Concept of Operations (CONOPS)

Version 1.2

July 27, 2012

Overview

Cloud computing technology allows the Federal Government to address demand from citizens for better, faster services and to save resources, consolidate services, and improve security. The essential characteristics of cloud computing - on-demand provisioning, resource pooling, elasticity, network access, and measured services - provide the capabilities for agencies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services. Agencies have realized the benefits of this technology and are integrating it into their information technology environment.

On December 9, 2010; the Office of Management and Budget (OMB) released the *25 Point Implementation Plan To Reform Federal Information Technology Management*, establishing the Cloud First policy and requiring agencies to use cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. The Federal Risk and Authorization Management Program (FedRAMP) was established by a memorandum issued by OMB on December 8, 2011, *Security Authorization of Information Systems in Cloud Computing Environments* (FedRAMP Policy Memo) to provide a cost-effective, risk-based approach for the adoption and use of cloud services.

A key element to successful implementation of cloud computing is a security program that addresses the specific characteristics of cloud computing and provides the level of security commensurate with specific needs to protect government information. Effective security management must be based on risk management and not only on compliance. By adhering to a standardized set of processes, procedures, and controls, agencies can identify and assess risks and develop strategies to mitigate them.

This document describes a general Concept of Operations (CONOPS) for the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based services. FedRAMP uses a “do once, use many times” framework that intends to saves costs, time, and staff required to conduct redundant agency security assessments and process monitoring reports.

The purpose of FedRAMP is to:

- Ensure that cloud based services 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.

FedRAMP was developed in collaboration with the National Institute of Standards and Technology (NIST), the General Services Administration (GSA), the Department of Defense (DOD), and the Department of Homeland Security (DHS). Many other government agencies and working groups participated in reviewing and standardizing the controls, policies and procedures.

The major participants in the FedRAMP process are:

- Federal agency customer – has a requirement for cloud technology that will be deployed into their security environment and is responsible for ensuring FISMA compliance
- Cloud Service Provider (CSP) – is willing and able to fulfill agency requirements and to meet security requirements
- Joint Authorization Board (JAB) – reviews the security package submitted by the CSP and grants a provisional Authority to Operate (ATO)
- Third Party Assessor (3PAO) – validates and attests to the quality and compliance of the CSP provided security package
- FedRAMP Program Management Office (PMO) – manages the process assessment, authorization, and continuous monitoring process

A CSP follows the process for a provisional authorization under FedRAMP and uses a 3PAO to assess and review their security control implementations. CSPs then provide documentation of the test results in a completed assessment package to the FedRAMP PMO. The security package is then reviewed by the JAB and if a CSP system presents an acceptable level of risk, a provisional Authorization is granted. Agencies can then leverage the Provisional ATO and grant their own ATO without conducting duplicative assessments.

Implementation of FedRAMP will be in phases. This document describes all the services that will be available at initial operating capability – targeted for June 2012. The Concept of Operations will be updated as the program evolves toward sustained operations.

Document Revision History

Date	Pages	Description	Author
06/04/2012	p. 8	Figure 1-1	FedRAMP Office
06/04/2012	p. 11	Table 2-1	FedRAMP Office
06/04/2012	p. 13	§ 2.2	FedRAMP Office
06/04/2012	p. 14	Table 3-1	FedRAMP Office
06/04/2012	p. 16	§ 3.2 and Figure 3-2	FedRAMP Office
06/04/2012	p. 21	§ 5.1	FedRAMP Office
06/04/2012	p. 38	§ 8.0 and Figure 8-1	FedRAMP Office
06/04/2012	p. 39	§ 8.1 and Figure 8-2	FedRAMP Office
06/04/2012	p. 40	Figure 8-3	FedRAMP Office
06/04/2012	p. 41	§ 8.2	FedRAMP Office
06/04/2012	p. 42	Figure 8-4	FedRAMP Office
06/04/2012	p. 46	Table 10-1	FedRAMP Office
07/27/2012	p. 35	Table 7-1	FedRAMP Office

Table of Contents

1. About this document 8
1.1. Who should use this document? 8
1.2. How this document is organized 8
1.3. How to contact us 9
2. FedRAMP Definition and purpose 10
2.1. Stakeholders 10
2.2. FedRAMP Governance and Roles 13
3. High Level Operations 14
3.1. Phased Approach 15
3.2. Priority Queue 16
3.3. FedRAMP Program Change 17
4. How to Use FedRAMP 18
4.1. Federal agencies 18
4.1.1. Leveraging Authorizations 18
4.1.2. Initiating Assessments with FedRAMP 18
4.1.3. Implement Continuous Monitoring 18
4.1.4. Ensure FedRAMP Requirements Are Met Contractually 19
4.2. Cloud Service Providers 19
4.3. Third Party Assessment Organizations (3PAO) 19
5. Third-Party Assessment Organizations 20
5.1. Applying for FedRAMP Accreditation 21
5.2. 3PAO Accreditation Evaluation 21
5.3. Maintaining the Accreditation 22
5.4. Transitioning to a Privatized Board 23
6. Security Assessments 24
6.1. Initiating A Request 25
6.2. Documenting the Security Controls 28
6.3. Performing the Security Testing 30
6.4. Finalizing the Security Assessment 32
7. Leveraging the Provisional Authorization 34
7.1. FedRAMP Secure Repository 35
7.1.1. CSP Supplied 35
7.1.2. Agency ATO 36
7.1.3. Agency ATO with Accredited 3PAO 36
7.1.4. JAB Provisional Authorization 36
8. Ongoing Assessment and Authorization (Continuous Monitoring) 38
8.1. Operational Visibility 39
8.2. Change Control Process 40
8.3. Incident Response 41
9. References 43
9.1. Applicable Laws and Regulations 43
9.2. Applicable Standards and Guidance 43
10. Deliverables 45
11. Acronyms 49

List of Tables

Table 2-1. FedRAMP Stakeholder Roles 11
Table 6-1. Initiate Request Deliverables 27
Table 6-2. Document Security Controls Deliverables 29
Table 6-3. Perform Security Testing Deliverables 31
Table 6-4. Finalize Security Assessment Deliverable 33
Table 7-1. Security Assessment Package Categories 35
Table 10-1. FedRAMP Deliverables by Process Area 45

Table of Figures

Figure 1-1. Relationship of FedRAMP Publications 8
Figure 2-1. FedRAMP Stakeholders 11
Figure 2-2. FedRAMP Governance Entities 13
Figure 3-1. FedRAMP Process Areas 14
Figure 3-2. FedRAMP Program Phases 16
Figure 5-1. Third Party Assessor Organization Accreditation 20
Figure 5-2. Applying for FedRAMP Accreditation 21
Figure 5-3. 3PAO Accreditation Process 22
Figure 5-4. Maintaining 3PAO Status 23
Figure 6-1. Security Assessment High Level Overview 25
Figure 6-2. Initiating a Request 26
Figure 6-3. Documenting Security Controls 29
Figure 6-4. Performing Security Testing 31
Figure 6-5. Finalizing the Security Assessment 33
Figure 7-1. Leveraging the Authorization Process 34
Figure 7-2. Security Control Responsibilities 35
Figure 8-1. Ongoing Assessment and Authorization 38
Figure 8-2. Operational Visibility 39
Figure 8-3. Change Control Process 40
Figure 8-4. Reporting a Security Incident 42

1. About this document

This document provides guidance on the operations of the Federal Risk and Authorization Management Program (FedRAMP). The relationships between this document and other reference documents for FedRAMP are illustrated in Figure 1-1.

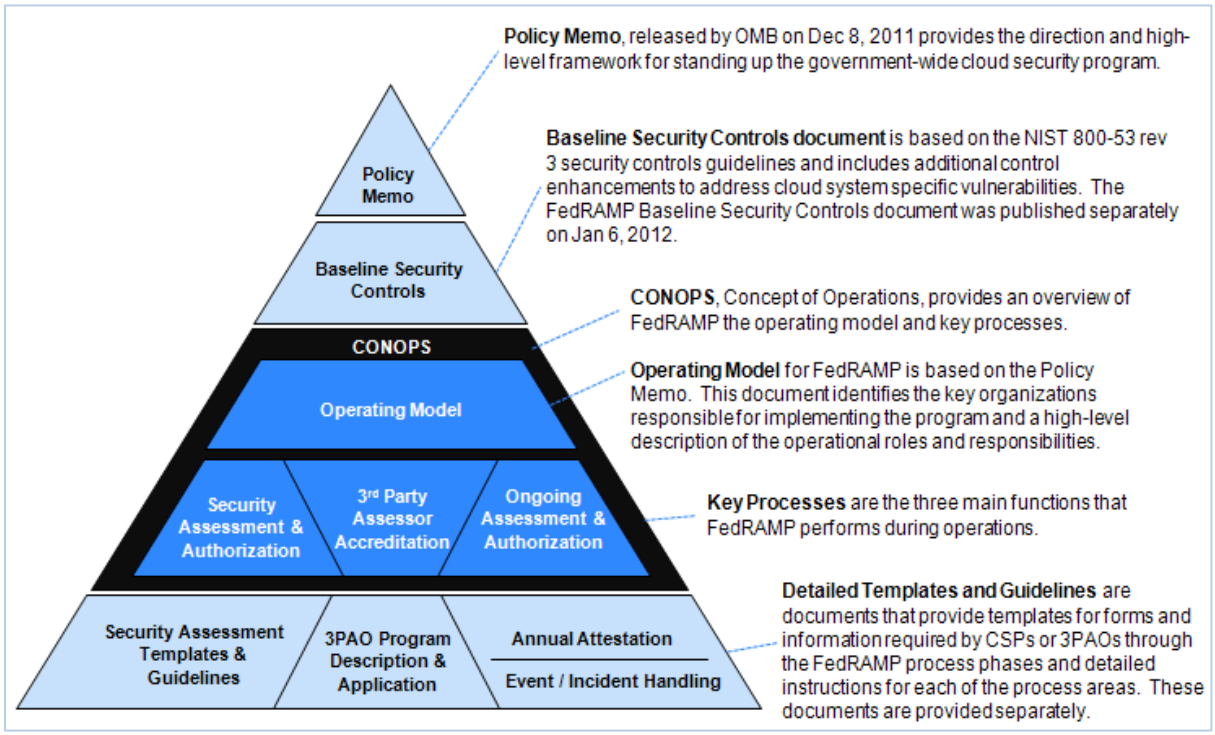

Figure 1-1. Relationship of FedRAMP Publications

1.1. Who should use this document?

This document is intended for Cloud Service Providers (CSPs), Third Party Assessment Organizations (3PAOs), government employees and contractors working on FedRAMP projects, and any outside organizations that want to use or understand the FedRAMP assessment process.

1.2. How this document is organized

This document is divided into sections and many include subsections.

- Section 1 describes how this document is organized and identifies the document audience.
- Section 2 describes the purpose of FedRAMP and defines the relationship between internal and external stakeholders.
- Section 3 describes FedRAMP operational areas, the phased implementation approach and the FedRAMP priority queue.
- Section 4 describes how to use FedRAMP and how a CSP and agency can leverage FedRAMP security assessment packages.

- Section 5 describes the role of 3PAOs within FedRAMP, the application process for the 3PAO, FedRAMP requirements for 3PAOs and the criteria by which information systems will be evaluated.
- Section 6 describes the approach for performing FedRAMP security assessment for cloud computing systems.
- Section 7 describes how to leverage a Provisional Authorization.
- Section 8 describes the ongoing assessment and authorization (continuous monitoring) process for cloud computing systems/services with FedRAMP Provisional Authorization.
- Section 9 provides references, guidance, and regulations related to FedRAMP.
- Section 10 provides a list of all deliverables and their point of use in the FedRAMP program.
- Section 11 provides a list of acronyms.

1.3.How to contact us

If you have questions about FedRAMP or something in this document, please send messages to:

info@FedRAMP.gov

For more information about the FedRAMP project, please see the website at:

http://www.FedRAMP.gov.

2. FedRAMP Definition and purpose

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that will save cost, time, and staff required to conduct redundant agency security assessments.

The purpose of FedRAMP is to:

- Ensure that cloud based 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.

FedRAMP uses a security risk model that can be leveraged among agencies based on a consistent security baseline. FedRAMP provides processes, artifacts and a repository that enables agencies to leverage authorizations with:

- Standardized security requirements and ongoing cyber security for selected information system impact levels;
- Conformity assessment program that identifies qualified independent, third-party assessments of security controls implemented by CSPs;
- Standardized contract language to help agencies integrate FedRAMP requirements and best practices into acquisitions;
- Repository of authorization packages for cloud services that can be leveraged government-wide; and
- Standardized Ongoing Assessment and Authorization processes for multi-tenant cloud services.

2.1. Stakeholders

The FedRAMP stakeholders include entities from across the Federal government and industry. In general, executive agencies serve in a governance and review capacity in the JAB and ongoing assessments; CSPs are applicants to the process, assisted by the 3PAOs; all agencies are potential consumers for Provisional Authorizations. The Program Management Office (PMO) is the coordinator of the process and conducts initial reviews. Relationships among the stakeholders are depicted in Figure 2-1.

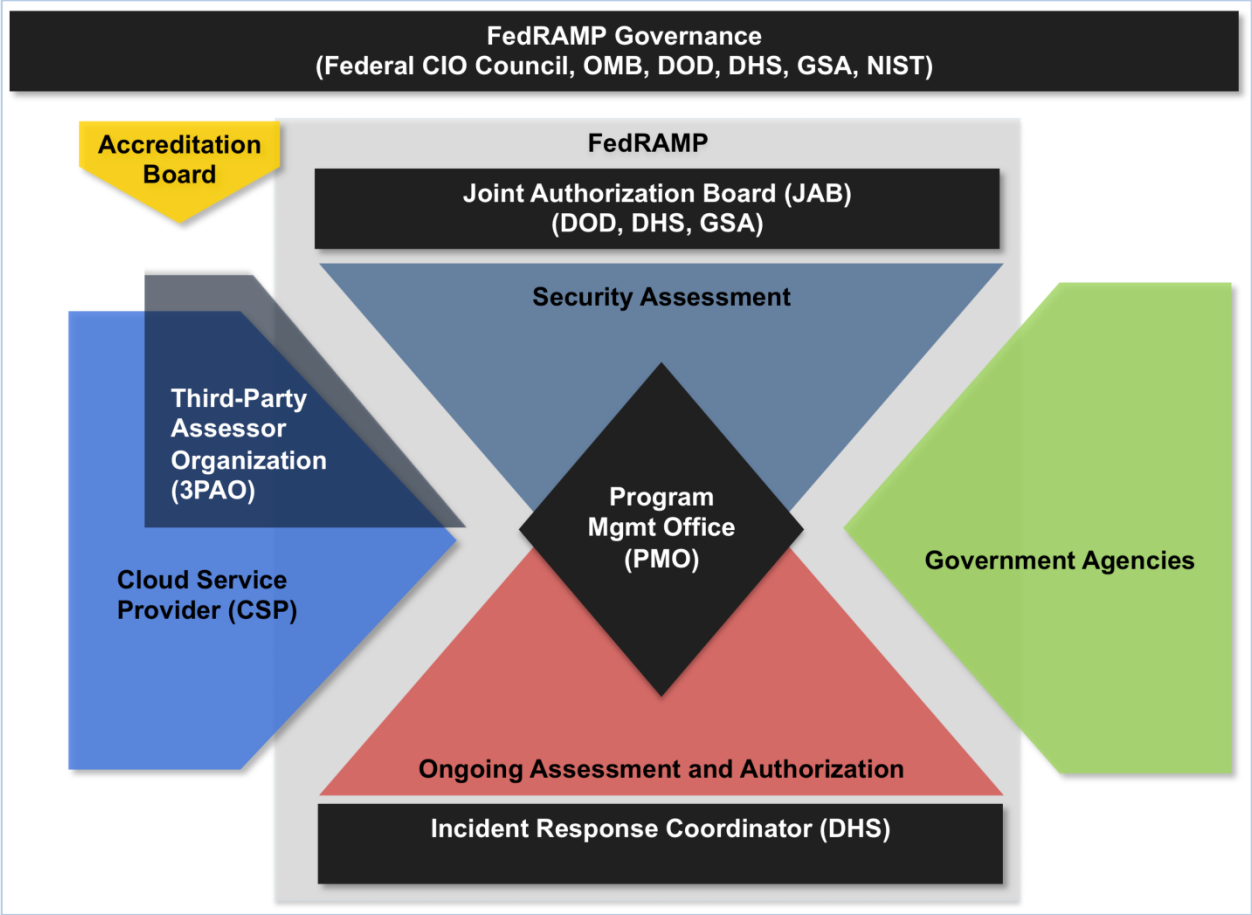

Figure 2-1. FedRAMP Stakeholders

Stakeholder responsibilities are established by OMB in the FedRAMP Policy Memo and are further delineated in the Joint Authorization Board charter. Table 2-1 details the responsibilities of each stakeholder.

Table 2-1. FedRAMP Stakeholder Roles

Role	Duties and Responsibilities
JAB Members (Chief Information Officers from GSA, DHS, and DOD)	• Define and update FedRAMP baseline security controls • Approve accreditation criteria for third-party assessment organizations. • Establish the priority queue, which sets the order in which the FedRAMP PMO performs the review of security packages. • Review security assessment packages for CSPs granted Provisional Authorizations • Ensure Provisional Authorizations are reviewed and updated regularly, notify agencies of changes to or removal of Provisional Authorizations
JAB Technical Representatives	• Provide subject matter expertise to the JAB Authorizing Official • Support FedRAMP PMO 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

Role	Duties and Responsibilities
FedRAMP Program Management Office (PMO) (GSA)	• Create processes for agencies and CSPs to request FedRAMP security authorization • Create a framework for agencies to leverage security authorization packages processed by FedRAMP • Work in coordination with DHS to establish a framework for continuous monitoring, incident response and remediation, and FISMA reporting. • Establish a secure repository for authorization packages that Agencies can leverage to grant security authorizations • Coordinate with NIST to implement a formal conformity assessment to accredit 3PAOs • Develop templates for standard contract language and service level agreements (SLAs), Memorandum of Understanding (MOU) and/or Memorandum of Agreement • Serve as a liaison to ensure effective communication among all stakeholders
Department of Homeland Security (DHS)	• Assist government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cyber security • Coordinate cyber security operations and incident response • Develop continuous monitoring standards for ongoing cyber security of Federal Information systems • Develop guidance on agency implementation of the Trusted Internet Connection (TIC) program with cloud services
Agencies	• Use the FedRAMP process when conducting risk assessments, security authorizations and granting an ATO to a cloud service • Ensure contracts require CSPs to comply with FedRAMP requirements and maintain FedRAMP Provisional Authorization • Provide to the Federal CIO an annual certification in listing all cloud services that the agency determines cannot meet FedRAMP requirements with appropriate rationale and proposed resolutions • Assess, authorize and continuously monitor security controls that are the Agency's responsibility
Cloud Service Provider *Either commercial or agency operator*	• Implement security controls based upon FedRAMP security baseline • Create security assessment packages in accordance with FedRAMP requirements. • Contract with an independent 3PAO to perform initial system assessment and required ongoing assessments and authorizations • Maintain Continuous Monitoring programs • Comply with Federal Requirements for Change Control and Incident Reporting
Third Party Assessment Organization (3PAO)	• Maintain compliance with FedRAMP 3PAO requirements for independence and technical competence • Independently performs security assessments of CSP systems and creates security assessment package artifacts in accordance with FedRAMP requirements

2.2.FedRAMP Governance and Roles

The FedRAMP Policy Memo establishes FedRAMP governance between Executive branch entities as illustrated in Figure 2-2. These entities are:

- JAB - performs risk authorization and grants the provisional ATO; members are the CIOs from the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Department of Defense (DoD);
- FedRAMP PMO – responsible for operational management;
- NIST –provides technical assistance to the 3PAO process, maintains FISMA standards and establishes technical standards;
- Federal CIO Council – coordinates cross agency communications; and
- DHS – monitors and reports on security incidents and provides guidelines for continuous monitoring.

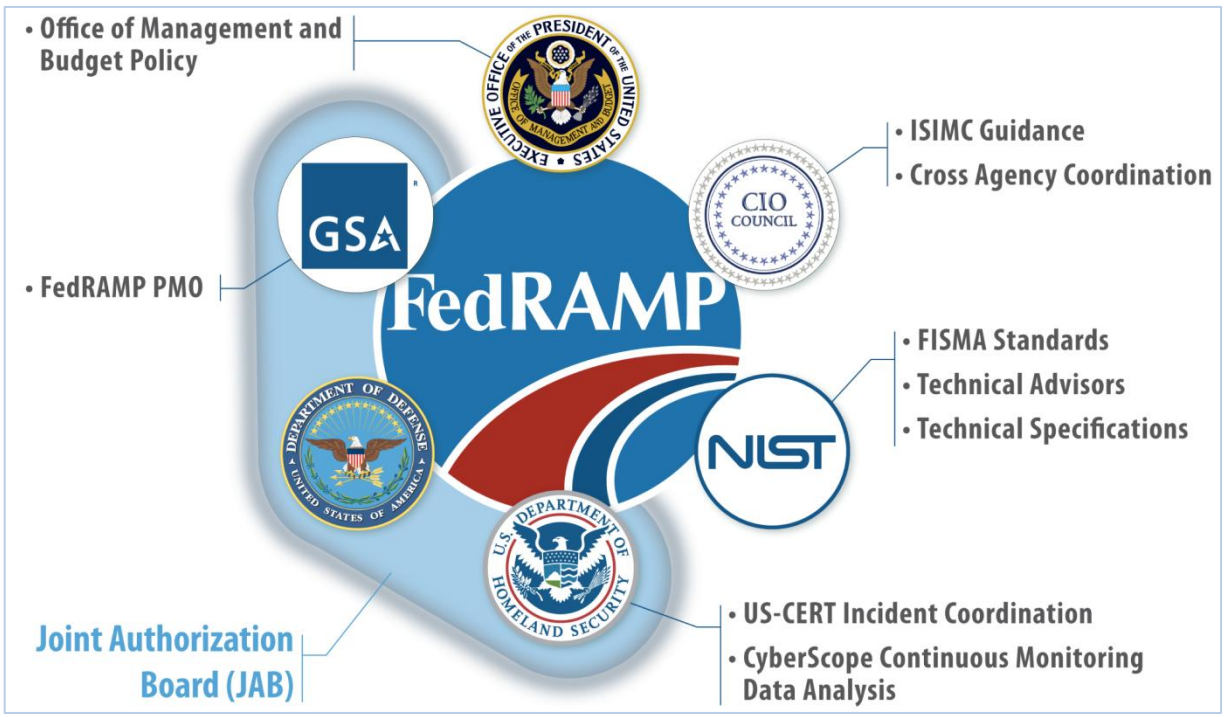

Figure 2-2. FedRAMP Governance Entities

`

3. High Level Operations

FedRAMP is a government-wide, standardized approach to security assessments and ongoing assessments and authorizations (continuous monitoring) designed to save cost, time, and staff required to assess and authorize cloud services. FISMA requires Federal agencies to accept the risk and authorize cloud systems at the agency level. Accordingly, the FedRAMP Policy Memo requires Federal agencies to use FedRAMP when assessing, authorizing, and continuously monitoring cloud services in order to aid agencies in this process as well as save government resources and eliminate duplicative efforts.

The FedRAMP security authorization process has four distinct areas:

- Security Assessment;
- Leverage the Authority to Operate (ATO);
- Ongoing Assessment and Authorization (Continuous Monitoring); and
- 3PAO Accreditation.

Figure 3-1 illustrates the relationship of these processes.

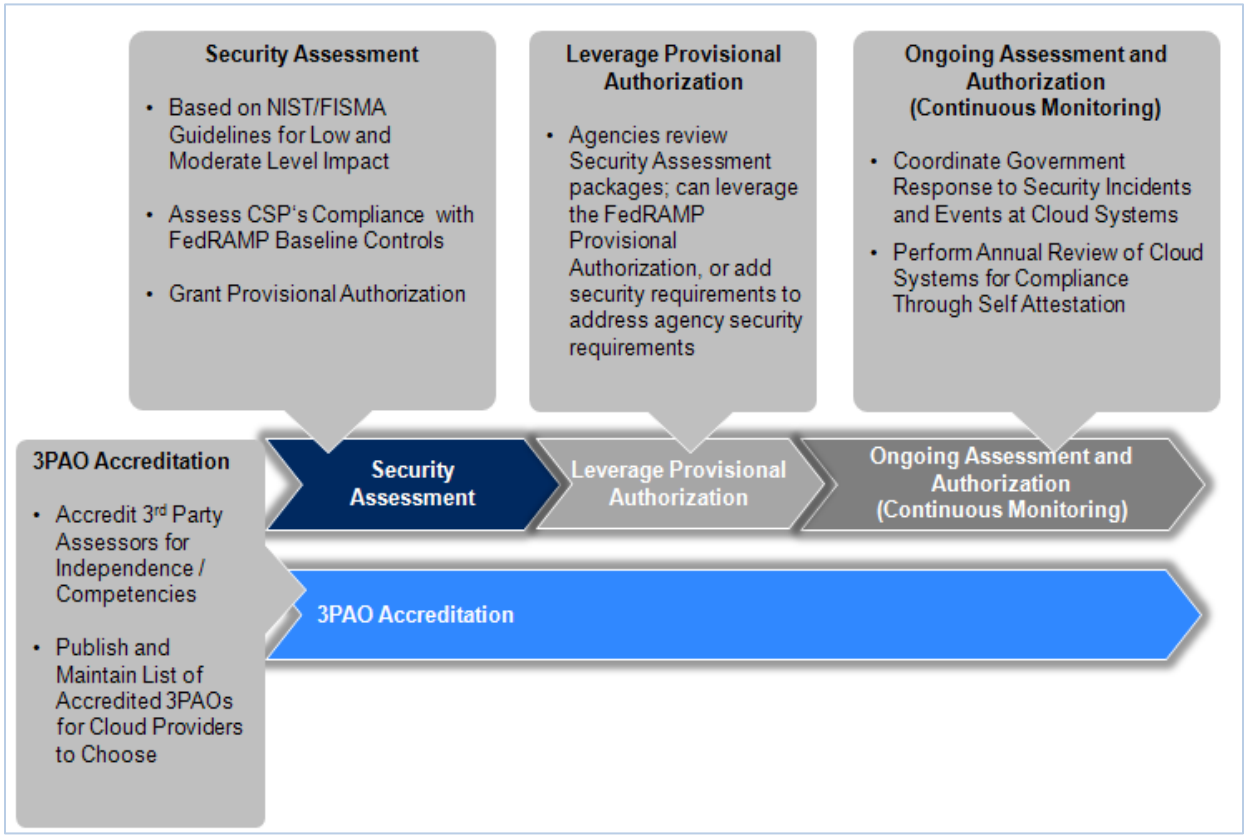

Figure 3-1. FedRAMP Process Areas

Security Assessment. A CSP or an agency may request a provisional ATO granted by the JAB under the FedRAMP security assessment process. The process follows the NIST 800-37 risk

management framework as tailored for a shared responsibility environment. The CSP identifies the appropriate baseline; implements appropriate security controls, and documents the implementation. The CSP contracts with an accredited 3PAO to independently verify and validate their security implementations and their security assessment package. The CSP submits the package to FedRAMP for review. Once documentation and test results are completed, the assessment is measured against the FedRAMP requirements and if the JAB is satisfied that the risks are acceptable, a Provisional Authorization is granted. Agencies can then leverage the JAB Provisional Authorization as the baseline for granting their own ATO.

Leverage ATO. The PMO will maintain a repository of FedRAMP Provisional Authorizations and associated security assessment packages for agencies to review. Agencies can use the Provisional Authorizations and security assessment packages as a baseline for granting their own ATO. If necessary, agencies can add additional controls to the baseline to meet their particular security profile.

Ongoing Assessment and Authorization (Continuous Monitoring). For systems with a Provisional Authorization, FedRAMP, in conjunction with DHS, conducts ongoing assessment and authorization (continuous monitoring) activities. Ongoing assessment and authorization (continuous monitoring) determines if the set of deployed security controls continue to be effective over time.

3PAO Accreditation. CSPs applying for an ATO must use an accredited 3PAO. A review board, with representation from NIST and the FedRAMP PMO, accredits 3PAOs. The approval process requires applicants to demonstrate their technical capabilities and their independence as an assessor. The approval process follows the conformity assessment approach outlined in ISO/IEC 17020. FedRAMP maintains a list of approved 3PAO from which CSPs can choose.

3.1. Phased Approach

FedRAMP is implemented in a phased approach starting with an initial operating capability, growing into sustaining operations. The FedRAMP PMO is responsible for managing the phased implementation. The phased approach is detailed in Figure 3.

	FY12	FY12	FY13 Q2	FY14
	Pre-Launch Activities	**Initial Operational Capabilities (IOC)**	**Full Operations**	**Sustaining Operations**
	FedRAMP Finalizes Requirements and Documentation in Preparation of Launch	*Launch IOC with Limited Scope and Cloud Service Provider (CSP)s*	*Execute Full Operational Capabilities with Manual Processes*	*Move to Full Implementation with On-Demand Scalability*
Key Activities	• Publish FedRAMP Requirements (Security Controls, Templates, Guidance) • Publish FedRAMP Compliance Guidance for Agencies • Accredit 3PAOs • JAB establishes Priority Queue for FedRAMP review of packages	• Authorize CSPs • Update CONOPS, Continuous Monitoring Requirements and CSP Guidance	• Conduct Assessments & Authorizations • Identify Scale Operations to Authorize More CSPs	• Implement Electronic Authorization Repository • Scale to Steady State Operations
		Gather Feedback and Incorporate Lessons Learned		
Outcomes	• Initial List of Accredited 3PAOs • Launch FedRAMP in to Initial Operating Capabilities	• Initial CSP Authorizations • Established Performance Benchmark	• Multiple CSP Authorizations • Define Business Model • Measure Benchmarks	• Authorizations Scale by Demand • Implement Business Model • Self-Sustaining Funding Model Covering Operations • Privatized Accreditation Board

Figure 3-2. FedRAMP Program Phases

3.2. Priority Queue

The Joint Authorization Board has the responsibility to establish the priority queue that determines the order in which security assessments are processed within the FedRAMP PMO based on available resources.

The JAB has defined the priority queue as:

> "FedRAMP will prioritize the review of cloud systems with the objective to assess and authorize cloud systems that can be leveraged government-wide.
>
> In order to accomplish this, FedRAMP will prioritize secure Infrastructure as a Service (IaaS) solutions, contract vehicles for commodity services, and shared services in alignment with the Administration's 'Cloud First' policy as discussed in the '25 Point Implementation Plan to Reform Federal Information Technology Management'.
>
> When reviewing cloud systems according to this priority, there are two distinct categories of cloud systems: (1) cloud systems with existing Federal agency Authority to Operate (ATO) designations and (2) cloud systems without an existing Federal agency ATO."

3.3. FedRAMP Program Change

As FedRAMP evolves and matures, the Joint Authorization Board will approve program updates that affect risk authorization. Changes requiring stakeholder compliance will be published with timelines for compliance. The FedRAMP requirements, templates, and supporting instructional materials may change over time. Updates to the program will be posted on www.FedRAMP.gov.

4. How to Use FedRAMP

Federal agencies, CSPs, and 3PAOs will use FedRAMP differently, but must all understand and use the FedRAMP security controls baseline and accompanying requirements. FedRAMP has defined the security control baseline for low (L-L-L) and moderate (M-M-M) impact level systems as defined by FIPS 199. This security controls were selected from the NIST catalog of controls and enhancements as described in Special Publication 800-53 as revised. Additionally, FedRAMP has defined additional requirements that agencies, CSPs, and 3PAOs must meet. These additional requirements include using FedRAMP templates, test cases, and ongoing assessment and authorization processes. All additional requirements are detailed in subsequent sections of this document.

4.1. Federal agencies

Federal agencies must use the baseline controls and accompanying FedRAMP requirements (templates, test cases, guidance) when leveraging assessments and authorizations or initiating assessments for cloud services. After granting an authorization, Federal agencies must then establish a security and privacy incident response and mitigation capability in accordance with DHS guidance to ensure the security controls are continuously monitored. Federal agencies must ensure these requirements are all met through contractual relationships with CSPs.

4.1.1. Leveraging Authorizations

Federal agencies are required by the FedRAMP Policy Memo to use FedRAMP when conducting risk assessments, security authorizations, and granting an ATO for cloud services. Agencies begin using FedRAMP by viewing the FedRAMP repository to see if it contains an assessment or authorization package for a cloud system an Agency is using or might procure.

If a cloud system is in the FedRAMP repository, Federal agencies can then leverage the security assessment package as detailed in Section 7.

4.1.2. Initiating Assessments with FedRAMP

If an Agency selects a CSP service that is not listed in the FedRAMP repository, the agency must use the FedRAMP PMO process and the JAB-approved FedRAMP security authorization requirements as a baseline for granting an ATO. Federal agencies may do this through initiating the process with the FedRAMP PMO and JAB detailed in Section 6 or by completing the FedRAMP process within their respective agency.

Once an agency has completed the assessment of a cloud system and granted an ATO, the Agency must submit a completed package (using the FedRAMP requirements) to the FedRAMP PMO for inclusion in the FedRAMP repository, which can be used by other Federal agencies to leverage the authorization package.

4.1.3. Implement Ongoing Assessment and Authorization (Continuous Monitoring)

Once a Federal agency has granted an ATO for a cloud system they must ensure they implement an ongoing assessment and authorization (continuous monitoring) capability to ensure the cloud system maintains and acceptable risk posture. Federal agencies must work with CSPs to implement an ongoing assessment and authorization plan to cover security and privacy incident response and mitigation capabilities. The FedRAMP requirements provide the necessary

elements for Agencies to ensure that they have a fully implemented ongoing assessment and authorization capability in accordance with all DHS guidance.

4.1.4. Ensure FedRAMP Requirements Are Met Contractually

Federal agencies are required to ensure that FedRAMP requirements are met through contractual provisions. This is to ensure that a CSP has a legal obligation to meet and maintain the FedRAMP requirements. To assist agencies in meeting this requirement, FedRAMP will provide standard template contract clauses and accompanying SLA guidance covering all FedRAMP requirements. Federal agencies can leverage these during the procurement process for acquiring cloud services.

4.2. Cloud Service Providers

Cloud Service Providers wishing to provide services to Federal agencies must use the baseline controls and accompanying FedRAMP requirements. CSPs can follow the security authorization process to categorize the system, implement controls, and document the implementations. A CSP must then use an accredited 3PAO to independently test their implementations. The completed security assessment package can be submitted either to the FedRAMP PMO, or a contracting agency. After a Federal agency commences operation on a CSP system, they must follow the ongoing assessment and authorization processes.

4.3. Third Party Assessment Organizations (3PAO)

Accredited Third Party Assessor Organizations (3PAO) play a critical role in the FedRAMP security assessment process. Accredited 3PAO have demonstrated independence and technical competency required to testing the security implementations and collect representative evidence. The resulting security assessment report and supporting evidence make up a key requirement for leveraging agencies to use FedRAMP security assessment packages. The 3PAO accreditation process is further described next in Section 5.

5. Third-Party Assessment Organizations

In the security assessment process, FedRAMP requires that CSP services and systems be assessed by an accredited 3PAO. Accredited 3PAOs are required to meet the ISO/IEC 17020:1998 standards for independence and managerial competence and meet FedRAMP requirements for technical FISMA competence through demonstrated expertise in assessing cloud-based solutions. The accreditation process for 3PAOs is based on the concept of conformity assessment – a methodology to demonstrate capability in meeting requirements relating to a product, process, system, person or body as defined by ISO/IEC 17020.

For FedRAMP, the conformity assessment ensures that accredited 3PAOs consistently perform security assessments with the appropriate level of rigor and independence. FedRAMP will only review security assessment packages from CSPs that have been assessed by an accredited 3PAO. In addition to the initial security assessment, 3PAOs perform periodic assessment of CSP systems to, provide evidence of compliance, and play an ongoing role in ensuring that CSPs continue to meet FedRAMP requirements. This section will detail how FedRAMP will use a conformity assessment process to accredit 3PAOs. A high level view of this process is described in Figure 5-1.

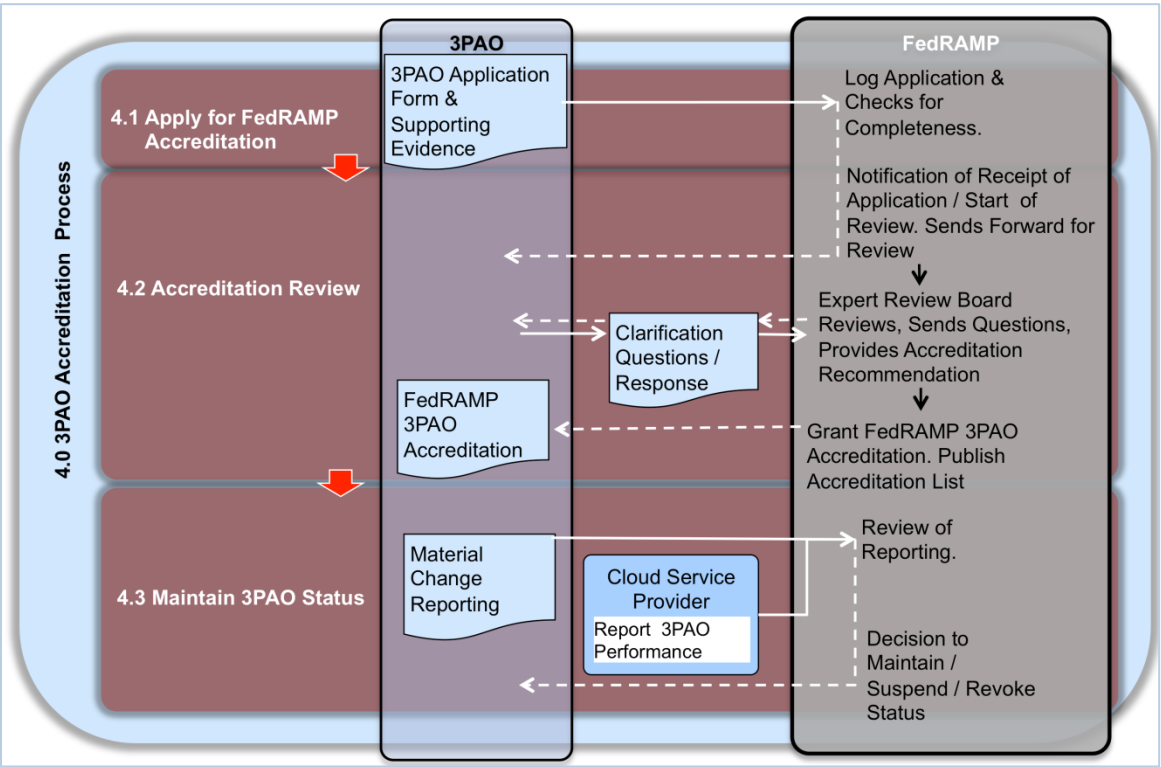

Figure 5-1. Third Party Assessor Organization Accreditation

Additional information about the 3PAO accreditation process, including all documents needed to apply for accreditation, are available at www.FedRAMP.gov/3PAO. Questions about this process should be directed to 3PAO@FedRAMP.gov.

There are four phases of 3PAO accreditation: applying for accreditation, accreditation review, maintain 3PAO status. These phases are detailed in the sections that follow.

5.1. Applying for FedRAMP Accreditation

To become a FedRAMP 3PAO, organizations must first submit an application. The 3PAO application requires 3PAOs to show they meet requirements in two areas:

- Independence and management system standards, and
- Technical FISMA competency.

For independence and management system standards, applicants must show that they conform to standards and requirements contained within ISO/IEC 17020:1998 for Type A or Type C organizations. For technical FISMA competency, applicants must demonstrate technical competency by completing a security assessment of a hypothetical cloud system based on a subset of the FedRAMP security controls. As part of this demonstration, the 3PAO must develop abbreviated system security plan (SSP), system assessment plan (SAP), and security assessment report (SAR) using the provided templates. The 3PAO must also explain the methodology used to perform the demonstration assessment, and provide evidence and findings from the simulated execution of the abbreviated SAP. This process is illustrated in Figure 5-2.

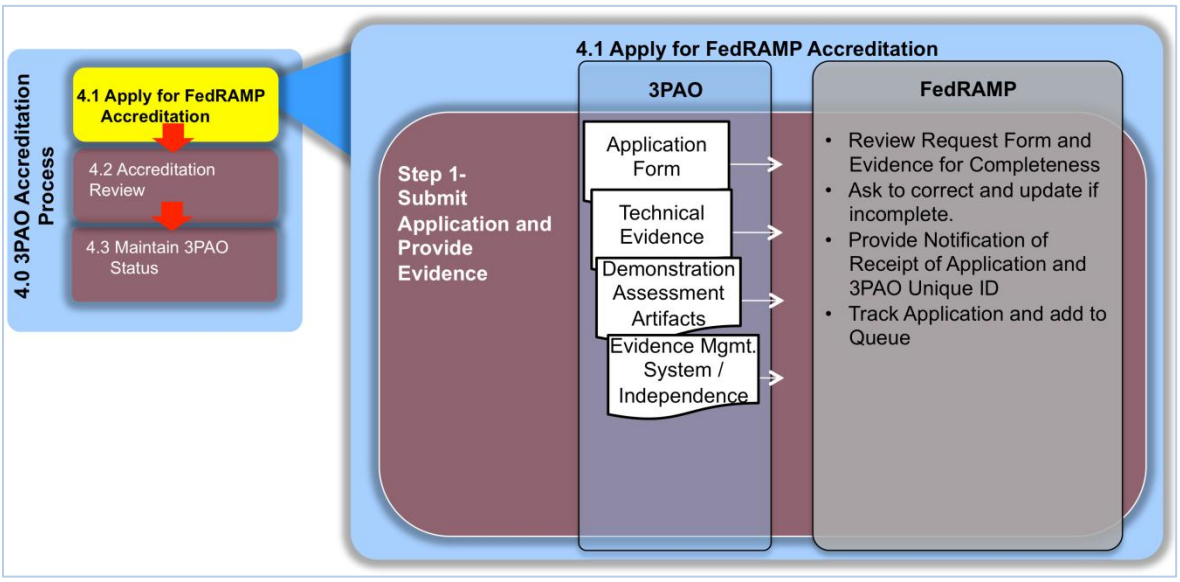

Figure 5-2. Applying for FedRAMP Accreditation

5.2. 3PAO Accreditation Evaluation

After a 3PAO submits an application to FedRAMP, the FedRAMP PMO will coordinate review of the application by an Expert Review Board (ERB). The FedRAMP PMO has established an ERB comprised of management, independence, and cyber security experts from NIST and GSA. This ERB reviews 3PAO applications to determine if they conform to the published FedRAMP requirements.

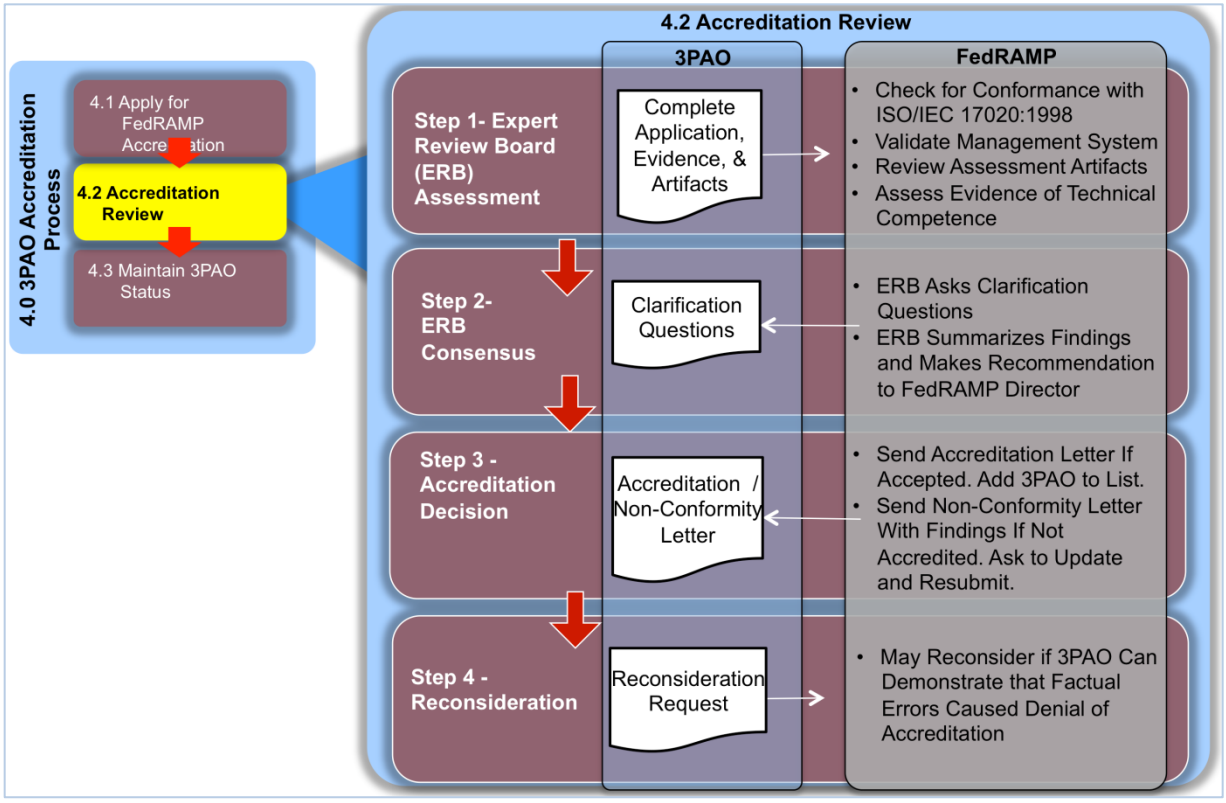

Figure 5-3. 3PAO Accreditation Process

The ERB will review 3PAO applicants and provide a recommendation to the FedRAMP Director regarding accreditation. The FedRAMP Director will be the authority that issues accreditation decisions for 3PAO applicants. If a 3PAO is accredited, they will be publicly listed on FedRAMP.gov as an accredited 3PAO and may begin work with CSPs who wish to obtain a FedRAMP Provisional Authorization. If a 3PAO is denied accreditation, the 3PAO applicant will receive a document detailing the findings of non-conformance. 3PAOs can re-apply with new evidence of conformance or apply for reconsideration if they believe the denial was based on a factual error in the accreditation decision. Review of 3PAO applications will be on an ongoing basis and reviewed on a first come, first served basis. The accreditation review process is illustrated in Figure 5-3.

5.3. Maintaining the Accreditation

After receiving 3PAO accreditation status, the 3PAO must maintain their accreditation by complying with FedRAMP requirements. 3PAOs must notify the FedRAMP PMO of any material changes that could affect its ability to perform assessments or maintain its independence and management system standards in accordance with ISO 17020:1998. FedRAMP will also monitor the quality of security assessment packages received as well as feedback from CSPs and agencies on the performance of accredited 3PAOs. Failure to meet FedRAMP requirements could result in the temporary suspension or permanent revocation of the 3PAO's accredited status and removal from the accredited 3PAO list. 3PAOs also have the option of requesting that FedRAMP withdraw their accredited status. This process is depicted in Figure 5-4 below.

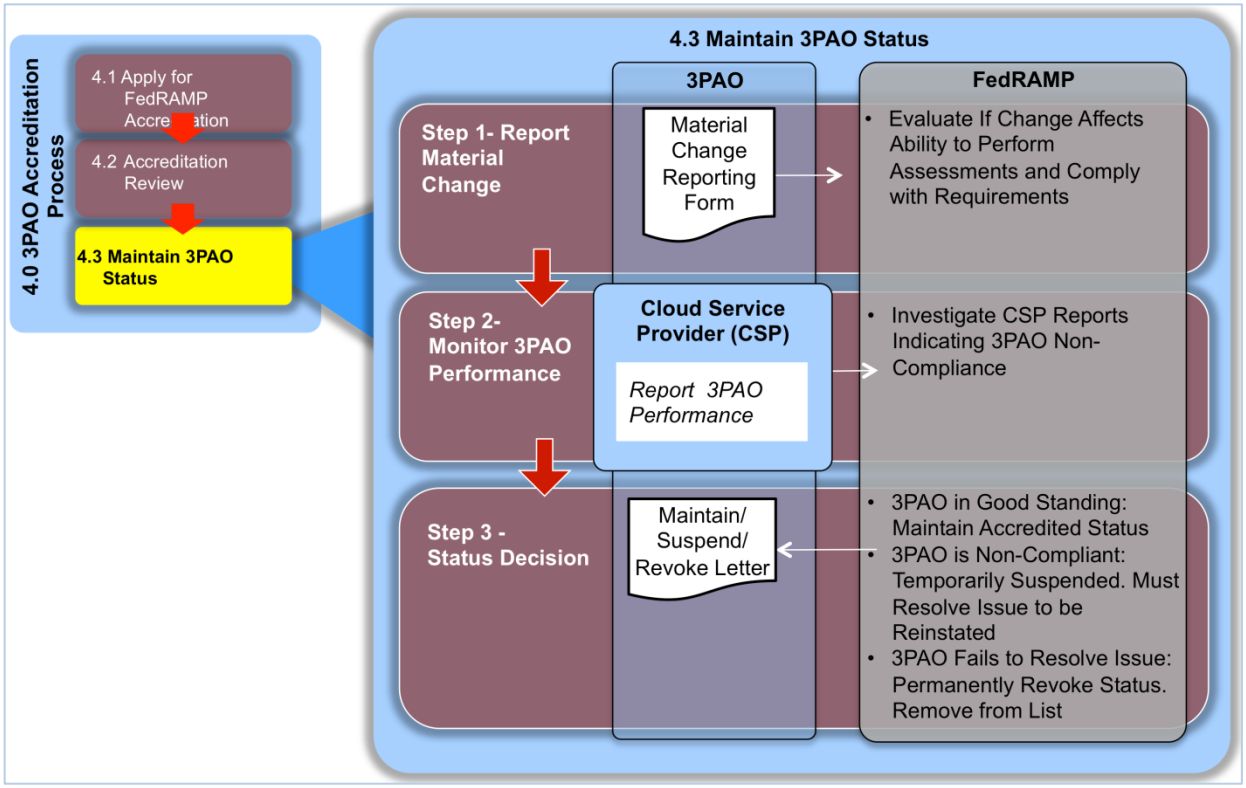

Figure 5-4. Maintaining 3PAO Status

5.4. Transitioning to a Privatized Board

The accreditation process will eventually migrate to a board managed by private sector organizations. The privatized board will be responsible for assessment and accreditation of 3PAOs. This board will still assess and accredit 3PAOs according to the standards as defined by the FedRAMP JAB and PMO.

After the private sector accreditation body has been established, the FedRAMP PMO will establish a transition timeframe for all 3PAOs to be accredited by the privatized board. During this transition timeframe, FedRAMP will accept security assessment packages that use either a 3PAO that was accredited by the ERB or a 3PAO accredited by the privatized board. 3PAOs accredited under the initial ERB process will have to transition to the privatized accreditation during the transition timeframe detailed by the FedRAMP PMO.

The transition to a privatized board will be defined in a subsequent publication by FedRAMP.

6. Security Assessments

Federal agencies are required to assess and authorize information technology systems in accordance with FISMA. The FedRAMP security assessment process is compliant with FISMA and is based on NIST *Special Publication 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems*. FedRAMP defines a set of controls for low and moderate impact level systems based on NIST baseline controls (SP 800-53 as revised) with a set of control enhancements that pertain to the unique security requirements of cloud computing.

The FedRAMP security assessment process is designed to align with what Federal agencies do now when assessing and authorizing cloud systems. This allows Federal agencies to meet FedRAMP requirements if a cloud system they wish to authorize is not prioritized for review by the JAB (discussed previously in Sections 3.2 and 4.1.2). FedRAMP uses the same documents and deliverables that NIST requires agencies to use in the SP 800-37 framework. The only part of the FedRAMP process that is new to Federal agencies is detailed in section 6.1 and involves the Control Tailoring Workbook and Control Implementation Summary. These two documents help delineate security responsibility and how the CSP plans to address the security controls on their system.

Agencies and CSPs can both apply to FedRAMP to initiate an assessment of a cloud service. All CSP security assessment packages must use an accredited 3PAO to verify and validate its security assessment package before it is submitted for FedRAMP review. The FedRAMP office coordinates the work between the JAB, the JAB technical representatives (TRs) and also serves as a liaison between the CSP, 3PAOs, and Federal agencies.

During the initiation of this process, FedRAMP and the CSP will define timeframes for submission and review of documents to ensure the process is as efficient and timely as possible. Timeframes will not be the same for every CSP due to difference in the size, complexity of the system being authorized as well as any previous FISMA and security authorization experience of the CSP. FedRAMP will work with CSPs to create timeframes that are reasonable and all parties feel comfortable they will be able to meet.

During the entire security assessment process, from the initiation and creation of the security plan through the submission of a finalized security assessment package, the CSP and FedRAMP office are in constant communications to address questions, solve challenges, and make the FedRAMP process as fast and seamless as possible.

A high level illustration of the security assessment process is found in Figure 6-1.

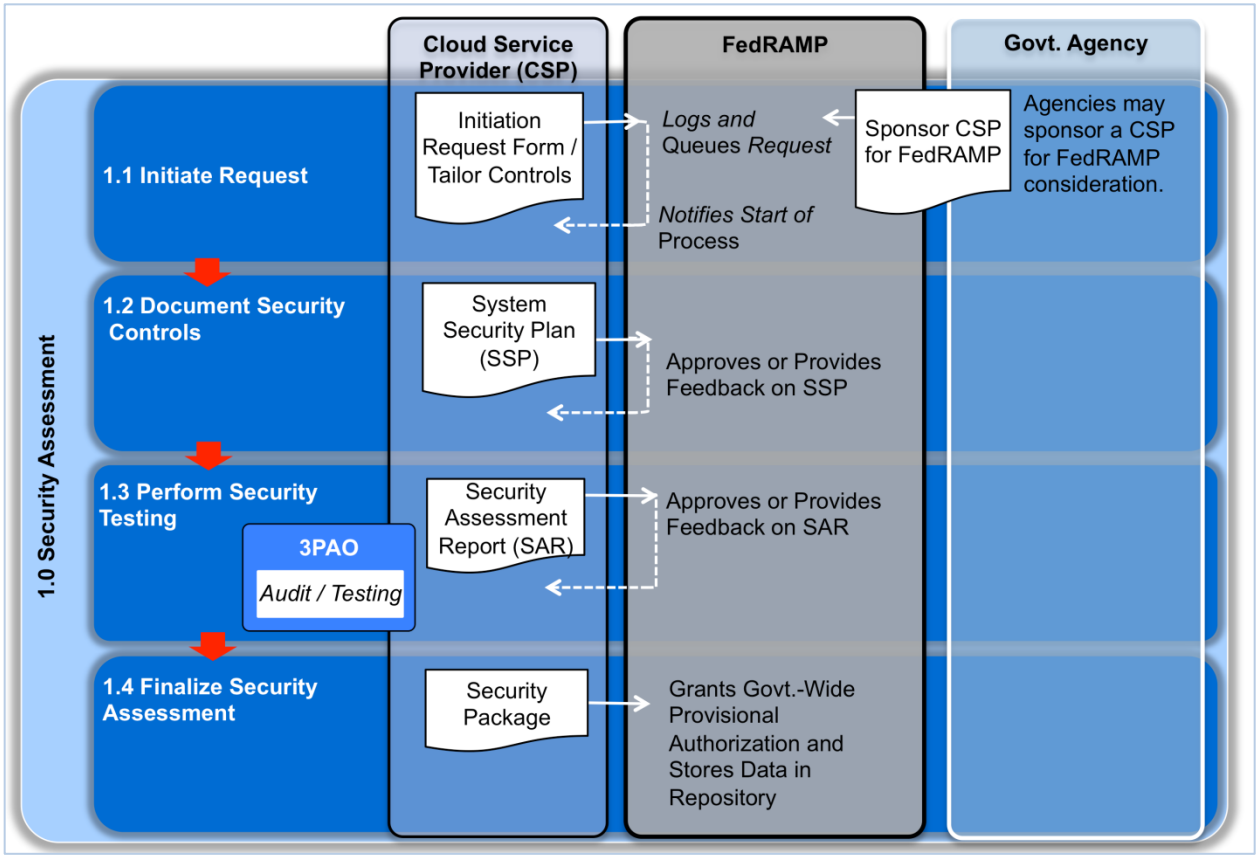

Figure 6-1. Security Assessment High Level Overview

The FedRAMP process can be viewed as linear and continuous with distinct steps that allow for the review and approval at each step. While it is expected that this process will require interactions and iterations, CSPs are limited to two resubmissions of each security assessment document for JAB review.

6.1. Initiating A Request

The initiation request process area is designed to help the CSP and FedRAMP understand the scope of services and current security implementations. This process, as illustrated in Figure 6-2 has four key steps. This process begins with the CSP initiating a request for FedRAMP authorization and is completed when the Control Implementation Summary, a FedRAMP document identifying the current security implementation status and responsibilities has been approved.

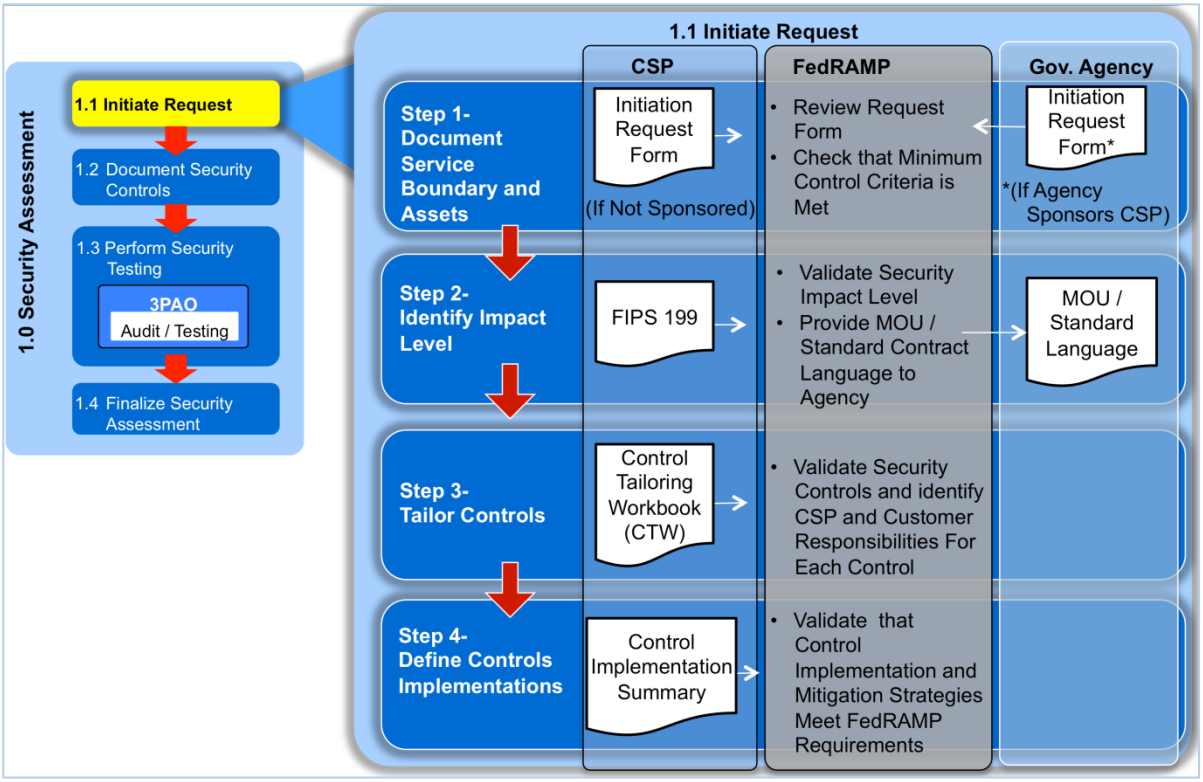

Figure 6-2. Initiating a Request

In order to initiate the FedRAMP process, a CSP or Federal agency must submit a completed FedRAMP Request Form and Federal Information Processing Standards (FIPS) 199 worksheet to the FedRAMP PMO. Requests for FedRAMP review are placed in a queue that is maintained by the FedRAMP PMO. The queue order is determined by the JAB's Priority Queue criteria (detailed in section 3.2).

When a CSP begins the security assessment process they will be assigned an Information System Security Officer (ISSO) from the FedRAMP PMO. The ISSO kicks off the assessment and provides guidance on implementing security controls, creating required documentation, and performing security testing.

The ISSO is the main point of contact for the CSP and sponsoring agency during the assessment process. The ISSO is responsible for performing the initial review of the CSP's security assessment documents and providing feedback as the CSP goes throughout the security assessment process. ISSOs play a key role in assessing the CSP's authorization package, as the ISSO is responsible for the initial review of all security authorization documents submitted to FedRAMP.

In completing the FIPS 199 worksheet, the CSP must categorize what type of data is (or will be) contained within the system and determine the impact level for the system. The categorization is based upon NIST Special Publication 800-60 (Volumes I and II) Guide for Mapping Types of Information and Information Systems to Security Categories. Based upon the information in the FIPS 199 worksheet, the appropriate FedRAMP security control baseline is selected and the CSP will need to implement controls at that level to meet FedRAMP requirements. At this time,

FedRAMP only performs security assessments for systems that have a low or moderate impact levels.

The FedRAMP ISSO will notify the CSP that the initiation request and the FIPS 199 worksheet have been approved. The next step is a Memorandum of Agreement (MOA) issued between FedRAMP and the CSP. The MOA acknowledges the authority for FedRAMP to perform an assessment of the CSP's system. If an agency has requested FedRAMP to perform a review of a CSP's system and has contracted with the CSP, this department or agency will be considered the sponsoring agency for the CSP in which case a Memorandum of Agreement (MOA) will be issued between FedRAMP and the sponsoring agency as well.

After the CSP has signed the MOA, the ISSO will direct the CSP to fill out the Control Tailoring Workbook (CTW) and the Control Implementation Summary (CIS). The CTW pre-qualifies the system for FedRAMP review and determines if a CSP has exceptions to the FedRAMP requirements (usually in control implementations or control boundaries) that must be considered by the JAB for authorization. The CIS provides a summary of the controls and delineates responsibility for the implementation of each control. The CSP may need to modify the CIS as they develop their System Security Plan. The CTW and CIS assist the CSP in documenting the implementation of the controls, defining the control boundaries, and mapping responsibility for each control.

After completing the CTW and CIS templates, the CSP submits the documents to the FedRAMP PMO. The FedRAMP ISSO performs an initial review of the documents for completeness and compliance. If the documents are not acceptable, the ISSO will notify the CSP and include specific findings that describe how the documents need to be revised. Once the CIS and CTW are complete, the documents are sent to the JAB for review.

The JAB will review the CIS and CTW and examine any exceptions to determine the risk these exceptions will pose to Federal Data placed in that service environment. If the JAB accepts the CTW and CIS, the CSP will be notified that their security assessment will move forward to the Document Security Controls process step. If the JAB has specific concerns about the CTW and CIS, the CSP will also be informed and given an opportunity to address the JAB's findings and resubmit the documents. The CSP deliverables for the Initiate Request process area are described in Table 6-1.

Table 6-1. Initiate Request Deliverables

Deliverable	Description
FedRAMP Request Form	The FedRAMP request form is used by Federal agencies and CSPs to request initiation of the FedRAMP security assessment process.
FIPS 199 Categorization	The FIPS 199 Security categorization is used to determine the impact level to be supported by the cloud information system/service. The provider categorizes their system based on the data types currently stored and not leveraging agency data.
Control Tailoring Workbook (new for FedRAMP)	This document is used by CSP to document their control implementation and define their implementation settings for FedRAMP defined parameters and any compensating controls.

Deliverable	Description
Control Implementation Summary (new for FedRAMP)	This document summarizes the control ownership and indicates which controls are owned and managed by the CSP and which controls are owned and managed by the leveraging agency.

6.2. Documenting the Security Controls

Once the CSP has implemented the required security controls, the next process is to document the security control implementations in a System Security Plan (SSP). The SSP details the security authorization boundary, how the implementations address each required control and enhancement in the selected control baseline, descriptions of roles and responsibilities, and expected behavior of individuals with system access.

In order to completely and accurately document the security control implementation in the SSP, CSPs must provide supporting documents that need to be submitted as attachments. These supporting documents include: an e-Authentication Worksheet, a Privacy Threshold Analysis (and if applicable, a Privacy Impact Assessment), the CSP's Information Security Policies, User Guide for the cloud service, Rules of Behavior, an IT Contingency Plan, a Configuration Management Plan, and an Incident Response Plan. Templates for all of these documents will be available on www.FedRAMP.gov.

The CSP submits the SSP and all supporting documentation to their FedRAMP ISSO for review. The ISSO will work with the CSP on any required revisions. Once the SSP is in a final state, the ISSO submits the SSP to the JAB for review to ensure the SSP adequately addresses the security needed for that cloud system. If the JAB approves the SSP, the CSP will next move to the security testing step. If the JAB has specific concerns about the SSP, the CSP will be informed and given an opportunity to address the JAB's findings and resubmit the documents.

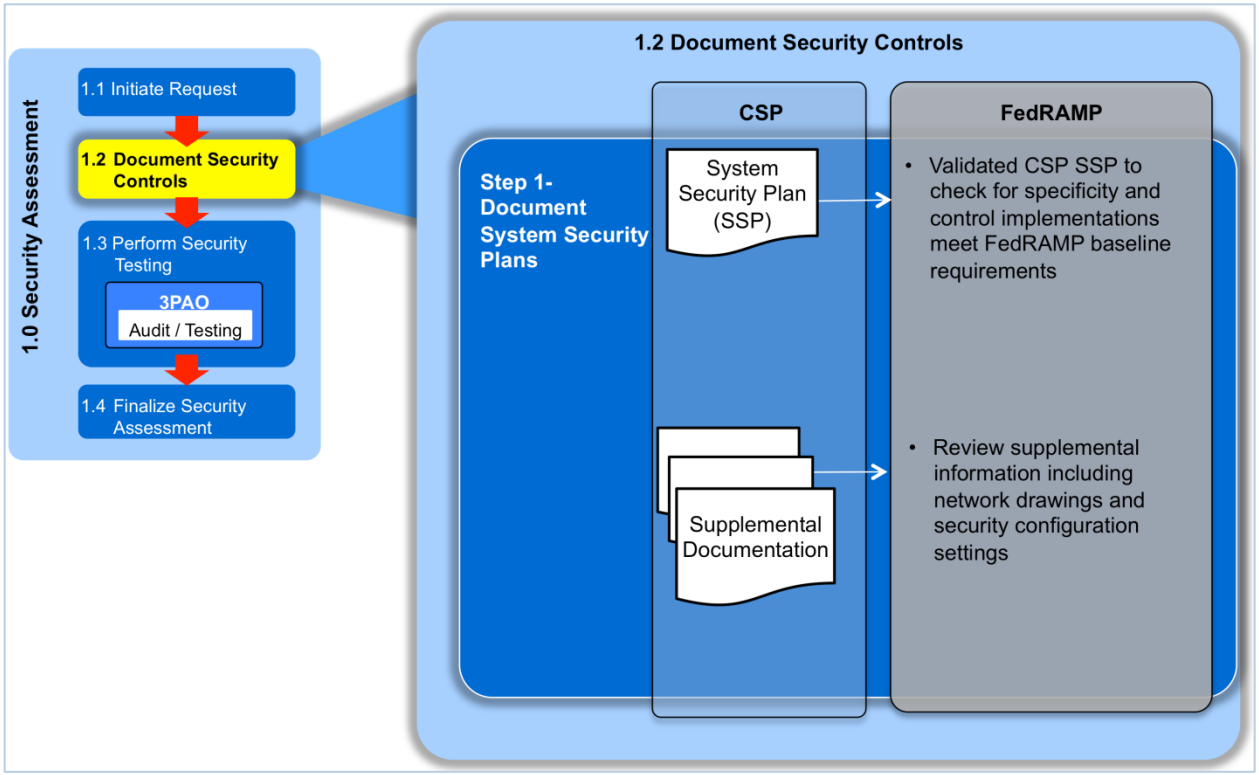

Figure 6-3. Documenting Security Controls

Documenting the security controls in the security assessment process is detailed in Figure 6-3; and the deliverables for this process area are described in Table 6-2.

Table 6-2. Document Security Controls Deliverables

Deliverable	Description
System Security Plan	This document describes how the controls are implemented within the cloud information system and its environment of operation. The SSP is also used to describe the system boundaries.
Information Security Policies	This document describes the CSP's Information Security Policy that governs the system described in the SSP.
User Guide	This document describes how leveraging agencies use the system.
Rules of Behavior	This document is used to define the rules that describe the system user's responsibilities and expected behavior with regard to information and information system usage and access.
IT Contingency Plan	This document is used to define and test interim measures to recover information system services after a disruption. The ability to prove that system data can be routinely backed up and restored within agency specified parameters is necessary to limit the effects of any disaster and the subsequent recovery efforts.
Configuration Management Plan	This plan describes how changes to the system are managed and tracked. The Configuration Management Plan should be consistent with NIST SP 800-128.

Deliverable	Description
Incident Response Plan	This plan documents how incidents are detected, reported, and escalated and should include timeframes, points of contact, and how incidents are handled and remediated. The Incident Response Plan should be consistent with NIST Special Publication 800-61.
E-Authentication Workbook	This template will be used to indicate if E-Authentication will be used in the cloud system and defines the required authentication level (1-4) in terms of the consequences of the authentication errors and misuse of credentials. Authentication technology is selected based on the required assurance level.
Privacy Threshold Analysis	This questionnaire is used to help determine if a Privacy Impact Assessment is required.
Privacy Impact Assessment	This document assesses what Personally Identifiable Information (PII) is captured and if it is being properly safeguarded. This deliverable is not always necessary.

6.3.Performing the Security Testing

Once the SSP has been approved, the CSP must begin work with accredited 3PAO. Once a CSP has contracted with an accredited 3PAO, they must submit a 3PAO Designation Form to the FedRAMP PMO. The 3PAO performs and independently tests the CSP's system to determine the effectiveness of the security control implementation. The JAB will only accept security assessment packages developed by an accredited 3PAO. Additional details on 3PAOs and the accreditation process are found in Section 5.

Once the 3PAO has been selected, the ISSO will hold a meeting with the CSP and 3PAO to discuss expectations and set timeframes for deliverables. The 3PAO creates a testing plan using the FedRAMP Security Assessment Plan (SAP) template. The SAP identifies all the assets within the scope of the assessment, including components such as hardware, software, and physical facilities. The SAP provides a roadmap and methodology for execution of the tests and indicates that the 3PAO will use the FedRAMP associated security test cases that are provided in the form of worksheets. The ISSO reviews and approves the SAP to ensure that the assessment will cover the stated authorization boundary and controls. The 3PAO performs an assessment of the CSP's controls in accordance with the SAP.

After the assessment of the controls has been completed, the 3PAO will generate a Security Assessment Report (SAR) that documents findings and provides an analysis of the test results to determine the risk exposure. The SAR also contains recommendations developed by the 3PAO to assist the CSP in mitigating security weaknesses.

After receiving the SAR from the 3PAO, the CSP develops a Plan of Action & Milestones (POA&M) that addresses the specific tasks, resources, and schedule for correcting each of the weaknesses and residual risks identified. The POA&M is a living document and lists current vulnerabilities within the system, along with the planned fix and a date that the fix will be implemented. The POA&M serves as a schedule and tracking system for the CSP's security "to do" list.

After completion of the POA&M, the CSP submits the SAR (with accompanying evidence) and the POA&M to the ISSO. The ISSO reviews the SAR and POA&M for completeness and overall risk posture. The ISSO then forwards the SAR and POA&M to the JAB for review. The JAB will review the SAR and POA&M to make a risk-based decision on whether to accept the vulnerabilities and planned fixes for the CSP's system to determine if that system poses an acceptable level of risk to hold Federal Data. If the JAB determines the risk level is too high, it recommends remediation steps. The FedRAMP ISSO shares the findings with the CSP and requests that the CSP correct control implementations, retest affected controls, and resubmit revised documentation. If the JAB accepts the risk associated with the information system, the ISSO will notify the CSP that they are ready to finalize the security assessment.

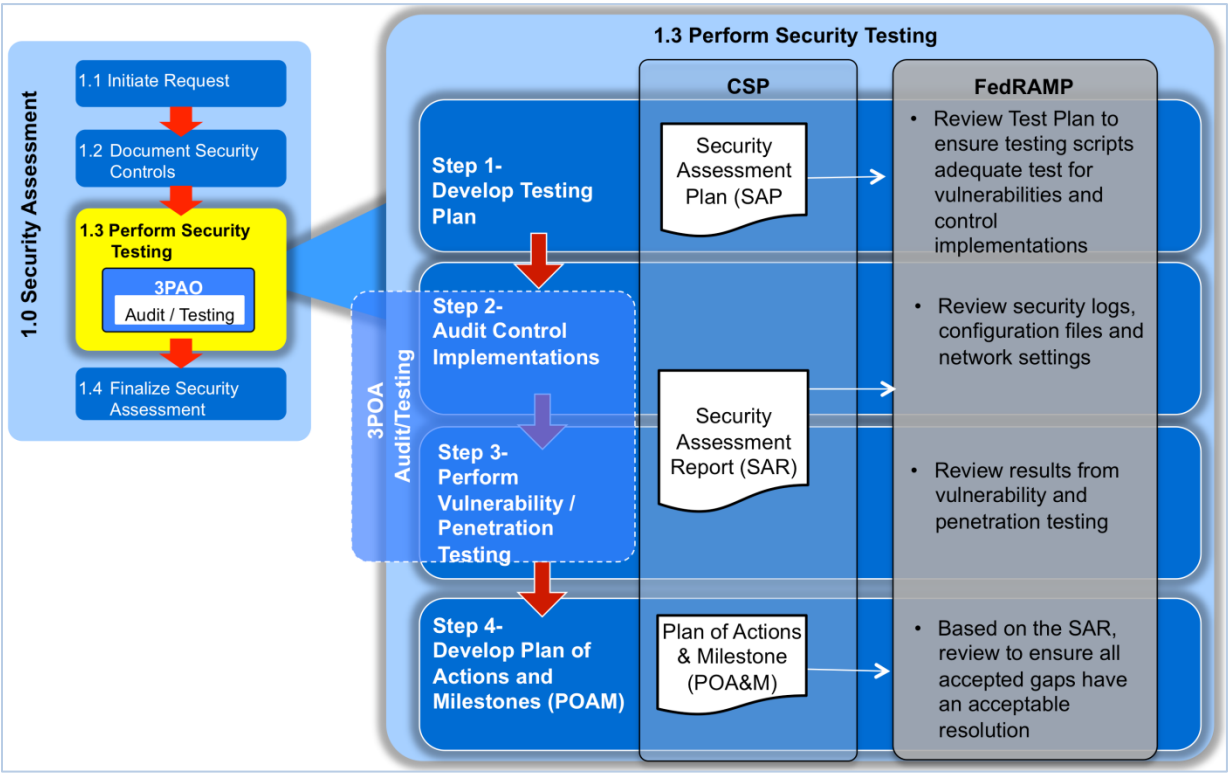

Figure 6-4. Performing Security Testing

Performing security testing in the security assessment process is detailed in Figure 6-4 and the deliverables are listed in Table 6-3.

Table 6-3. Perform Security Testing Deliverables

Deliverable	Description
3PAO Designation Form	The CSP submits this form to FedRAMP in order to designate the FedRAMP accredited 3PAO that will perform an independent assessment of the CSP's system.

Deliverable	Description
Security Assessment Plan (SAP)	The SAP describes the scope of the assessment including: • Security controls and control enhancements under assessment using the FedRAMP security control baseline; • Use of FedRAMP Assessment Test Procedures to determine security control effectiveness; and • Assessment environment, assessment team, and assessment roles and responsibilities.
Security Assessment Test Cases	Security Assessment Test Cases are based on NIST SP 800-53 A. NIST test procedures have been tailored for FedRAMP. These test cases are captured in the form of an Excel Workbook.
Security Assessment Report (SAR)	The SAR is used to document the overall status and deficiencies in the security controls. The SAR serves as the primary document that the JAB will review to guide their Provisional Authorization decision. This document will show security weaknesses that will be mapped to corresponding POA&M items.
Plan of Action and Milestones (POA&M)	Describes the CSP's specific tasks and timelines for remediating or changing system or control specific implementations.

6.4. Finalizing the Security Assessment

During the final security assessment step, the CSP compiles the security documents into a single security assessment package. In this final assembly of documents, the CSP will also submit a Supplier's Declaration of Conformance to verify and attest to the truth of the security control implementations detailed in the security assessment package. The CSP then submits it to their FedRAMP ISSO for review. When the ISSO has completed the review and determines the package is complete, the ISSO forwards the package to the JAB for review.

The JAB reviews the security assessment package and all documentation provided to make a final risk-based decision on whether or not to grant a Provisional Authorization. If the JAB does not grant a Provisional Authorization, FedRAMP will send a denial notification and provide instructions on how the CSP can reapply for a FedRAMP security assessment.

CSPs that receive a provision ATO will be added to the list of authorized CSPs on www.FedRAMP.gov. The listing will provide basic information about the service offerings of the CSP and is targeted towards agencies looking to procure cloud-based services.

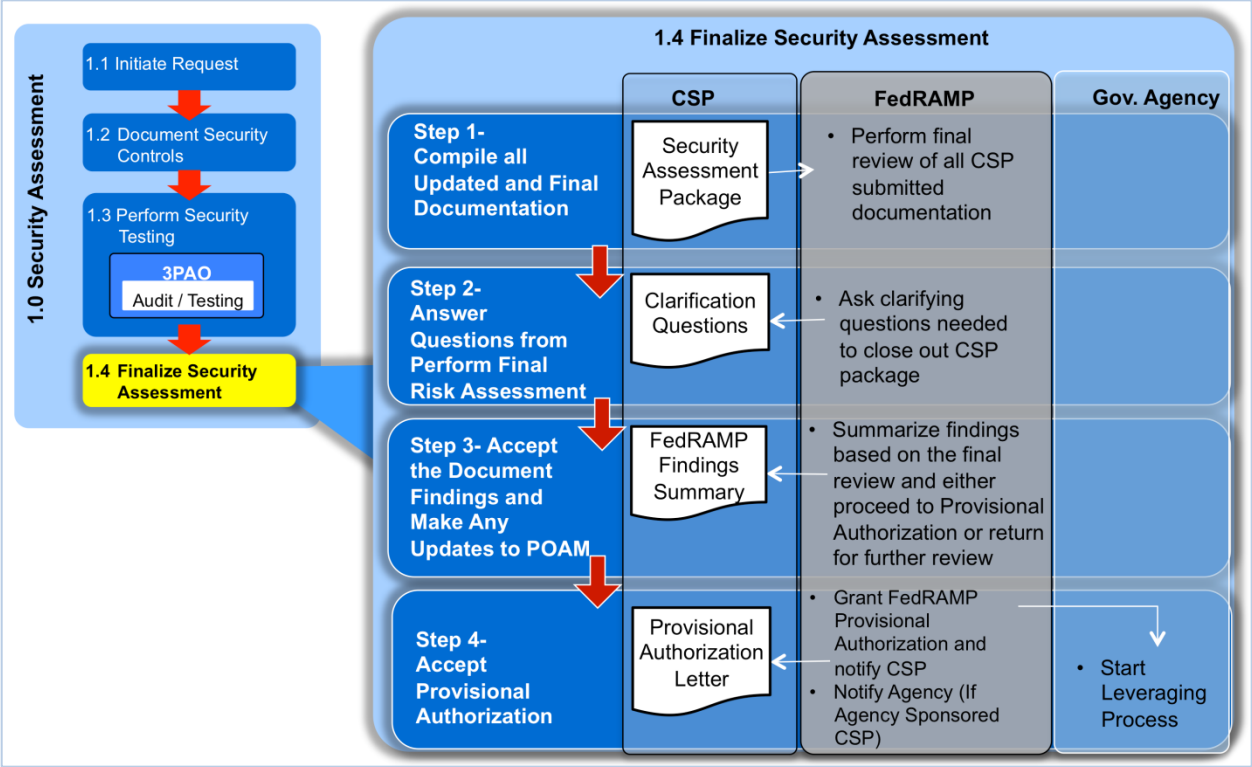

Figure 6-5. Finalizing the Security Assessment

The Provisional Authorization letter and security authorization package will be stored in a secure, access-controlled repository for review by agencies that wish to leverage the CSP's Provisional Authorization in order to issue their own ATO. Finalizing the security assessment is detailed in Figure 6-5 and deliverables associated with the process are listed in Table 6-4.

Table 6-4. Finalize Security Assessment Deliverable

Deliverable	Description
Finalized Security Assessment Package	Complete package of all security assessment deliverables and related evidence.
Supplier's Declaration of Conformity (SDOC)	CSPs verify and attest to the truth of the implemented security controls as detailed in their security assessment package.

7. Leveraging the Provisional Authorization

Federal agencies are required by FISMA to individually accept the risk and grant the ATO before placing any Agency Data into a system. The FedRAMP leveraging authorization process details how agencies can use FedRAMP Provisional Authorizations and the secure repository to grant an ATO in accordance with FISMA. Agencies must use FedRAMP when granting an ATO for a cloud service. A high level illustration of the leveraging the authorization process is found in Figure 7-1.

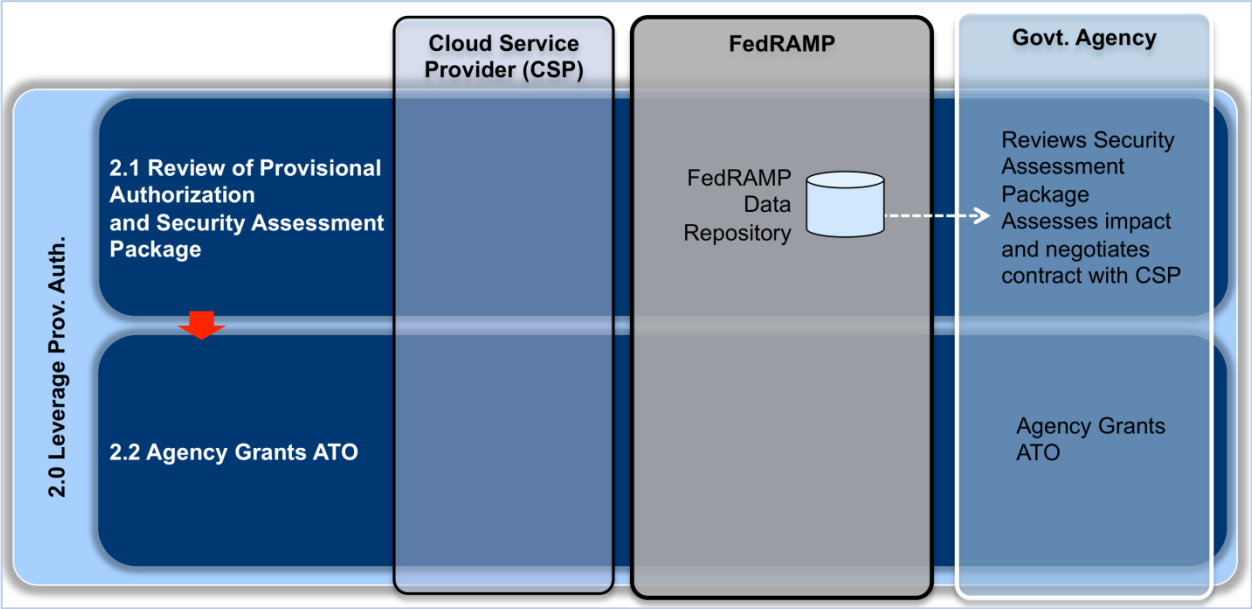

Figure 7-1. Leveraging the Authorization Process

One of the primary benefits of FedRAMP is the ability for agencies to reuse the Provisional Authorizations granted by the JAB and to leverage the work that has been completed. Agencies can review the CSP's application of security control implementations, including evidence of the implementation of these controls. Additionally, agencies can review any existing vulnerabilities and risk mitigations plans for the cloud service represented by the package.

Part of the review of the assessment package requires Federal agencies to understand the control responsibility. The CIS (detailed in the security assessment process) will clearly delineate the control responsibility between the CSP, Federal agency, or hybrid (shared responsibility). The responsibility for security control implementation varies by cloud deployment model and is detailed in Figure 7-2.

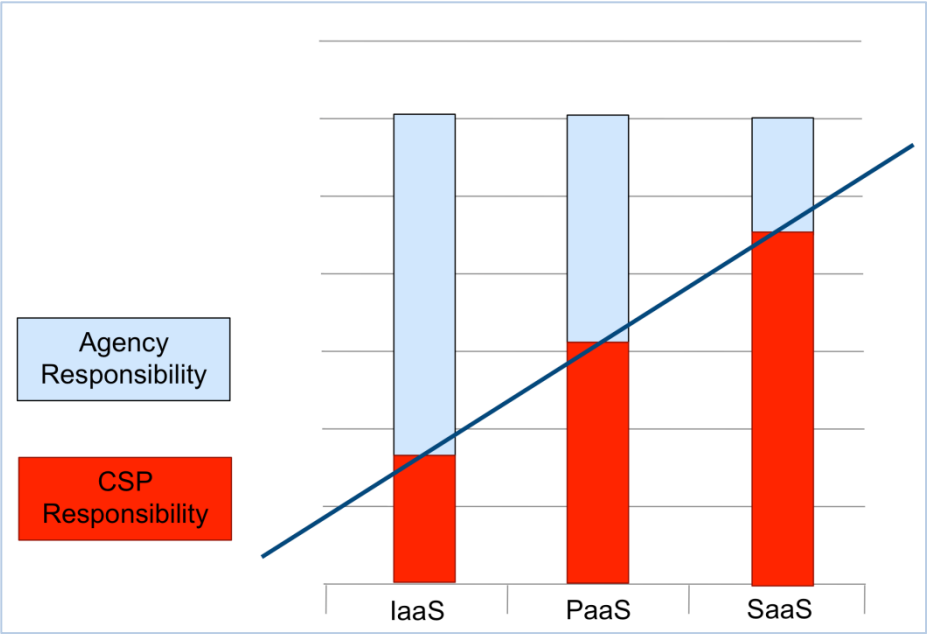

Figure 7-2. Security Control Responsibilities

After reviewing the security assessment package and the accompanying Provisional Authorization, Agencies can then grant an ATO under their own authority.

7.1. FedRAMP Secure Repository

The FedRAMP PMO maintains a secure repository of security assessment packages that Federal agencies can leverage. The repository will hold assessment packages in four different categories and will includes information about how to review current versions of the security assessment package as described in Table 7-1.

Table 7-1. Security Assessment Package Categories

Category Name	Category ID	Assessed by	Authorizing Authority
CSP Supplied	C	Accredited 3PAO	N/A
Agency ATO*	A	Any 3PAO*	Agency
Agency ATO with FedRAMP 3PAO	W	Accredited 3PAO	Agency
FedRAMP Provisional Authorization	P	Accredited 3PAO	JAB (+ Agency)

**Not eligible for JAB review and Provisional Authorization*

The different categories of assessment packages offer flexibility for Federal agencies and CSPs to allow for unique leveraging of security assessments. When reviewing security assessment packages, agencies will come to understand the level of review the security assessment package has received, as well as the risk exposure associated with the cloud service.

7.1.1. CSP Supplied

The CSP will self-supply a security assessment package using the FedRAMP process. The CSP will follow the FedRAMP security assessment process utilizing internal ISSOs and an accredited

3PAO. The FedRAMP office reviews the package for completeness and will ensure that all FedRAMP documents and templates were used as required, however, neither the JAB nor a Federal agency has made a risk based decision about the security control implementations.

Level of Review: None

Assessment of Risk: Utilized a FedRAMP accredited 3PAO annually based on the security assessment anniversary date

All materials in the CSP supplied security assessment packages must be timely so FedRAMP will require CSPs to re-submit all assessment materials at the time of the CSP's annual self-attestation SDOC letter.

7.1.2. Agency ATO

Agencies must use the FedRAMP process as a framework to grant an ATO when they wish to use a cloud service that is not in the FedRAMP repository. Federal agencies must follow the FedRAMP security assessment process (using all accompanying templates and guidance) utilizing internal Agency ISSOs. In this category, Federal agencies did not use a FedRAMP accredited 3PAO. However, Federal agencies will be required to submit an attestation describing the independence and technical qualifications of the 3PAO utilized to assess that CSP package. Agencies must submit to FedRAMP complete authorization packages with accompanying ATO letter.

Level of Review: Federal agency has granted an ATO

Assessment of Risk: Did not use an accredited 3PAO

Federal agencies will ensure the FedRAMP PMO is provided with any updates to a CSP authorization package annually. Without an accredited 3PAO, these authorizations will not be eligible for JAB review and Provisional Authorization.

7.1.3. Agency ATO with Accredited 3PAO

Agency ATO with accredited 3PAO meets the same requirements as Agency ATO in section 7.1.2 except that an accredited 3PAO was used in the assessment of a CSP package.

Level of Review: Federal agency has granted an ATO

Assessment of Risk: Utilized a FedRAMP accredited 3PAO

Federal agencies will ensure the FedRAMP PMO is provided with any updates to a CSP authorization package annually.

7.1.4. JAB Provisional Authorization

JAB Provisional Authorizations are designations given to security authorization packages that have gone through the FedRAMP assessment process and are authorized by the JAB as detailed in Section 6. Any subsequent Agency ATO that leverages the FedRAMP Provisional Authorization will be listed in addition to the JAB ATO to provide agencies with knowledge of the full level of Federal Government review of authorization packages.

Level of Review: JAB has granted a Provisional Authorization

Assessment of Risk: Utilized a FedRAMP accredited 3PAO

The CSP must supply to the FedRAMP PMO an annual self-attestation SDOC letter annually. Additionally, the JAB will review all JAB Provisional Authorizations without Agency ATO at the time of annual self-attestation to determine if they wish to maintain the JAB Provisional Authorization.

8. Ongoing Assessment and Authorization (Continuous Monitoring)

Ongoing assessment and authorization, often referred to as continuous monitoring, is the third and final process for cloud services in FedRAMP. Ongoing assessment and authorization is part of the overall risk management framework for information security and is a requirement for CSPs to maintain their Provisional Authorization. This process determines whether the set of deployed security controls in an information system remain effective in light of planned and unplanned changes that occur in the system and its environment over time.

The FedRAMP ongoing assessment and authorization program is based on *NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organization*. Ongoing assessment and authorization results in greater transparency into the security posture of the CSP system and enables timely risk-management decisions. Security-related information collected through continuous monitoring is used to make recurring updates to the SSP, SAR, and POA&M. Continuous monitoring keeps the security authorization package timely and provides information about security control effectiveness. This allows agencies to make informed risk management decisions as they use cloud services. A high level illustration of the ongoing assessment and authorization process is detailed in Figure 8-1.

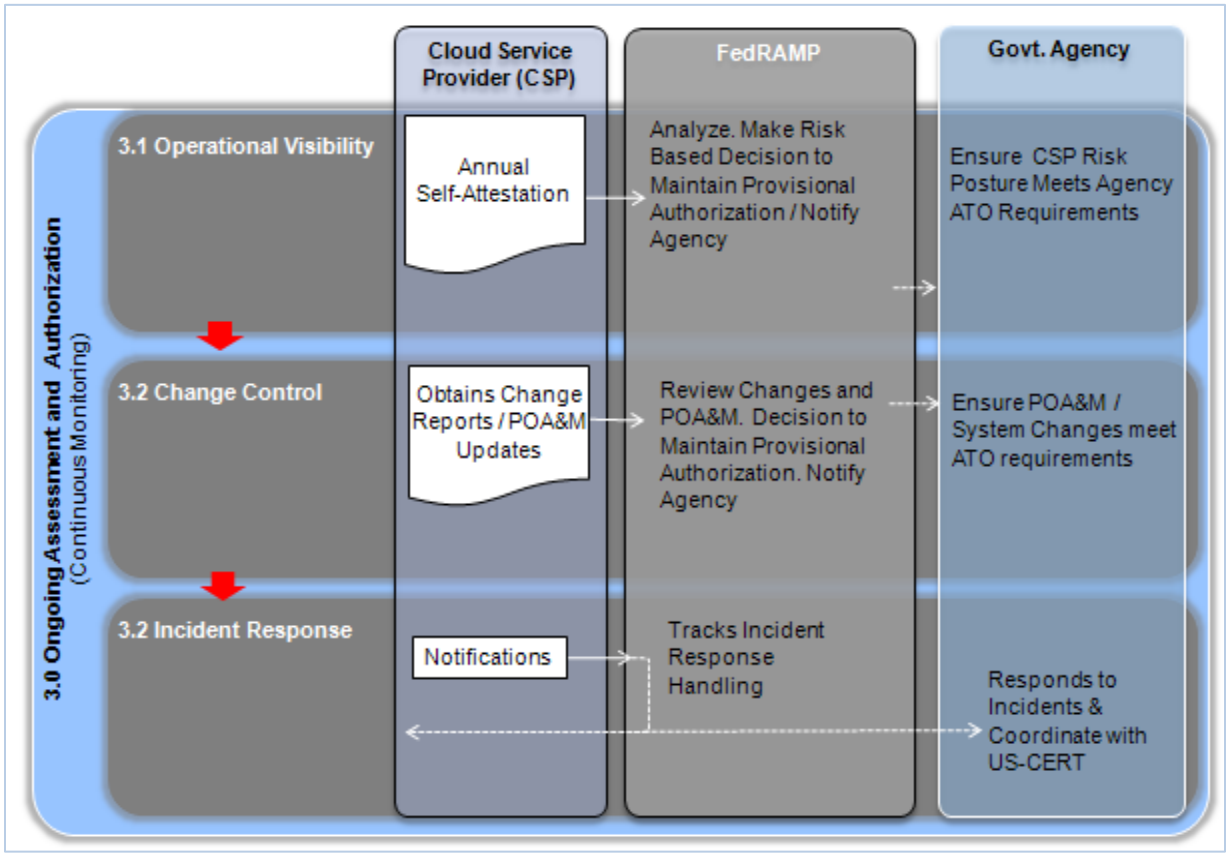

Figure 8-1. Ongoing Assessment and Authorization

8.1. Operational Visibility

The goal of operational visibility is to reduce the administrative burden associated with demonstrating compliance and instead shift toward real-time oversight monitoring through automated approaches in accordance with OMB Memo M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.* To achieve operational visibility, CSPs provide two different types of information: periodically submitted specific control evidentiary artifacts, and annual self-attestation reports. The operational visibility process is illustrated in Figure 8-2.

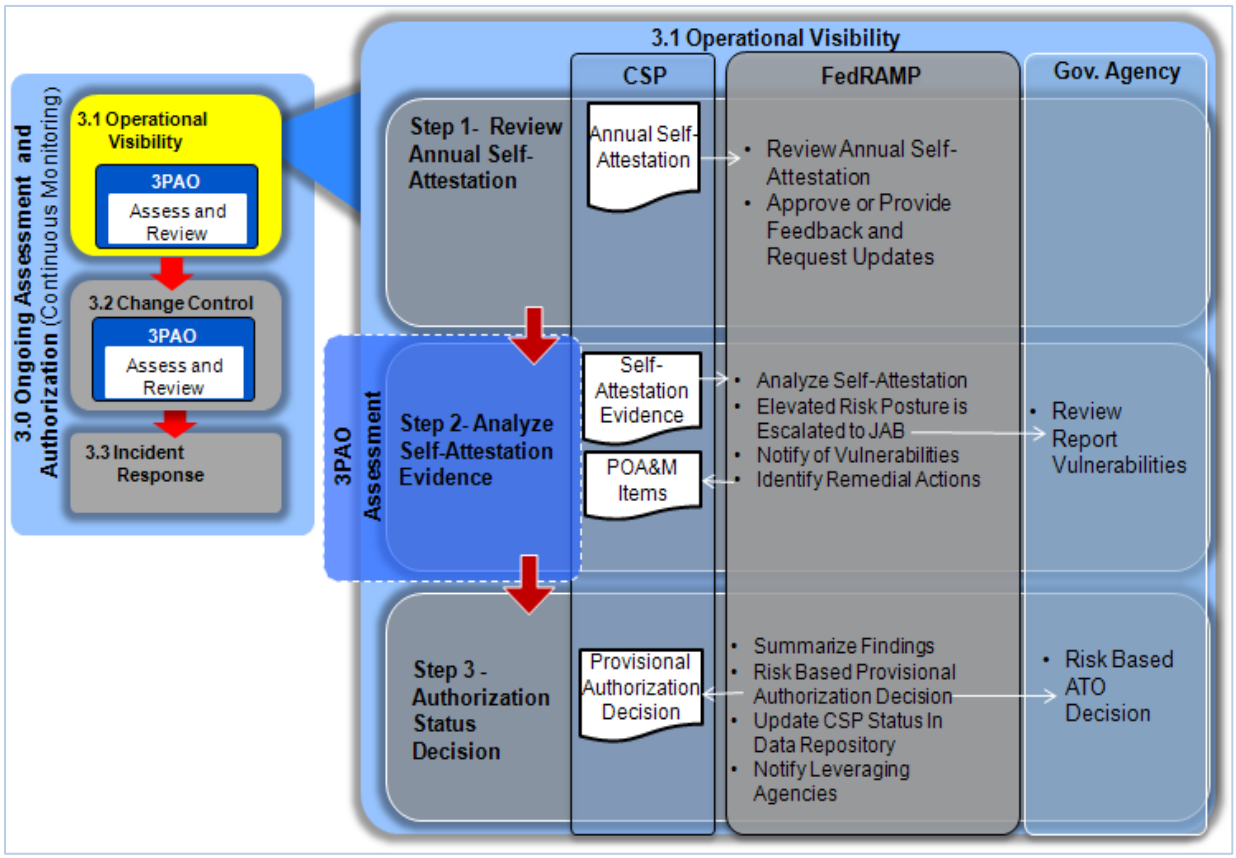

Figure 8-2. Operational Visibility

Annually, CSPs must re-assess a subset of the security controls and send results to FedRAMP and leveraging agencies. The re-assessment of these controls must be completed by an accredited 3PAO. The ISSO will advise the CSP and 3PAO which controls should be reassessed based on recommendations from the JAB. To verify this work was completed, CSPs must submit an annual self-attestation report certifying that all controls are working properly.

Both the JAB and leveraging agencies use the self-attestation to make risk based decisions on whether to continue the CSP's Provisional Authorization and/or Agency ATO. When changes in

the environment are required, the CSP follows the processes documented in the Configuration Management Plan for their system.

8.2. Change Control Process

CSPs will make periodic changes to their system. This process area is not designed for routine changes as described in the Configuration Management Plan; but rather for significant changes that change the scope of an approved Provisional Authorization or impact the authorization boundary. In this change control process, CSPs provide effective information on the nature of changes and what impact the change makes on the CSP system. This allows FedRAMP and leveraging Federal agencies to make an informed risk based decision about what residual risks will be accepted through the any changes to an authorized system. The change control process area is illustrated in Figure 8-3.

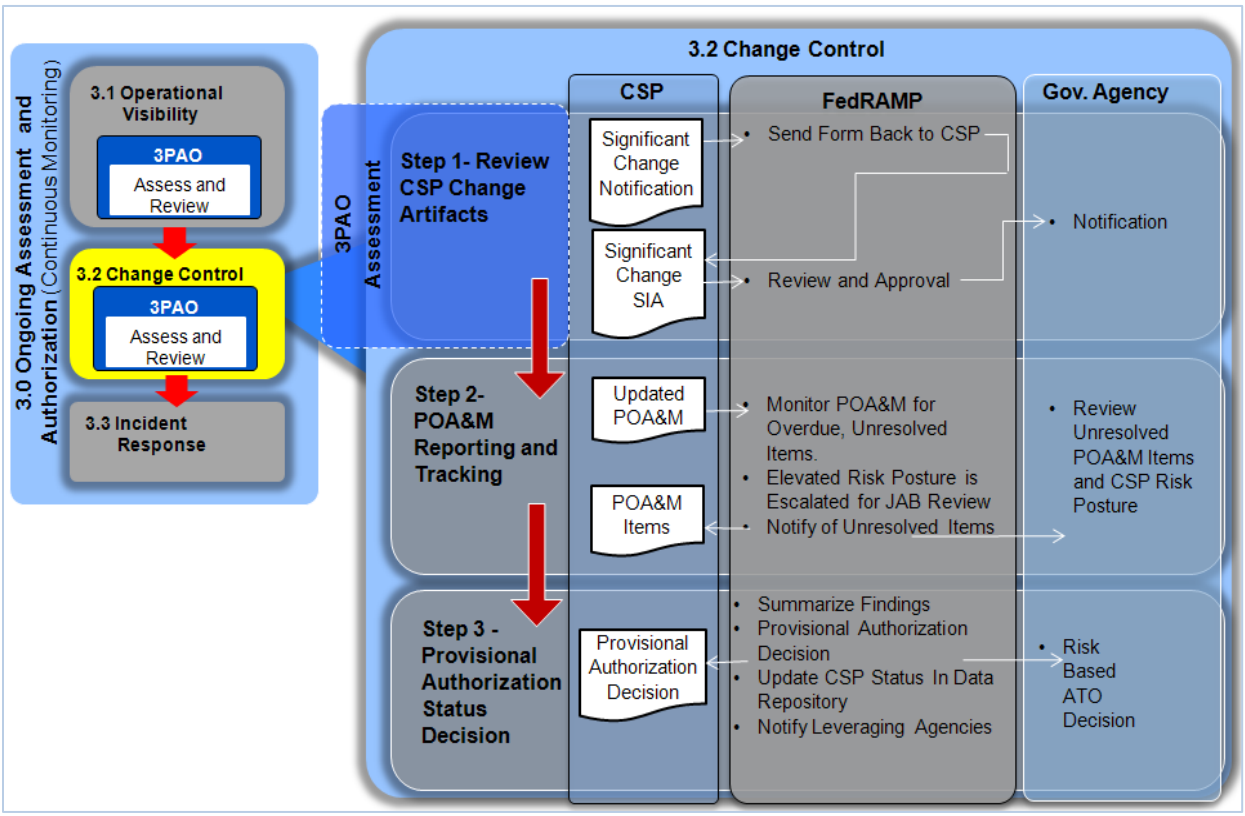

Figure 8-3. Change Control Process

CSPs must report any changes or proposed changes that significantly impact the CSP's ability to meet FedRAMP requirements. These changes include, but are not limited to, changes in the CSP's point of contact with FedRAMP, changes in the CSP's risk posture, changes to any applications residing on the cloud system, and/or changes to the cloud system infrastructure. The CSP provides updates to their FedRAMP ISSO by submitting an updated Configuration Management Plan and any other documents that capture significant changes such as the SSP and the IT Contingency Plan. CSPs must notify the ISSO of any impending significant change. The ISSO will provide the CSP with a Significant Change Security Impact Analysis form. Then the CSPs must fill out and submit the form which must be reviewed by the ISSO and agreed to by the JAB. If any intended change will either add residual risk or change a leveraging agency's

responsibilities, the CSP must review the planned implementation with the Government ISSO responsible for the Provisional Authorization. The Government ISSO will review the proposed change with the Authorizing Authority and make recommendations to the CSP. If the proposed change will create risks that the JAB finds unacceptable, the Provisional Authorization will either be updated to reflect revisions to the POA&M, additional conditions, or could result in a revocation of the Provisional Authorization if the change is implemented.

After a significant change, any impacted security controls must be documented in the SSP, re-assessed by a 3PAO, and updated documentation must be provided to FedRAMP. FedRAMP will notify leveraging agencies that a change has been made. The leveraging agency should review the significant impact and updated documentation.

Implemented changes may alter current security control implementations or create a new vulnerability to a cloud system. Accordingly, CSPs must update their POA&M that is submitted to and reviewed quarterly by their FedRAMP ISSO. The FedRAMP ISSO reviews the updated CSP POA&M to determine if CSPs are complying with continuous reporting requirements and that any changes to the POA&M do not introduce unacceptable risk. The ISSO will summarize any changes to the CSP POA&M and make recommendations to the JAB on whether or not the CSP is complying with the FedRAMP requirements and their system still presents an acceptable level of risk.

8.3. Incident Response

The shared tenant architecture of cloud services implies that a single incident may impact multiple Federal agencies leveraging the cloud services. FedRAMP will work with US-CERT (an office within DHS) to coordinate incident response activities.

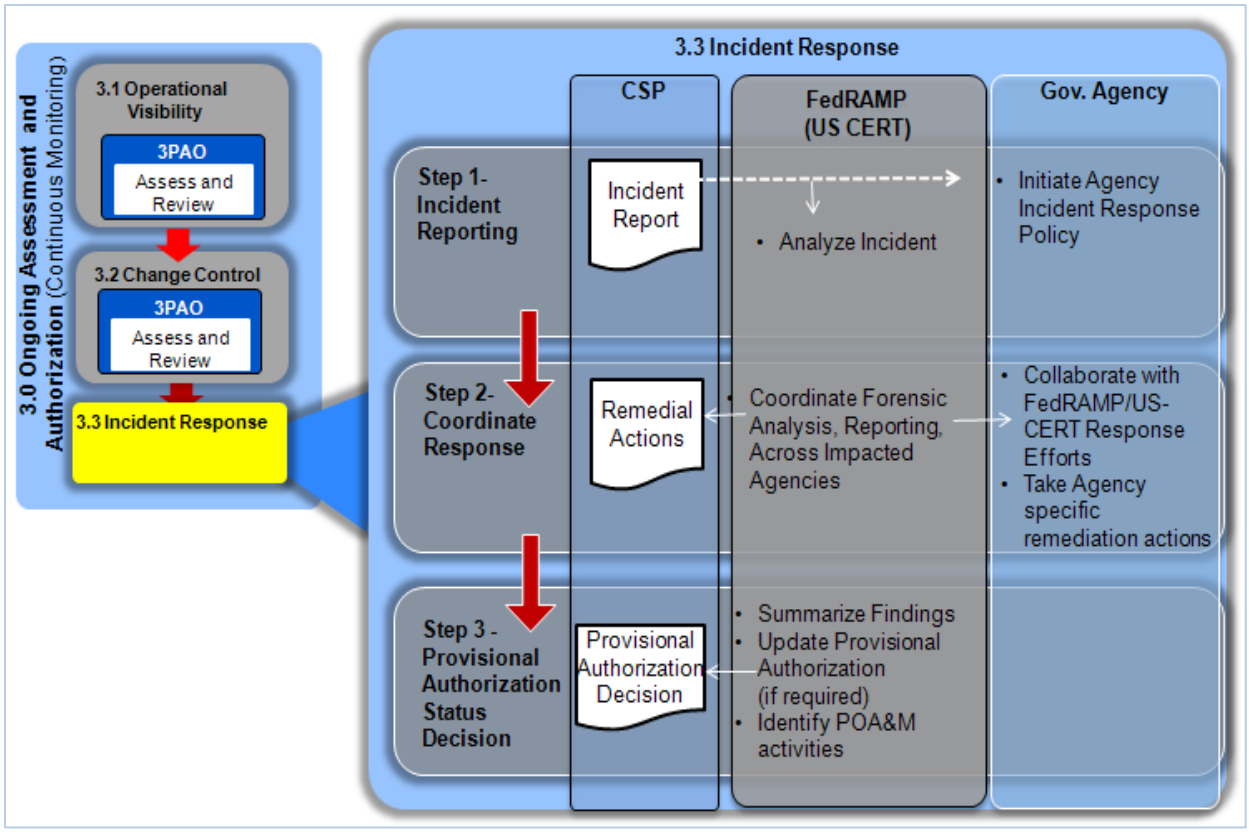

Figure 8-4. Reporting a Security Incident

Part of a CSP security authorization package requires CSPs to have incident response plans in accordance with existing Federal Policies such as OMB M-07-16 and NIST Special Publication 800-61. In the event of a security incident, a CSP must notify both US-CERT and the impacted Federal agency Security Operation Centers (SOCs).

FedRAMP and US-CERT will then coordinate response efforts across impacted Government Agencies including activities such as forensic analysis through root cause and recommended remediation actions. Impacted agencies provide input to agency specific remediation actions that are required per contractual or compliance requirements.

FedRAMP and US-CERT will summarize the findings in an Incident Report that will be made available by FedRAMP to agencies leveraging the FedRAMP Provisional Authorization. Additionally, if CSP actions must be taken to prevent future occurrences, the actions will be recorded by the CSP in their POA&M and monitored. Based on the severity of the incident and the impact it has on Federal agencies, the FedRAMP PMO may initiate a review of a CSP's Provisional Authorization with the JAB. The incident response process is depicted in Figure 8-4.

9. References

9.1. Applicable Laws and Regulations

The following laws and regulations are applicable to the FedRAMP program:

- Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
- E-Authentication Guidance for Federal Agencies [OMB M-04-04]
- Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
- Federal Information Resources Management Regulation [41 CFR C 201]
- Freedom of Information Act As Amended in 2002 [PL 104-232, 5 USC 552]
- Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
- Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7]
- Internal Control Systems [OMB Circular A-123]
- Management of Federal Information Resources [OMB Circular A-130]
- Management's Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
- Privacy Act of 1974 as amended [5 USC 552a]
- Protection of Sensitive Agency Information [OMB M-06-16]
- Records Management by Federal Agencies [44 USC 31]
- Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
- Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]

9.2. Applicable Standards and Guidance

The following standards and guidance are applicable to the FedRAMP program:

- A NIST Definition of Cloud Computing [NIST SP 800-145]
- Computer Security Incident Handling Guide [NIST SP 800—61, Revision 1]
- Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
- Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]
- General Criteria for the Operation of Various Types of Bodies Performing Inspection [International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17020:1998]
- Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53A]
- Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Revision 1]
- Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]

- Guide for Mapping Types of Information and Information Systems to Security Categories [NISP SP 800-60, Revision 1]
- Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]
- Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
- Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
- Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-1]
- Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 3]
- Risk Management Guide for Information Technology Systems [NIST SP 800-30]
- Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
- Security Requirements for Cryptographic Modules [FIPS Publication 140-2]
- Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
- Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]

10. Deliverables

Deliverables noted in Table 10-1 must be created using the FedRAMP templates. All deliverable templates are available on www.FedRAMP.gov.

Table 10-1. FedRAMP Deliverables by Process Area

Process Area	Deliverable	Description
Security Assessment Process Area, Initiate Request Process	FedRAMP Request Form	The FedRAMP request form is used by Federal agencies and CSPs to request initiation of the FedRAMP security assessment process.
	FIPS 199 Categorization	The FIPS 199 Security categorization is used to determine the impact level to be supported by the cloud information system/service. The provider should categorize based on the system data currently stored and not leveraging agency data to be hosted on their system.
	Control Tailoring Workbook	This document is used by CSP to document their control implementation and define their implementation settings for FedRAMP defined parameters and any compensating controls.
	Control Implementation Summary	This document summarizes the control ownership and indicates which controls are owned and managed by the CSP and which controls are owned and managed by the leveraging agency.
Security Assessment Process Area, Documenting Security Controls	System Security Plan (SSP)	The SSP describes how the controls are implemented within the cloud information system and its environment of operation. The SSP is also used to describe the system boundaries.
	Information Security Policies	The CSP's Information Security Policy that governs the system described in the SSP.
	User Guide	The User Guide describers how leveraging agencies use the system.
	Rules of Behavior	This document is used to define the rules that describe the system user's responsibilities and expected behavior with regard to information and information system usage and access.

	IT Contingency Plan	These documents define and test interim measures to recover information system services after a disruption. The ability to prove that system data can be routinely backed up and restored within agency specified parameters is necessary to limit the effects of any disaster and the subsequent recovery efforts.
	Configuration Management Plan	This plan describes how changes to the system are managed and tracked. The Configuration Management Plan should be consistent with NIST SP 800-128.
Security Assessment Process Area, Documenting Security Controls	Incident Response Plan	This plan documents how incidents are detected, reported, and escalated and should include timeframes, points of contact, and how incidents are handled and remediated. The Incident Response Plan should be consistent with NIST Special Publication 800-61.
	E-Authentication Workbook	This template is used to indicate what authentication level (1-4) will be used in the cloud system. It defines the level in terms of the consequences of the authentication errors and misuse of credentials. It is also used to complete a risk assessment and mapping identified risks.
	Privacy Threshold Analysis	This questionnaire is used to help determine is a Privacy Impact Assessment is required.
	Privacy Impact Assessment	This document assesses what Personally Identifiable Information (PII) is captured and if it is being properly safeguarded. This deliverable is not always necessary depending on the outcome of the Privacy Threshold Analysis.
Security Assessment Process, Performing the Security Tests	3PAO Designation Form	The CSP submits this form to FedRAMP in order to designate the FedRAMP accredited 3PAO that will perform an independent assessment of the controls protecting the CSP's system.
	Plan of Action and Milestones (POA&M)	Describes the CSP's specific tasks and timelines for remediating or changing system or control specific implementations.
	Security Assessment Plan (SAP)	The SAP describes the scope of the assessment including: • Security controls and control enhancements under assessment using the FedRAMP security control baseline; • Use of FedRAMP Assessment Test Procedures to determine security control effectiveness; and • Assessment environment, assessment team, and assessment roles and responsibilities.

	Security Assessment Test Cases	Security Assessment Test Cases are based on NIST SP 800-53 A. NIST test procedures have been tailored for FedRAMP. These test cases are captured in the form of an Excel Workbook.
	Security Assessment Report (SAR)	The SAR is used to document the overall status and deficiencies in the security controls. The SAR serves as the basis document that the JAB will utilize to guide their Provisional Authorization decision. This document shows security weaknesses that will be mapped to corresponding POA&M items. In situations where a security control cannot be successfully implemented through standard practice or a compensating control, it will be considered a residual risk.
Continuous Monitoring Process	Supplier's Declaration of Conformity (SDOC)	CSPs verify and attest to the truth of the implemented security controls as detailed in their assessment package.
	Incident Reporting	Reports of security incidents in accordance with the timeframes in the documented in the Incident Response Plan.
	POA&M Update	Update of POA&M contains system owner "to do" list for mitigating security weaknesses.
	Vulnerability Scan Reports	Reports generated from scans that test security controls for vulnerabilities.
	Updated System Security Plan (SSP)	Updated SSP includes changes in control implementations, reviewed at least annually.
	Updated IT Contingency Plan (ITCP)	ITCP updated to reflect contingency plan changes.
	IT Contingency Plan Test Report	Report resulting from annual test of ITCP.
	Updated Separation of Duties Matrix	User roles are reviewed to ensure separation of duties.
	IT Security Awareness & Training	Training designed to educate users on how to safeguard the system.
	Updated Configuration Management Plan	Reflects changes in the Configuration Management process.
	Security Assessment	Assessment to determine new risks to the system.
	IT Security Policies	CSP's IT Security Policies.
	Incident Response Test Report	Report resulting from annual test of Incident Response Plan.
	Physical Access Review Report	Report detailing physical access to CSP data centers.

11. Acronyms

Acronym	Definition
3PAO	Third Party Assessment Organization
ATO	Authority To Operate
CONOPS	Concept Of Operations
CIS	Control Information Summary
CSP	Cloud Service Provider
CTW	Control Tailoring Workbook
DHS	Department of Homeland Security
DOD	Department Of Defense
ERB	Expert Review Board
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
GSA	General Services Administration
ISSO	Information System Security Officer
JAB	Joint Authorization Board
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PMO	Program Management Office
POA&M	Plan Of Action & Milestones
SAP	Security Assessment Plan
SDOC	Supplier's Declaration of Conformity
SLA	Service Level Agreement
SOC	Security Operations Center
SSP	System Security Plan
US-CERT	U.S. Computer Emergency Response Team