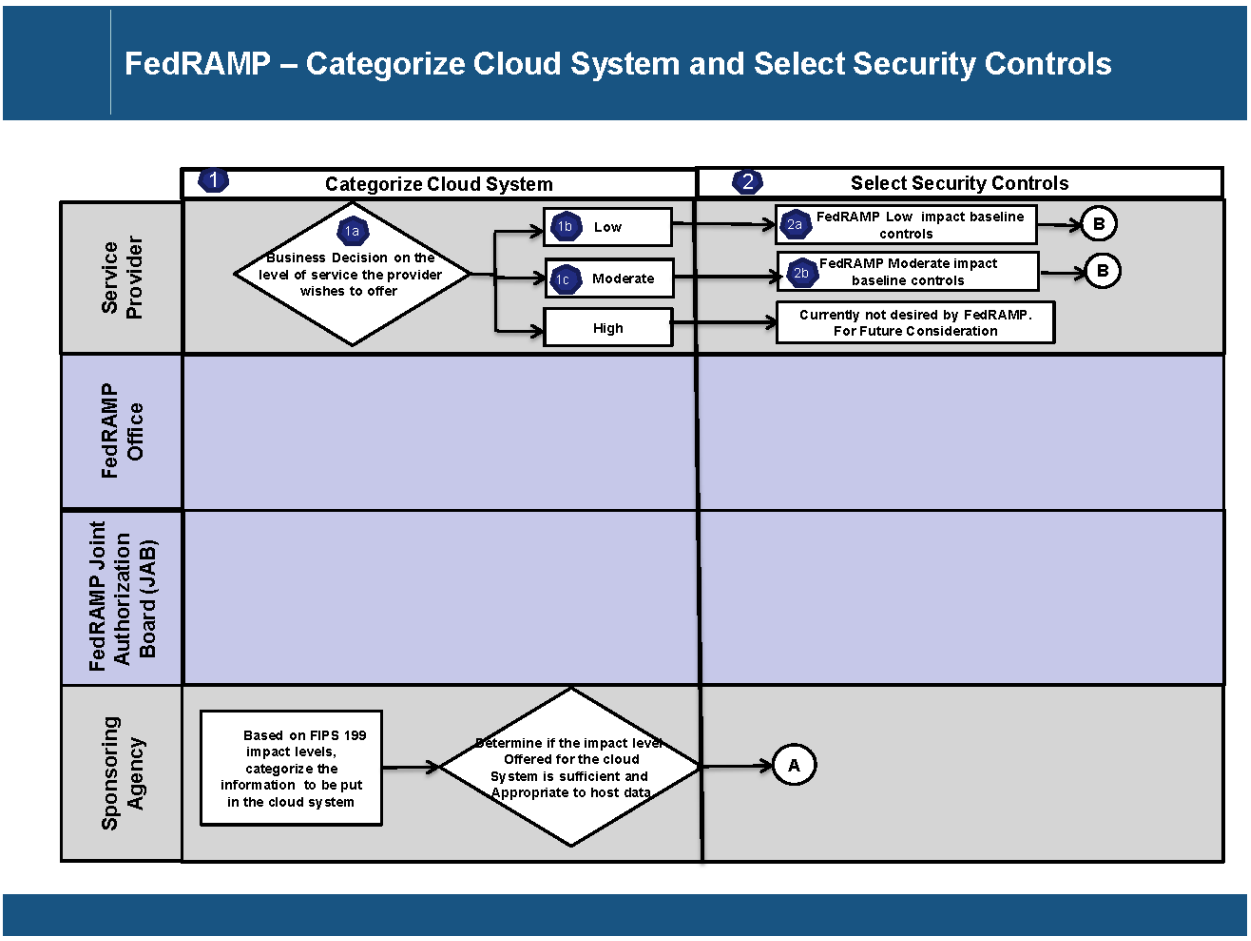
583 • Continuous Monitoring Plan (CMP)
584 • FedRAMP Control Tailoring Workbook
585 • Control Implementation Summary Table
586 • Results of Penetration Testing
587 • Software Code Review
588 • Interconnection Agreements/Service Level Agreements/Memorandum of Agreements

589 3.4.2.4. Assessment and Authorization Process Workflow

590 FedRAMP Assessment and Authorization is an effort composed of many entities/stakeholders
591 working together in concert to enable government-wide risk management of cloud systems. The
592 following diagrams describe the steps and workflow of the FedRAMP Assessment and
593 Authorization process.

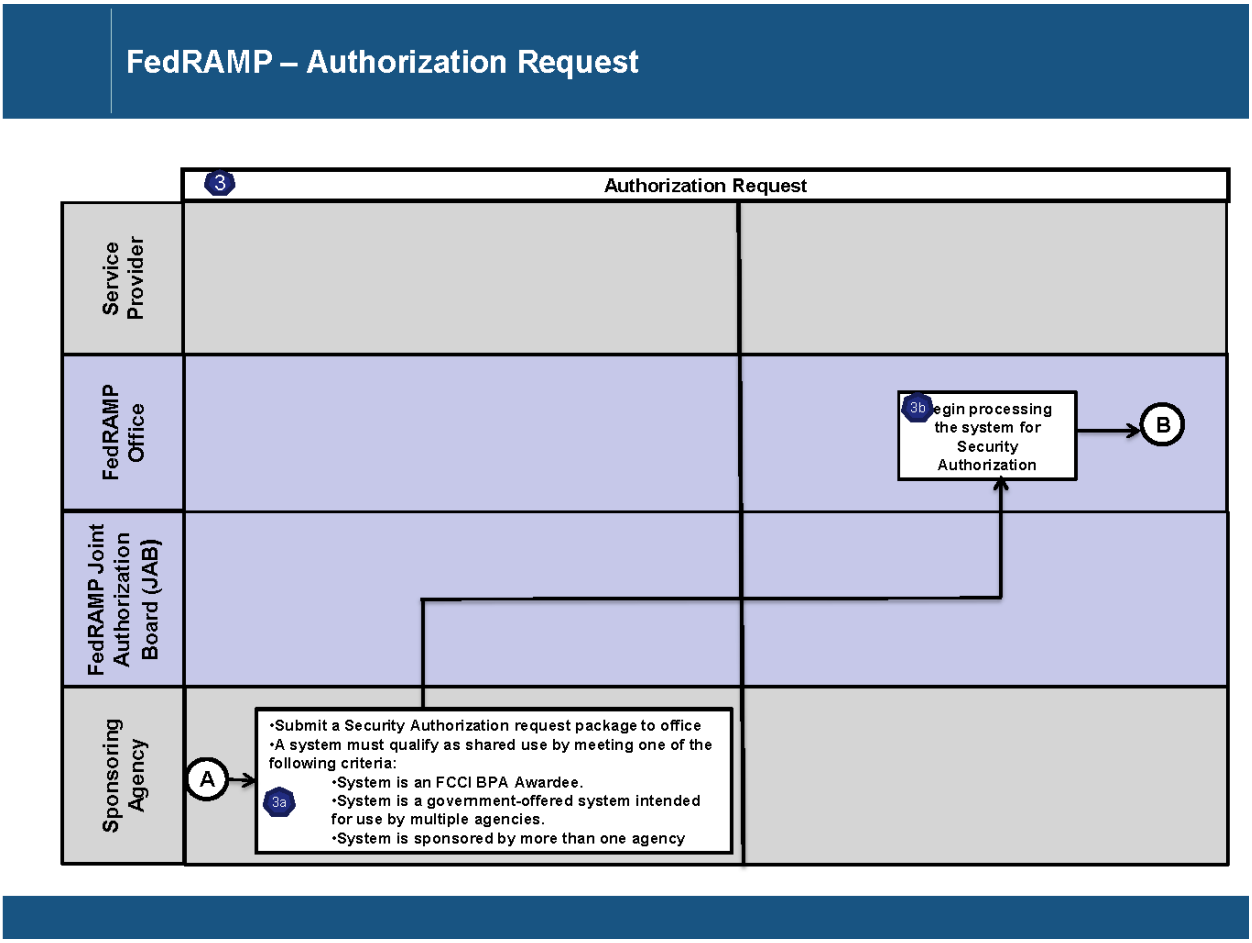
594

595 **Figure 6: FedRAMP Assessment and Authorization Process**



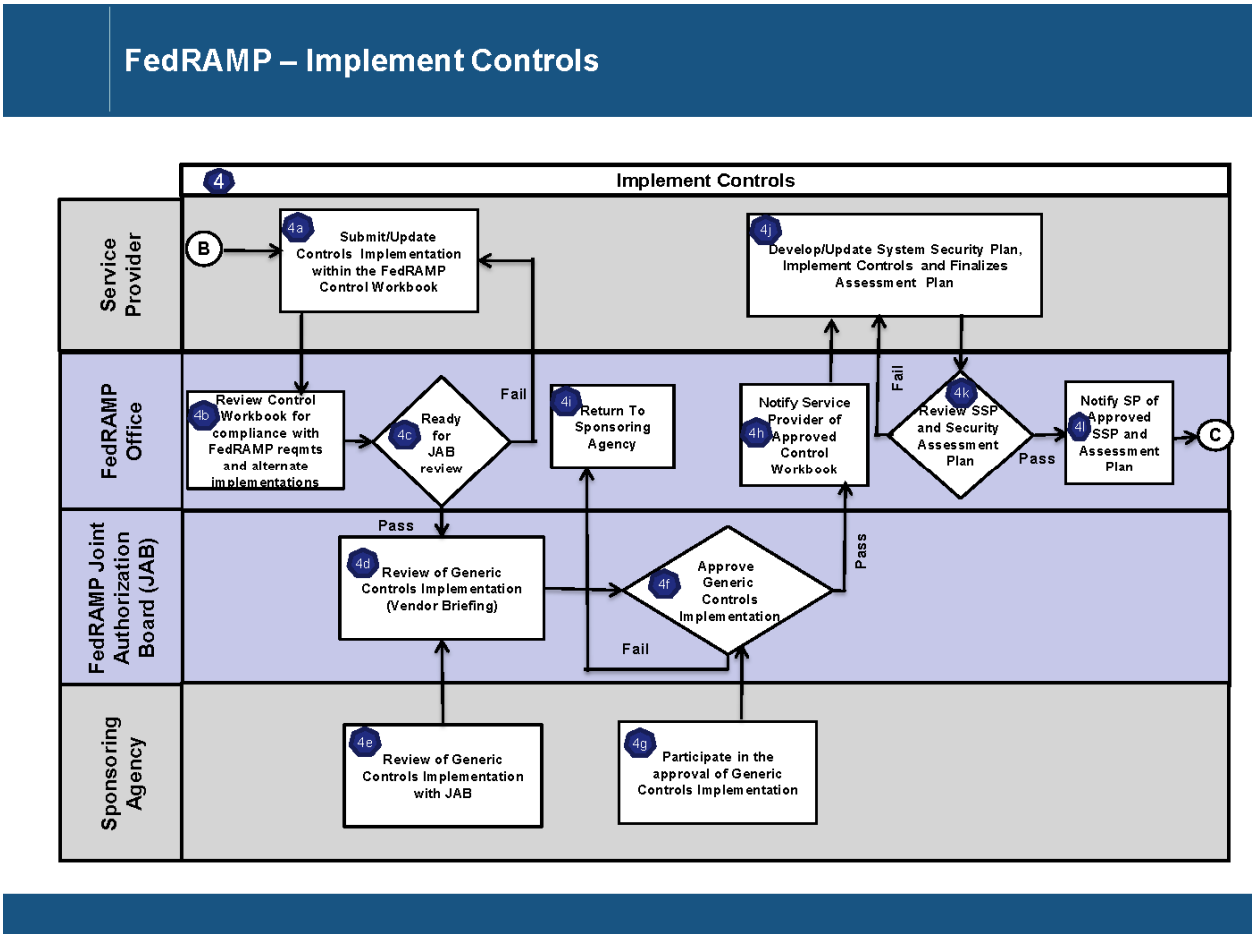
596
597

Figure 7: FedRAMP Categorization of Cloud System and Select Security Controls

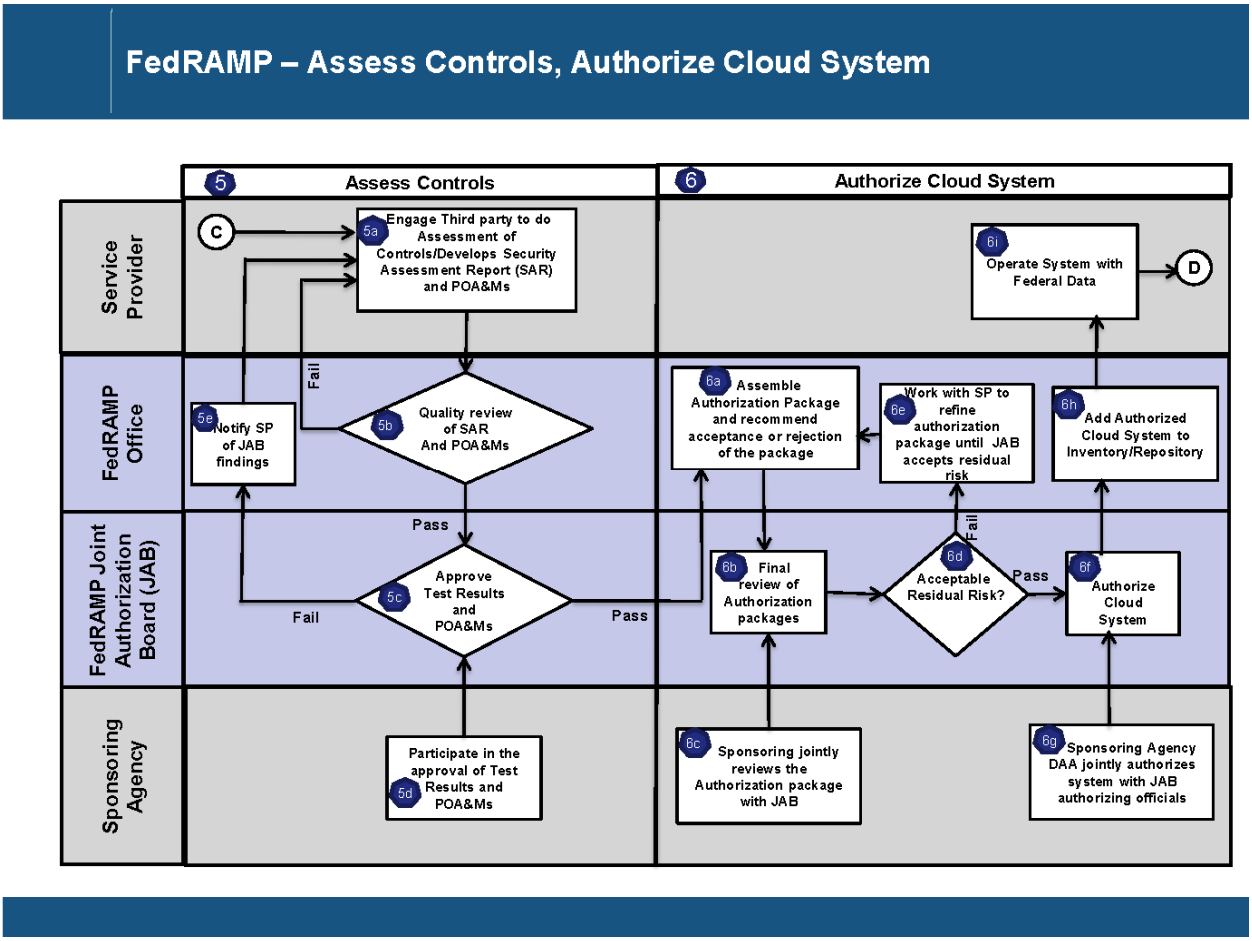


598
599

Figure 8: FedRAMP Authorization Request



600
601 **Figure 9: Implement Controls**



602
603 **Figure 10: Assess Controls, Authorize Cloud System**

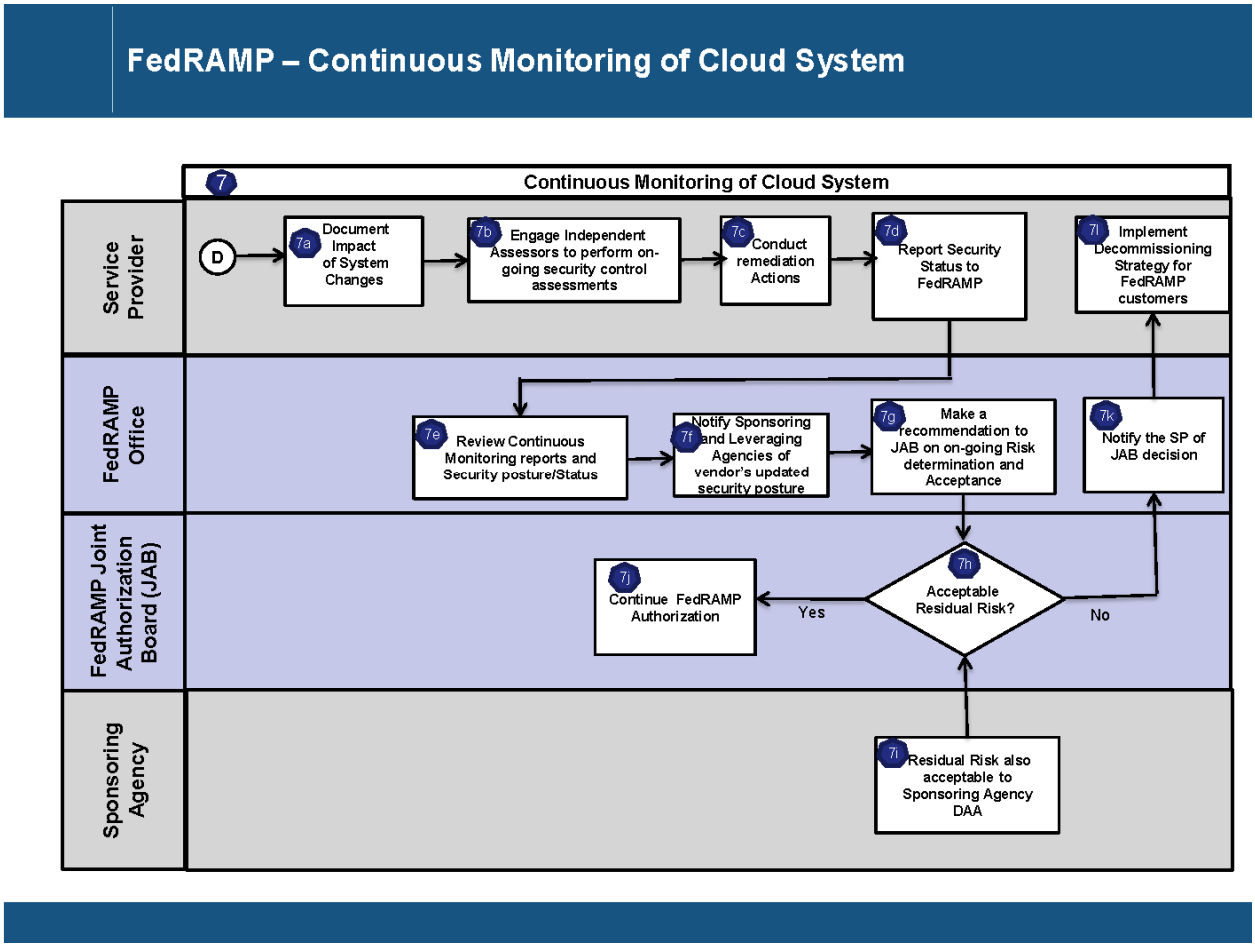


Figure 11: Continuous Monitoring

606 The following section provides the list of NIST special publications, FIPS publications, OMB
607 Memorandums, FedRAMP templates and other guidelines and documents associated with the
608 seven steps of the FedRAMP process:

609 **Step 1 - Categorize Cloud System:** (FIPS 199 / NIST Special Publications 800-30, 800-39,
610 800-59, 800-60.)

611 **Step 2 – Select Security Controls:** (FIPS Publications 199, 200; NIST Special Publications
612 800-30, 800-53 R3, FedRAMP security control baseline)

613 **Step 3 – Authorization Request:** (FedRAMP primary Authorization Request letter, FedRAMP
614 secondary authorization request letter)

615 **Step 4 - Implement Controls:** (FedRAMP control tailoring workbook; Center for Internet
616 Security (CIS); United States Government Configuration Baseline (USGCB); FIPS
617 Publication 200; NIST Special Publications 800-30, 800-53 R3, 800-53A R1)

618 **Step 5 – Assess Controls:** (FedRAMP Test Procedures: Center for Internet Security (CIS);
619 United States Government Configuration Baseline (USGCB); NIST Special
620 Publication 800-53A R1)

621 **Step 6 – Authorize Cloud System:** OMB Memorandum 02-01; NIST Special Publications 800-
622 30, 800-53A R1)

623 **Step 7 – Continuous Monitoring:** FedRAMP Test Procedures; NIST Special Publications
624 800-30, 800-53A R1, 800-37 R1

A description of the process steps is listed in Table 4: FedRAMP Process Steps. The table is organized by step process families relating to the aforementioned steps. The table provides the following information:

- **Process Step** – The distinct step in the process and divided into sub-steps identified with a letter appendix such as "1a".
- **Description** – A high level description of the activities occurring with each step.
- **Deliverable** – A list of the deliverables associated with the steps if the step has any applicable deliverables. Where no deliverable is expected, the table cell is blank.
- **Primary Responsibility** – The entity with the primary responsibility of executing/implementing the steps.
- **Notes/Instructions** – Specific comments on how the entity with primary responsible implements each step.

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
1 Categorize Cloud System				
1a, 1b, and 1c	Cloud Service Provider (CSP) makes a business decision of the security impact level (Low or Moderate) they wish to support or get authorized for their system/cloud offering.	• Authorization request letter documenting FIPS 199 impact level to be supported by the cloud system.	Cloud System Owner and Customer Agency	In this phase, the customer Agency is required to categorize the information/data to be put in the cloud and determine if the impact level offered by the CSP is sufficient and appropriate to host their Agency data.
2 Select Security Controls				
2a and 2b	• If the CSP chooses to be authorized at Low impact level, they need to comply with the FedRAMP Low impact security control baseline (provided in Chapter 3) • If the CSP chooses to be authorized at Moderate impact level, they need to comply with the FedRAMP Moderate impact security control baseline (provided in Chapter 3)		Cloud System Owner	In this phase, the Sponsoring Agency may add any agency-specific controls over the FedRAMP baseline.

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
3 Authorization Request				
3a and 3b	• Submit a Security Authorization request package to FedRAMP. A request package must include ALL of the following documents: a. Authorization request letter from the requesting agency's CIO. • Once all documents are received, the "security authorization request" will be officially acknowledged and documented in request log and FedRAMP will begin processing the system for security authorization.	• FedRAMP primary and secondary Authorization Request Letter (if applicable) • Copy of Signed Contract	Sponsoring Agency	• **Verify multi-agency use of the system** In order to undergo FedRAMP Authorization, a system must qualify as shared use by meeting one of the following criteria: a. System is an FCCI BPA Awardee. b. System is a government-offered system intended for use by multiple agencies. c. System is sponsored by more than one agency
4 Implement Controls				
4a	The service provider begins the FedRAMP authorization process by documenting generic controls implementation and defining the implementation settings for organization defined parameters and any compensating security controls as required by FedRAMP Control Tailoring Workbook	• FedRAMP Control Tailoring Workbook • Control Implementation Summary table.	Cloud Service Provider (CSP)	• *Instruction:* Complete column G of the workbook and submit to FedRAMP for verification/approval as part of the initial SSP with sections 1-12 and select controls in section 13 completed. This is required before assessment activities can begin to assure agreement of organizational settings by the JAB • All service providers must complete the Control Implementation Summary Table

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
				(*Sample provided in FedRAMP Templates)***-** which is customized for the service provider's system and its environment. The completed table identifies controls types (common vs. hybrid controls vs. app specific controls) with implementation status (Fully Implemented, Partially Implemented, Not Implemented, Not Applicable) across all required controls. The service provider completed table must reflect controls based on NIST 800-53 R3 and provide status for both controls and enhancements (as applicable per FIPS 199 impact and FedRAMP required controls). The columns can and should be customized to the service providers' environment to account for controls and minor apps (as necessary).
4b	FedRAMP reviews the Control Tailoring Workbook provided by the vendor for compliance with FedRAMP security requirements and acceptable risk criteria			

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
4c	FedRAMP determines if the Control Tailoring Workbook is ready for JAB review. If yes, then see 4d and 4e, otherwise FedRAMP sends the workbook back to the service provider to fix it.			
4d and 4e	JAB (consisting of DHS, DOD and GSA) and the Requesting/Sponsoring Agency receive a CSP/FedRAMP briefing on the generic control implementation. JAB and requesting Agency review the Control Tailoring Workbook for compliance and alternate implementations/compensating controls to determine effectiveness and make a risk-based decision.			• **Instruction** - When the FedRAMP Control Tailoring Workbook and Control Summary have been completed and submitted to FedRAMP for review, FedRAMP may request a meeting with the Service Provider at this stage to review the documents or give the go-ahead to proceed with the authorization process.
4f and 4g	JAB and the Requesting/sponsoring Agency jointly Approve/Reject the Control Tailoring Workbook and the decision to proceed further.			
4h	If approved, FedRAMP notifies the service provider of JAB approval and allow the vendor to proceed with the development of System Security Plan (SSP) and Assessment plan			
4i	If rejected, then FedRAMP notifies the requesting agency, which then asks the service provider to come for FedRAMP Authorization when they meet the FedRAMP requirements.			

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
4j	If the Control Tailoring Workbook is approved, then service provider proceeds with the development of SSP, Assessment plan and implementation of the controls per SSP. Upon completion of SSP and Assessment plan, it is submitted to the FedRAMP for review.	• System Security Plan (SSP) • Assessment Plan		• The FedRAMP security assessment test procedures, as located in reference materials, must be used as the basis for all security assessment and continuous monitoring activities. • **Instruction** - The FedRAMP must accept the System Security Plan and Security Assessment Plan before assessment activities can begin. System Security Plan and Security Assessment Plan should be submitted to the FedRAMP for review and approval at this time.
4k	FedRAMP reviews the SSP and Assessment plan.			
4l	If satisfactory, then see 5a otherwise the SSP and/or Assessment plan are sent back to the service provider to fix the issues identified.			

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
5 Assess Controls				
5a	Upon approval of SSP and Assessment plan from FedRAMP, the service provider should engage third party independent assessor to assess the effectiveness of implemented controls using FedRAMP's Assessment Procedures. The independent assessor documents the results of the assessment in the Security Assessment Report (SAR) using FedRAMP's template. Any outstanding issues should be documented in the POA&M's. Both SAR and POA&M are submitted to FedRAMP for review.	• Security Assessment Report (SAR) • POA&M • Updated SSP		Service Provider Owner should update the system security plan based on the results of the risk assessment and any modifications to the security controls in the information system. Update the SSP to reflect the actual state of the security controls implemented in the system following completion of security assessment activities.
5b	FedRAMP reviews the test results documented in the SAR and any outstanding issues in the POA&M to determine if the documented risk seems acceptable for JAB. FedRAMP repeats this process with the CSP until the documents are acceptable. Once they are acceptable, then FedRAMP provides these documents to the JAB including the requesting Agency with a summary of the results in the documents.			

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
5c and 5d	JAB and the requesting agency review the test results and POA&M's. If the test results demonstrate that the security controls are effectively implemented and if the outstanding issues in the POA&M are acceptable, then the JAB notifies FedRAMP of their approval and the process moves to Step 6a.			
5e	However, JAB may have questions/concerns associated with the test results or outstanding issues. FedRAMP communicates these with the CSP in this step.			
6 Authorize Cloud System				
6a	FedRAMP assembles the authorization package based on the updated deliverables received from the CSP to this point and makes a recommendation of acceptance or rejection of the package to the JAB	• Complete CSP authorization package	FedRAMP and CSP	
6b and 6c	JAB including the requesting/sponsoring Agency performs a final review of the CSP authorization package			
6d	Based on the review in steps 6b and c, make a determination on the acceptance or rejection of the residual risk.			

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
6e	If rejected, then FedRAMP works with the CSP to refine the package until the residual risk in the cloud system is acceptable to the JAB			
6f and 6g	If accepted, then the JAB including the requesting/sponsoring Agency issues the Authority To Operate the cloud system			
6h	FedRAMP authorized systems are added to a repository of authorized systems that can be leveraged by other Federal Agencies			
6i	The cloud system is operational with Federal data processed on the system			
7 Continuous Monitoring				More details about the FedRAMP Continuous Monitoring phase can be found in Chapter 2: Continuous Monitoring.

633 **Table 4: FedRAMP Process Steps**

3.4.2.5. Risk Acceptability Criteria

The following table lists the FedRAMP JAB acceptable risk criteria. In particular the table lists the "Not Acceptable" risk criteria and the ones requiring JAB prior approval.

Not Acceptable	Requires JAB Prior Approval
• Vulnerability Scanner output has HIGH vulnerabilities not remediated. • More than 5% of total security controls are reflected within the POA&M. • False Positive claims are not supported by evidence files. • FedRAMP audit shows configuration, which differs from presented documentation. • OS out of lifecycle Support (Windows XP and before). • Hot fix patches not implemented, without justification • Does not support 2-factor authentication from customer agency to cloud for moderate impact system. Does not support FIPS 140-2 from customer agency to the cloud.	• Change in inter-connections. • Change in ISA/MOU. • Change in physical location. • Change in Security Impact Level. • Threat Changes. • Privacy Act security posture change. • OS Change (2K to 2K3, Windows to Linux, etc). • Change in SW (i.e. Oracle to SQL).

Table 5: FedRAMP Risk Acceptability Criteria

3.5. Authorization Maintenance Process

Once a system has received a FedRAMP authorization, several events take place. First, the system is added to the FedRAMP online repository of authorized systems. Next, FedRAMP will begin facilitating agency access to the approved authorization package to enable agency review of the material. Lastly, FedRAMP will begin overseeing continuous monitoring of the system and advise the JAB of any changes to risk posture.

FedRAMP will maintain an online repository of cloud system authorizations in two categories:

- Authorizations granted by the JAB
- Authorizations granted by individual Agencies

This web based resource will be publicly accessible and will be the authoritative source of FedRAMP system authorization status. The web based resource will maintain the following information for each currently authorized system.

- System Name and scope of authorization (examples of scope include IaaS, PaaS or SaaS, entire or partial suite of products offered by CSP)
- FIPS 199 impact level supported by the cloud system
- Expiration date for Authorization
- Version of FedRAMP requirements and templates used to authorize the system

- Points of Contact for the cloud system

FedRAMP will also maintain a secure website (separate from the public website) accessible only to Federal officials to access CSP authorization packages and communicate cloud system specific updates on the risk posture.

3.6. Authorization Leveraging Process

The purpose of all of the FedRAMP authorizations is to facilitate the leveraging of these authorizations for use by multiple federal agencies ("Approve once. Use often"). Leveraging such authorizations is employed when a federal agency chooses to accept all of the information in an existing authorization package via FedRAMP.

A FedRAMP joint authorization is not a "Federal Authority to Operate" exempting Federal Agencies, Bureaus, and Divisions from individually granting Authorities to Operate. A FedRAMP Authorization provides a baseline Authorization for Federal Agencies, Bureaus, and Divisions to review and potentially leverage. As is consistent with the traditional authorization process, an authorizing official in the leveraging organization is both responsible and accountable for accepting the security risks that may impact the leveraging organization's operations and assets, individuals, other organizations, or the Nation.

The leveraging organization reviews the FedRAMP authorization package as the basis for determining risk to the leveraging organization. When reviewing the authorization package, the leveraging organization considers risk factors such as the time elapsed since the authorization results were produced, the results of continuous monitoring, the criticality/sensitivity of the information to be processed, stored, or transmitted, as well as the overall risk tolerance of the leveraging organization.

FedRAMP will provide leveraging agencies with access to the authorization packages to assist in their risk management decision. If the leveraging organization determines that there is insufficient information in the authorization package or inadequate security measures in place for establishing an acceptable level of risk, the leveraging organization needs to communicate that to FedRAMP. If additional information is needed or additional security measures are needed such as increasing specific security controls, conducting additional assessments, implementing other compensating controls, or establishing constraints on the use of the information system or services provided by the system these items will be facilitated by FedRAMP. The goal is to keep unique requirements to a minimum, but consider any other additional security controls for implementation and inclusion in the baseline FedRAMP security controls.

The leveraged authorization approach provides opportunities for significant cost savings and avoids a potentially costly and time-consuming authorization process by the leveraging organization. Leveraging organizations generate an authorization decision document and reference, as appropriate, information in the authorization package from FedRAMP.

All of the FedRAMP authorizations do not consider the actual information placed in the system. It is the leveraging agencies responsibility to do proper information categorization and determination if privacy information will be properly protected and if a complete Privacy Impact Assessment is in place. In almost all cases the FedRAMP authorization does not consider the actual provisioning of users and their proper security training. In all cases additional security measures will need to be documented. The leveraging organization documents those measures

by creating an addendum to the original authorization package of FedRAMP or a limited version of a complete package that references the FedRAMP authorization. This addendum may include, as appropriate, updates to the security plan (for the controls that is customer Agency's implementation responsibility), security assessment report, and/or leveraging organization's plan of action and milestones. FedRAMP will report the base system for FISMA purposes and the leveraging agency will need to report their authorization via their organizational FISMA process.

Consistent with the traditional authorization process, a single organizational official in a senior leadership position in the leveraging organization is both responsible and accountable for accepting the information system-related security risks that may impact the leveraging organization's operations and assets, individuals, other organizations, or the Nation.

The leveraged authorization remains in effect as long as the leveraging organization accepts the information system-related security risks and the authorization meets the requirements established by federal and/or organizational policies. This requires the sharing of information resulting from continuous monitoring activities conducted by FedRAMP and will be provided to agencies that notify FedRAMP that they are leveraging a particular package. The updates will include such items as updates to the security plan, security assessment report, plan of action and milestones, and security status reports. To enhance the security of all parties, the leveraging organization can also share with the owning organization, the results from any RMF-related activities it conducts to supplement the authorization results produced by the owning organization.

3.7. Communications Process

FedRAMP interacts with multiple stakeholders during the security lifecycle of a system. To streamline the workflow, a secure website is under development to facilitate updates on status, provide secure posting of artifacts and provide baseline information. However, in addition to this online web portal, proactive communication is required to ensure the success of each individual cloud system authorization. It is expected that the Cloud Service Providers, FedRAMP and Sponsoring and Leveraging Agencies will communicate regularly to ensure that information is disseminated effectively.

The following communication templates will be employed:

- Sponsorship Letter
- Status Report
- Confirmation Receipts (Complete Package, Incomplete Package)
- Review Recommendation (Acceptable, Unacceptable)
- Missing Artifact List
- Incident Report

The communication plan in Table 6: Communications Plan identifies the touch points and how communication will be delivered between FedRAMP, Leveraging Agencies, Sponsoring Agencies, and the Cloud Service Providers. Additional emails, conference calls and in-person meetings to facilitate the process as the team deems necessary may augment the communication plan. As changes are integrated into the requirement process, the communication plan may be updated to respond to required changes to the communication process. At a minimum, the

738 communication plan will be reviewed annually. The table is organized by phases and depicts
739 the communication flow in the following areas:

740 • **Trigger Event** – Identifies the event that will start the require communication during the
741 different operational processes of FedRAMP
742 • **Deliverable** –Artifact used to communicate the results/output of the trigger event to
743 FedRAMP stakeholders
744 • **Initiator** – The entity responsible for starting the communication process.
745 • **Target Audience** – Receivers of the deliverable in the communication process.
746 • **Delivery Method** – How the artifacts will be communicated to the target audience.

#	Trigger Event	Deliverable	Initiator	Target Audience	Delivery Method
Authorization Request, Assessment and Authorization Phases					
1	Initiation of FedRAMP A&A Process	Sponsorship Letter, Contract	Sponsoring Agency	FedRAMP	Upload through FedRAMP Website
2	Receipt of Sponsorship Letter	Kickoff Meeting	FedRAMP	Sponsoring Agency, Cloud Service Provider	Scheduled with the participants identified through the sponsorship letter, this first meeting will allow the participants an opportunity to understand the process and establish milestone dates.
3	Weekly Status Report	Status Report	FedRAMP	Sponsoring Agency, Cloud Service Provider	Uploaded to Secure Web Portal, the status report is updated weekly advising of current status and future target dates.
4	Questions about requirements	Email Inquiry	Cloud Service Provider	FedRAMP	Cloud Service Provider may email questions to FedRAMP.
5	Received Questions	Email Clarification	FedRAMP	Cloud Service Provider	FedRAMP will respond to email questions within two business days.
6	Package Submission	Completed Artifact(s)	Cloud Service Provider	FedRAMP	Securely uploaded through FedRAMP Website.
7	Completed Package Submission	Confirmation Receipt – Completed Package	FedRAMP	Cloud Service Provider	Emailed acknowledgement receipt by FedRAMP Review Team identifies the received artifacts and target date for completed review.

#	Trigger Event	Deliverable	Initiator	Target Audience	Delivery Method
8	Incomplete Package Submission	Confirmation Receipt – Incomplete Package	FedRAMP	Cloud Service Provider	Emailed acknowledgement receipt by FedRAMP Review Team identifies which artifacts have been received and which are still missing.
9	FedRAMP completes artifact review, recommends ATO	Review Recommendation	FedRAMP	JAB, Sponsoring Agency, Cloud Service Provider	Emailed recommendation explains the Cloud Service Provider's compliance with the required risk management controls.
10	FedRAMP completes artifact review, recommends improvements	Review Recommendation	FedRAMP	Cloud Service Provider	Emailed Review Recommendation includes individual areas of focus required by the Cloud Service Provider to be compliant with FedRAMP requirements.
11	Completed review, improvements recommended	Findings Review Meeting	FedRAMP	Sponsoring Agency, Cloud Service Provider	Scheduled by FedRAMP, this meeting allows the Cloud Service Provider and the Sponsoring Agency an opportunity to discuss and understand any deficiencies identified by the FedRAMP review team.
Authorization Maintenance Phase					

#	Trigger Event	Deliverable	Initiator	Target Audience	Delivery Method
12	FedRAMP authorizes system	Joint Authorization Letter	JAB, FedRAMP	Cloud Service Provider, Sponsoring Agency, Leveraging Agency	Post the following information on a public FedRAMP website about the authorized system: System Name FIPS 199 impact level the system is authorized at Version of FedRAMP security controls and other templates used Authorization Expiration Date Privacy Questionnaire Maintain the authorization package including but not limited to SSP, SAR, Contingency Plan, Incident reporting plan, POA&M's on a secure website accessible by Government officials only
13	Granting authorization package access to leveraging Agencies	CSP Authorization Package	FedRAMP	Leveraging Agency	Provide secure access (login) to Government-only website for accessing CSP authorization package
Continuous Monitoring Phase					

#	Trigger Event	Deliverable	Initiator	Target Audience	Delivery Method
14	Creation of updated artifacts (e.g. SSP, POA&M's)	Updated Artifacts	Cloud Service Provider	FedRAMP	Uploaded to Secure Web Portal, the Cloud Service Provider will post all regular recurring artifacts for FedRAMP team review.
15	Receipt of Updated Artifacts	Confirmation Receipt	FedRAMP	Cloud Service Provider	Email acknowledgement receipt of uploaded artifacts.
16	Accepted Artifacts	Review Recommendation – Acceptable	FedRAMP	Leveraging Agencies, Cloud Service Provider	Update on secure website that Cloud Service Providers updated artifacts meet compliance requirements.
17	Unacceptable Artifacts	Review Recommendation - Unacceptable	FedRAMP	Leveraging Agencies, Cloud Service Provider	Email Notification of what issues the Cloud Service Provider is required to remediate to remain within compliance. Update on Secure Web Site identifying outstanding issues.
18	Updated Artifacts not received with 1 week of due date	Missing Artifact List	FedRAMP	Cloud Service Provider	Email Notification to the Cloud Service Provider that their artifacts have not been received.
17	Updated Artifacts not received with 2 weeks of due date	Missing Artifact List	FedRAMP	Leveraging Agencies, Cloud Service Provider	Email Notification to the Cloud Service Provider that their artifacts have not been received and their ATO is at risk.
18	Incident	Incident Reporting/Notification	Cloud Service Provider	Leveraging Agencies, FedRAMP	

747 **Table 6: Communications Plan**

3.8. Change Management Process

The technology changes within the dynamic and scalable cloud computing environment are expected to be quite swift. As the cloud computing market matures, best practices associated with the implementation and testing of security controls will evolve.

There are multiple industry groups, academic collaborations, engineering teams, policy firms and assorted cadre of experts striving to maximize the potential of cloud computing in a secure environment. It is therefore obvious that FedRAMP will maintain resources to keep abreast of the technological and security enhancements in near real time. As these cloud computing best practices evolve, FedRAMP security requirements, processes and templates will also under go an evolution. The following sections define the FedRAMP change management process.

3.8.1. Factors for change

The following internal and external factors will drive the change to FedRAMP security requirements, processes and templates.

- ***Update to NIST special publications and FIPS publications***: FedRAMP templates and requirements are based on the NIST special publications and FIPS publications. If the NIST SP 800-53 r3 is updated with new security controls and enhancements for low and moderate impact level, FedRAMP security controls will need to be updated. Also, if NIST publishes new guidance associated with cloud computing best practices, these will be considered for updates to FedRAMP security requirements and evaluation criteria/test procedures.
- ***Requirements from other Federal security initiatives***: Government-wide security initiatives and mandates such as Trusted Internet Connections (TIC) and Identity, Credential and Access Management (ICAM) will drive updates to FedRAMP requirements for wider adoption of cloud computing systems and services across the Government. As the solutions for various cloud service models (IaaS, PaaS, SaaS), which is currently under active investigation, are adopted, they will be disseminated by FedRAMP. FedRAMP and the JAB will rely on both ISIMC and NIST to recommend changes to security controls over time. While these bodies will not have the authority to implement the changes, their expertise and reputation lend themselves to providing invaluable assistance to FedRAMP. It should be noted that security requirements can ***only*** be approved for change by the JAB.
- ***Agency-Specific requirements beyond the FedRAMP baseline:*** Federal Agencies leveraging FedRAMP authorizations for use within their own Agencies may add specific additional security controls, conduct additional assessments, or require implementation of other compensating controls**.** The leveraging agencies should notify FedRAMP of these additional requirements. FedRAMP JAB will meet regularly to discuss any required updates and possible inclusion of these additional security measures to FedRAMP security controls baseline and assessment procedures/evaluation criteria. If different leveraging Agencies have added different requirements and additional security measures for the same cloud system, FedRAMP will maintain a list of these additions and may consider updating either the FedRAMP baseline for all cloud systems or just that specific

cloud system. In both cases, FedRAMP will assess these additional controls/measures during the continuous monitoring phase.

- ***Industry best practices, development of standards or use of new tools/technology:*** FedRAMP requirements may be updated to adopt new standards as they are created for cloud computing interoperability, portability and security. As cloud computing market matures and as industry develops new tools and technologies for automated and near real time monitoring of controls and automated mechanisms for exposing audit data to comply with regulatory requirements become available, FedRAMP processes will also be updated accordingly.
- ***Changes to cloud service provider offering:*** As new features and components are added to the cloud service provider offering, additional requirements and assessments might be necessary to ensure that robust security posture of the system is maintained.

3.8.2. Security Documents/Templates Change Control

All security document templates are to be considered "living documents". Over time, as requirements change, methodologies evolve, or new technologies and threats present themselves, these documents will undergo some degree of modification. FedRAMP is solely responsible for implementing these changes. It should be noted that FedRAMP security document templates are designed to assist the user with proper documentation related to their authorization package. These also serve to provide a more uniform content collection method that aids the CSP and agencies with achieving authorization status for the cloud service offering. As changes are made, updated templates will be posted to the FedRAMP website with instructions related to use.

3.8.3. Requirements for Cloud Service Provider Change Control Process

Once a requirement is approved, CSP's have 30 days to develop and submit an implementation plan. CSP's are responsible for implementing the plans. The implementation plan needs to define the actions that the CSP must perform in order to comply with the new requirement. In most cases the implementation of the new control will be implemented within the 30 day window. However, there may be instances where the implementation of the controls will require the CSP to add the control to the POAM sheet, with milestones, target date, and resource allocations documenting the future implementation due to the nature of the control itself. Furthermore, it is understood that, depending on the particular infrastructure related to the security control, that it might be necessary for the CSP to implement a compensating control. This control will accomplish the same goal as the new requirement. However, it accomplishes the goal in a different manner. All compensating controls must receive authorization from the JAB. When situations arise where the new requirement cannot be implemented on a system due to the legacy nature of the infrastructure, or in cases where the control itself will have a severely negative impact on the mission of the system, the CSP may request a waiver. Waivers, though rare, must be presented to the JAB for approval. Once the control change is implemented, FedRAMP is to be notified and the security control baseline will be adjusted and documented.

828 ### 3.8.4. Sponsoring Agency CCP

829 Sponsoring federal agencies maintain their responsibility for establishing and maintaining their
830 own internal change control process. Responsibilities related to the cloud computing service
831 offering should be limited to the interconnection between the agency and the CSP, and the input
832 to any change requests.

833