FedRAMP SECURITY ASSESSMENT FRAMEWORK

Version 2.4

November 15, 2017

FedRAMP

EXECUTIVE SUMMARY

This document describes a general Security Assessment Framework (SAF) 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 save costs, time, and staff required to conduct redundant Agency security assessments and process monitoring reports.

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.

DOCUMENT REVISION HISTORY

DATE	VERSION	PAGE(S)	DESCRIPTION	AUTHOR
06/06/2014	2.0	All	Major revision for NIST SP 800-53 Revision 4. Includes new template and formatting changes.	FedRAMP PMO
12/04/2015	2.1	All	Formatting changes throughout. Clarified distinction between 3PAO and IA. Replaced Figures 2 and 3, and Appendix C Figures with current images.	FedRAMP PMO
06/06/2017	2.2	Cover	Updated logo	FedRAMP PMO
11/06/2017	2.3	All	Removed references to CSP Supplied Path to Authorization and the Guide to Understanding FedRAMP as they no longer exist.	FedRAMP PMO
11/15/2017	2.4	All	Updated to the new template	FedRAMP PMO

HOW TO CONTACT US

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

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. FEDRAMP OVERVIEW

1.1. APPLICABLE LAWS AND REGULATIONS

- 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]
- 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]

1.2. APPLICABLE STANDARDS AND GUIDANCE

- The NIST Definition of Cloud Computing [NIST SP 800-145]
- Computer Security Incident Handling Guide [NIST SP 800-61, Revision 2]
- 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]
- Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53A, Revision 4]
- Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18]
- Guide for Applying 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 [NIST 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]
- Managing Information Security Risk: Organization, Mission, and Information System View [NIST SP 800-39]
- 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 4]
- Guide for Conducting Risk Assessments [NIST SP 800-30 Revision 1]
- 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]

1.3. FedRAMP OVERVIEW

FedRAMP is a U.S. Government program to standardize how the *Federal Information Security Management Act* (FISMA) applies to cloud computing services. Cloud computing offers many advantages over traditional computing. Through cloud computing, Federal Agencies are able to consolidate and provision new services faster, at the same time reducing information technology costs. Cloud computing also enables efficiencies for services to citizens and offers stronger cyber security safeguards than what is possible using traditional information technology (IT) methods.

FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring of cloud based services. Using a “do once, use many times” framework, FedRAMP reduces the cost of FISMA compliance and enables Government entities to secure Government data and detect cyber security vulnerabilities at unprecedented speeds.

FedRAMP was developed in collaboration with the NIST, GSA, DOD, and DHS. Other Government Agencies, working groups, and industry experts participated in providing input to the development of FedRAMP. This document replaces the FedRAMP Concept of Operations and describes the Security Assessment Framework (SAF) for FedRAMP. When Authorizing Officials (AOs) incorporate the FedRAMP SAF with internal security authorization processes, it

will ensure they meet the FedRAMP requirements for cloud services they use. The FedRAMP SAF is subject to updates as the program evolves toward sustained operations.

1.4. AUTHORITIES

On December 9, 2010, the Office of Management and Budget (OMB) released a plan to reform Federal information technology initiatives: *25 Point Implementation Plan to Reform Federal Information Technology Management.*[1] In this plan, Point 3 created the "Cloud First" Policy, which requires U.S. Federal Agencies to use cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. In a follow-up to the 25 Point Plan, on February 8, 2011, OMB released the *Federal Cloud Computing Strategy*,[2] giving Agencies a defined strategy and roadmap for effectively migrating services to the cloud. To provide a cost-effective, risk-based approach for the adoption and use of cloud services, on December 8, 2011, OMB released the *Security Authorization of Information Systems in Cloud Computing Environments,* also known also as the *FedRAMP Policy Memo*.[3] The *FedRAMP Policy Memo* requires that all Federal Agencies meet the FedRAMP requirements for all Agency use of cloud services by June 2014.[4]

1.5. 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 framework that saves costs, time, and staff required to conduct redundant Agency security assessments.

The purpose of FedRAMP is to:

- Ensure that cloud systems used by Government entities have adequate safeguards
- Eliminate duplication of effort and reduce risk management costs
- Enable rapid and cost-effective Government procurement of information systems/services

---

[1] http://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf

[2] https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf

[3] https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf

[4] The FedRAMP SAF applies to all cloud computing deployment and service delivery models. More information can be found about what services qualify as cloud services in *NIST SP 800-145*.

FedRAMP uses a security risk-based model that can be leveraged across multiple Agencies. All FedRAMP Cloud Service Providers (CSP) use a standardized security baseline geared towards cloud systems. FedRAMP provides processes, artifacts, and a Secure Repository that enables Agencies to leverage authorizations with:

- Standardized security requirements
- Conformity assessment identifying qualified independent, third-party security assessors
- Repository of authorization packages for secure clouds that all Agencies can leverage
- Standardized ongoing assessment and authorization approach for Government clouds
- Standardized contract language to help Agencies integrate FedRAMP requirements and best practices into acquisitions.

1.6. GOVERNANCE AND STAKEHOLDERS

FedRAMP is governed by Executive branch entities that work in collaboration to develop, manage, and operate the program, as illustrated in

Figure 1. FedRAMP stakeholders are those individuals and teams with a vested interest in the implementation and operations of FedRAMP. The *FedRAMP Policy Memo* outlined stakeholder responsibilities that have been further delineated in the Joint Authorization Board (JAB) Charter. FedRAMP stakeholders and their responsibilities are described in the sections that follow. A summary of stakeholder responsibilities can be found in Table 1 of this document.

Figure 1 – FedRAMP Governance Entities

1.6.1. OFFICE OF MANAGEMENT AND BUDGET

OMB is responsible for implementing and enforcing Presidential policies and priorities Government-wide. These duties extend to FedRAMP, where OMB is responsible for:

- Establishing Federal policy for protection of Federal information cloud services
- Describing the key components of FedRAMP and its operational capabilities
- Defining Executive Department and Agency responsibilities in developing, implementing, operating, and maintaining FedRAMP
- Defining the requirements for Executive Departments and Agencies using FedRAMP in the acquisition of cloud services

Most of these requirements are established by the FedRAMP Memo issued by OMB. The OMB also has an active role in measuring FedRAMP compliance by gathering data from Federal Agencies through Portfolio Stat.

1.6.2. FEDRAMP JOINT AUTHORIZATION BOARD

The JAB members are the Chief Information Officers (CIOs) from DHS, GSA, and DOD. The JAB defines and establishes the FedRAMP baseline system security controls and the accreditation criteria for Third Party Assessment Organizations (3PAO). The JAB works closely with the FedRAMP Program Management Office (PMO) to ensure that FedRAMP baseline security controls are incorporated into consistent and repeatable processes for security assessment and authorizations of CSPs, through this FedRAMP SAF.

The JAB also follows the FedRAMP SAF to issue a Provisional Authority to Operate (P-ATO) for cloud services it believes will be leveraged the most, Government-wide. For those P-ATOs, the JAB also ensures those systems maintain an acceptable risk posture through continuous monitoring.

1.6.3. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

NIST is the Federal Government's leading body for the establishment of standards. As required by FISMA, NIST's security standards (NIST Special Publication [SP] 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*; Federal Information Processing Standards [FIPS] Publication [PUB] 199, *Standards for Security Categorization of Federal Information and Information Systems*; FIPS PUB 200, *Minimum Security Requirements for*

Federal Information and Information Systems; and NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*) serve as the foundation for FedRAMP. NIST advises FedRAMP on FISMA compliance requirements and also assists in developing standards for the accreditation of independent 3PAOs.

1.6.4. DEPARTMENT OF HOMELAND SECURITY

DHS sets the continuous monitoring strategy for all U.S. Federal Agencies. As such, FedRAMP subscribes to DHS continuous monitoring practices in accordance with DHS guidance. DHS also manages the United States Computer Emergency Readiness Team (US-CERT), which is the Government entity that coordinates and responds to security incidents for all U.S. Federal Agencies. Last, DHS manages the Trusted Internet Connections (TIC) and assists Agencies in implementing TIC compliant interconnections.

1.6.5. FEDRAMP PROGRAM MANAGEMENT OFFICE

The FedRAMP PMO is responsible for the development of the FedRAMP program and manages its day to day operations. The PMO creates processes, guidance, and templates for Agencies and CSPs to use for the purpose of developing, assessing, and authorizing cloud systems in accordance with FISMA. This FedRAMP SAF works in concert with these processes, guidance, and templates and all are available publicly at www.fedramp.gov.

The PMO also works with the JAB to provisionally authorize cloud services providers. The PMO facilitates cloud service providers through the FedRAMP SAF and resulting continuous monitoring activities. Additionally, the FedRAMP PMO manages the 3PAO accreditation program based on the criteria established by the JAB.

Finally, the PMO serves as the communications liaison to all stakeholders and assists CSPs, 3PAOs, and Agencies in understanding FedRAMP requirements.

1.6.6. FEDERAL AGENCIES

Federal Agencies, including Departments and Offices, are consumers of cloud computing services. They must ensure that all cloud systems that process, transmit, or store Government information use the FedRAMP baseline security controls by using the FedRAMP SAF when

granting security authorizations under FISMA. Federal Agencies must enforce the FedRAMP requirements through their contracts with CSPs.[5]

When Federal Agencies grant security authorizations using the FedRAMP SAF, they must use any existing authorizations as a starting point in applying the FedRAMP SAF. Once an Agency grants an authorization that follows the FedRAMP SAF, then they must submit that security authorization package to the FedRAMP PMO for verification of meeting the FedRAMP requirements (if not already in the repository). Additionally, the Federal Agency must have an "Authority to Operate" (ATO) letter on file with the FedRAMP PMO.

1.6.7. FEDERAL CHIEF INFORMATION OFFICERS COUNCIL

The Federal CIO Council coordinates cross Agency communications and hosts events to disseminate FedRAMP information to Federal CIOs and their representatives. The FedRAMP PMO participates in Federal CIO Council events and reviews all CIO Council input on FedRAMP.

1.6.8. THIRD-PARTY ASSESSMENT ORGANIZATIONS

3PAOs play a critical role in the FedRAMP security assessment process, as they are the independent assessment organizations that verify cloud providers' security implementations and provide the overall risk posture of a cloud environment for a security authorization decision. These assessment organizations must demonstrate independence and the technical competence required to test security implementations and collect representative evidence. 3PAOs must:

- Plan and perform security assessments of CSP systems
- Review security package artifacts in accordance with FedRAMP requirements

The Security Assessment Report (SAR) created by the 3PAO is a key deliverable for leveraging Agencies to use FedRAMP security assessment packages.

The FedRAMP JAB requires that a 3PAO be accredited through the FedRAMP 3PAO Program for any JAB P-ATOs. Agencies are highly encouraged to use these organizations for Agency authorizations that meet the FedRAMP requirements. While Agencies are free to use non-3PAO Independent Assessors (IA), use of a 3PAO assessor removes the Agency requirement to provide an attestation to the independence and competency of the security control assessor.

[5] Templates for contract language are available on www.fedramp.gov.

1.6.9. CLOUD SERVICE PROVIDERS

CSPs offer cloud computing services for use by consumers. CSPs interested in having the U.S. Government as a consumer of their service must meet the FedRAMP security requirements and implement FedRAMP baseline security controls. CSPs verify their compliance with FedRAMP security requirements by following the FedRAMP SAF. Through this process, the risks of a CSPs services are determined and it gives Agency authorizing officials the ability to determine if the risk posture of a CSP service meets the risk posture needed to host Government data. If a CSP is authorized following the FedRAMP SAF, they must also perform continuous monitoring to maintain that authorization.

CSPs must review information published on www.fedramp.gov for periodic updates to guidance, templates, and FedRAMP news.

2. FedRAMP REQUIREMENTS

A key element to successful Government adoption of cloud computing is to ensure that essential security controls are properly implemented on cloud systems that process, store, and/or transmit Government data. Additionally, cloud systems need to provide 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.

FISMA requires Federal Agencies to review risk and make risk-based decisions on whether or not to authorize a system. FedRAMP builds upon FISMA. 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.

2.1. TWO AUTHORIZATION PATHS

2.1.1. JOINT AUTORIZATION BOARD P-ATO

Either a CSP or an Agency can make a request to have a system processed for a JAB P-ATO by submitting an Initiate Request form on www.fedramp.gov. For JAB P-ATOs,[6] the JAB will provide the risk review of all documentation provided by the CSP in the security authorization package. CSPs will work with the FedRAMP PMO through the SAF and present all documentation to the JAB for risk review.

When the JAB grants the P-ATO, the JAB will provide a recommendation to all Federal Agencies about whether a cloud service has a recommended acceptable risk posture for Federal Government use at the designated data impact levels.

For FedRAMP JAB P-ATOs, CSPs must contract with an accredited 3PAO to independently verify and validate the security implementations and the security assessment package.

2.1.2. FedRAMP AGENCY ATO

CSPs may work directly with an Agency to obtain a FedRAMP Agency ATO. In this case, the Federal Agency will provide the risk review of all documentation provided by the CSP in its security authorization package. CSPs will work directly with the Federal Agency security office and present all documentation to the Authorizing Official (AO) or equivalent for an authorization.

As noted in Section 1.6.8, Federal Agencies may elect to use a FedRAMP accredited 3PAO or a non-accredited IA to perform the independent assessment. If a non-accredited assessor is used, the Agency must provide evidence of the assessor's independence and provide a letter of attestation of the assessor's independence with the security authorization package. The FedRAMP PMO highly recommends Agencies select an assessor from the FedRAMP 3PAO accreditation program.

Once an Agency authorizes a package, the Agency must inform the FedRAMP PMO by sending an email to info@FedRAMP.gov. The PMO then instructs the CSP how to submit the package for PMO review. After reviewing the package to ensure it meets all of the FedRAMP

[6] Under FISMA, the JAB cannot accept risk on behalf of any Agency. Therefore, it issues "Provisional" ATOs to indicate that a CSP has met all of the FedRAMP requirements that Agencies can use to grant ATOs.

requirements, the FedRAMP PMO will publish the package in the Secure Repository for other Agencies to leverage.

2.2. CONTRACTUAL LANGUAGE

The *FedRAMP Policy Memo* requires Federal Agencies to ensure that FedRAMP requirements are met through contractual provisions. This is to ensure that a CSP has a contractual obligation to meet and maintain the FedRAMP requirements. To assist Agencies in meeting this requirement, FedRAMP provides standard template contract language as well as template contract clauses covering all FedRAMP requirements. Federal Agencies can use these contract clauses during the procurement process for acquiring cloud services. FedRAMP contract clauses are available on www.fedramp.gov.

2.3. USING A CSP NOT LISTED IN THE SECURE REPOSITORY

If an Agency would like to use a CSP system that is not listed in the FedRAMP Secure Repository, the Agency must use the FedRAMP SAF and processes and must ensure the CSP has implemented the FedRAMP baseline security control requirements before granting an ATO.

3. FEDRAMP SECURITY ASSESSMENT FRAMEWORK

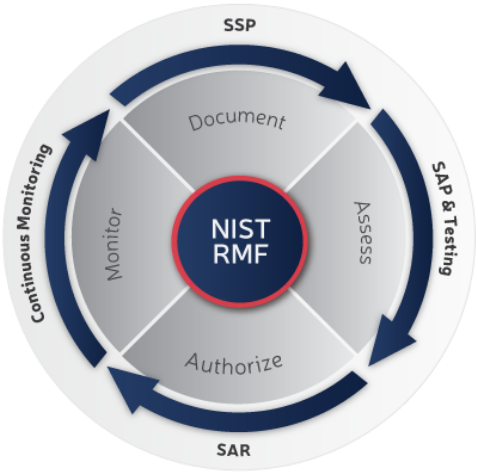
Federal Agencies are required to assess and authorize information systems in accordance with FISMA. The FedRAMP SAF is compliant with FISMA and is based on *NIST Special Publication 800-37.* FedRAMP defines a set of controls for Low and Moderate security impact level systems based on NIST baseline controls (*NIST SP 800-53*, as revised) with a set of control enhancements that pertain to the unique security requirements of cloud computing.

FedRAMP uses the same documents and deliverables that NIST requires Agencies to use, as described in *NIST SP 800-37*. The only part of the FedRAMP process that is new to Federal Agencies involves the *Control Implementation Summary*. These two documents help delineate and summarize security responsibilities for CSPs and Agencies.

FedRAMP simplifies the NIST Risk Management Framework by creating four process areas that encompass the six steps detailed within *NIST SP 800-37*: Document, Assess, Authorize, and Monitor as shown in

Figure 2, below.

Figure 2 – FedRAMP Risk Management Framework



3.1. DOCUMENT

In the document phase of the SAF, Steps 1-3 of the Risk Management Framework will be covered by categorizing the information system, selecting the security controls, and implementing and documenting the security controls and implementations in the System Security Plan (SSP) and supporting documents.

3.1.1. CATEGORIZE THE INFORMATION SYSTEM

To categorize the system, the CSP determines the information types and completes a FIPS PUB 199 worksheet to categorize what types of data are (or can be) contained within the system to 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*.

The analysis of the data contained in the system, based upon the information in the FIPS PUB 199 worksheet, will determine if the security categorization for the system is at the Low, Moderate, or High impact level. At this time, FedRAMP only supports security assessments of systems that have Low or Moderate impact levels. A template for the FIPS PUB 199 is available on www.fedramp.gov.

3.1.2. SELECT SECURITY CONTROLS

After completing a categorization in accordance with FIPS PUB 199, the CSP selects the FedRAMP security controls baseline that matches the FIPS PUB199 categorization level from Section 3.1. The FedRAMP security control baseline is published on www.fedramp.gov. Additionally, Section 13 of the *FedRAMP System Security Plan Template* summarizes the controls for both Low and Moderate security impact level systems.

The FedRAMP security control baseline provides the minimum set of controls that CSPs will need to implement to meet FedRAMP's requirements for Low or Moderate security impact level systems.

3.1.3. IMPLEMENT SECURITY CONTROLS

Once the CSP has selected the FedRAMP security control baseline, the next step is to implement the security controls related to that impact level. For most providers, many of the controls are already implemented but need to be described adequately within the FedRAMP templates. Some controls might require the implementation of new capabilities, and some controls might require a re-configuration of existing implementations.

The FedRAMP program takes into account that systems may vary between vendors and allows some flexibility in implementing compensating controls or alternative implementations. The imperative part of implementing security controls is that the intent of a security control is met. CSPs may provide alternative implementations that demonstrate the implementation satisfies the intent of the control requirement. For any control that cannot be met, CSPs must provide justification for not being able to implement the control.

3.1.3.1. SYSTEM SECURITY PLAN

After implementing security controls, CSPs must document the details of the implementation in a System Security Plan. Every security package must include an SSP based on the FedRAMP template. All cloud providers must use the FedRAMP template, regardless of what type of ATO they are vying for. The SSP describes the security authorization boundary, how the implementation addresses each required control, roles and responsibilities, and expected behavior of individuals with system access. Additionally, the SSP allows AOs and review teams to understand how the system is architected, what the system boundaries are, and what the supporting infrastructure for the system looks like.

The SSP template can be found on www.fedramp.gov. Additional guidance about how to describe control implementations in the SSP can be found within the SSP template.

3.1.3.2. INHERITING CONTROLS FROM A LOWER-LEVEL SYSTEM

In the cloud space, many cloud systems rely on other cloud systems to provide a comprehensive set of services for the end customer. An example of this is a software provider utilizing an infrastructure provider to deliver the Software as a Service (SaaS). In this case, the software provider will inherit security controls from the infrastructure provider.

The FedRAMP SSP template provides for marking a control as inherited and from which system that control is being inherited. By allowing for inherited controls, FedRAMP enables the stacking of authorization packages like building blocks. In this model, the SSP for each system must only describe the implementation of that specific system (for example, SaaS service providers in the example above would not detail any implementation details of the leveraging infrastructure provider within the SaaS service SSP). This eliminates redundancy across authorization packages and keeps authorizations delineated by system.

Much in the same way the software provider in the example above relies on the infrastructure provider to deliver services, the software provider also relies on the security implementations and authorization of the infrastructure provider for the software provider's implementations and authorization. Accordingly, if a CSP has inherited controls within the System Security Plan, the authorization of that CSP will be dependent on the authorization of the CSP whose controls they inherit and systems they use to deliver the end service.

3.1.3.3. ADDITIONAL SECURITY CONTROLS FOR SPECIFIC NEEDS

Agencies may require additional security controls above the FedRAMP baseline due to specific Agency mission needs. In this case, the CSP may need to add to the FedRAMP baseline or alter parameters to appropriately address Agency customer needs. CSPs and Agencies must address delta controls by adding them to the FedRAMP templates or by providing a delta document that addresses the unique Agency requirements above the FedRAMP baseline (recommended).

3.1.3.4. SUPPORTING DOCUMENTS

In order to completely and accurately document the security control implementation in the SSP, CSPs must submit supporting documents at the same time the SSP is submitted. 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, a Control Information Summary (CIS), and an Incident Response Plan. Templates for many of these documents are available on www.fedramp.gov.

3.2. ASSESS

CSPs must use an independent assessor to test the information system to demonstrate that the controls are effective and implemented as documented in the SSP. This assessment starts with documenting the methodology and process for testing the control implementation in the Security Assessment Plan (SAP).

3.2.1. USE OF A THIRD-PARTY ASSESSMENT ORGANIZATION

CSPs that seek a JAB P-ATO must use a 3PAO to perform the testing phase of the process.

3.2.2. USE OF A NON-ACCREDITED INDEPENDENT ASSESSOR

CSPs submitting Agency ATO FedRAMP packages must have the system tested by an independent third party; however, they are not required to use a FedRAMP accredited 3PAO. If a non-accredited IA is used, Federal Agencies will be required to submit an attestation describing the independence and technical qualifications of the IA utilized to assess that CSP package.

3.2.3. COMPLETE THE SECURITY ASSESSMENT PLAN

The Security Assessment Plan (SAP) is developed by the 3PAO or IA. The 3PAO or IA creates a testing plan using the FedRAMP SAP template. The SAP identifies all the assets within the scope of the assessment, including components such as hardware, software, and physical facilities. It also provides a roadmap and methodology for execution of the tests and indicates that the 3PAO or IA will use the FedRAMP associated security test cases that are provided in the form of a worksheet.

The SAP template can be found on www.fedramp.gov. Additional details about what must be included within the SAP are located within the SAP template.

3.2.4. USE TEST CASE PROCEDURES

All 3PAOs and IAs must use the FedRAMP baseline security test case cases when assessing a cloud system slated for FedRAMP compliance. FedRAMP baseline security test case procedures are available on www.fedramp.gov.

For any alternative implementations of controls a cloud provider details in the SSP, the 3PAO or IA must create alternative test cases that adequately test the effectiveness of the CSP's control implementation and any risk associated with that implementation.

3.2.5. PERFORM SECURITY TESTING

The 3PAO or IA performs the testing of the CSP's system by following the procedures detailed in the SAP and in accordance with the test case procedures.

While the 3PAO or IA is responsible for performing the tests, this process requires the coordination with the CSP, who must work with the 3PAO or IA to detail an appropriate plan to coordinate on site visits, personnel interviews, and schedule when scans will be performed on the system. CSPs must lock down the system as much as possible during testing in order to remediate any risks found during testing.

3.3. AUTHORIZE

Once testing has been completed, the next step is for AOs to make an authorization decision based on the completed package of documents and the risks identified during the testing phase.

3.3.1. ANALYSIS OF RISKS

After testing the security controls, the 3PAO or IA analyzes the risks and presents the results in a Security Assessment Report (SAR) using the FedRAMP provided template available on www.fedramp.gov. The SAR contains information about vulnerabilities, threats, and risks discovered during the testing process. Additionally, the SAR contains guidance for CSPs in mitigating the security weaknesses found.

The SAR must first be delivered to the CSP for review in order to discuss any mitigating factors, false positives, and other information the 3PAO or IA might not have considered when creating the SAR. Once the CSP and 3PAO or IA have finished their reviews, the 3PAO or IA will then share the SAR with the AO's security team. The AO's team will analyze the SAR to determine the overall risk posture of the CSPs system.

A SAR template is available on www.fedramp.gov and includes guidance on the identification and presentation of risks.

3.3.2. PLAN OF ACTION AND MILESTONES

After receiving the SAR from the 3PAO or IA, the CSP develops a Plan of Action & Milestones (POA&M) that addresses the specific vulnerabilities noted in the SAR. The CSP needs to demonstrate that it has a plan in place, complete with staffing, resources, and a schedule, for correcting each security weakness identified. The POA&M serves as a tracking system for the CSP and represents the CSP's "to do" list.

A POA&M template is also available on www.fedramp.gov.

3.3.3. SUBMISSION OF A SECURITY PACKAGE FOR AUTHORIZATION

Following the development of the SAR, the CSP must assemble a final package and submit the package for authorization review. A final package will include all documents created and referenced within Section 3; all test plans and associated results completed during testing in Section 4, and the SAR and POA&M created in Section 5. AOs will review the entire security package and make a risk-based decision on whether or not to authorize the system.

Note: *All submitted packages must have proper sensitivity markings on the cover page and footer page of documents. Sensitivity markings may be taken into consideration in the event of a Freedom of Information Act (FOIA) request.*

3.3.4. AUTHORIZATION LETTER

Once an AO has made a risk-based decision to authorize a CSP environment for use, they formalize this decision in an ATO letter. AOs provide this letter to the CSP system owner. AOs must also copy the FedRAMP PMO on these letters so that the FedRAMP PMO can verify Agency use, and keep Agencies informed of any changes to a CSP's authorization.

CSPs that have an Agency authorization will have authorization letters granted by a specific Government Agency which allows that Agency to house its data within that CSP's environment. CSPs that go through the JAB will have a P-ATO letter signed by the JAB.

CSPs that receive either type of authorization will be added to the list of authorized CSPs on www.fedramp.gov. The listing will provide basic information about the service offering related to the authorized system. The authorization letter and security package will be stored in a secure, access-controlled, repository for review by Agencies that wish to leverage the CSP's authorization in order to issue their own ATO.

Federal Agencies can leverage FedRAMP security packages from Agencies and the JAB in the same exact fashion. Federal Agencies must review either type of package and make an Agency determination of whether the CSPs risk posture is acceptable for use at that Agency.

3.3.5. LEVERAGING FEDRAMP SECURITY PACKAGES

One of the primary benefits of FedRAMP is the ability for Agencies to reuse authorization packages and to leverage the work that has already been completed–the "do once, use many

times" framework. Agencies may want to review the list of security packages already available before attempting to acquire services from a CSP that is not in the FedRAMP Secure Repository.

The PMO maintains a Secure Repository of FedRAMP security packages for Agencies to review when making procurement decisions. Packages available for review are listed on the FedRAMP website.

This listing on www.fedramp.gov provides a description of the CSPs that have FedRAMP compliant packages, the type of services they offer and the assessment level of the package. It also describes CSPs that are undergoing assessment but have not yet received a P-ATO. After reviewing the list of available CSP packages, Agencies may contact FedRAMP to request access to specific CSP security packages available in the FedRAMP Secure Repository.

The FedRAMP PMO has a prescribed process for allowing access to security package and the FedRAMP Secure Repository. All package reviewers must have a .gov or a .mil email address.

The packages allow Agencies to use existing documentation to assess 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.

If an Agency decides to procure services from a CSP that is listed in the FedRAMP security repository, regardless of the package type, there is a requirement to report this information to the FedRAMP PMO. Agencies can report this information by sending an email to info@FedRAMP.gov. The FedRAMP PMO keeps track of how many times a particular package has been leveraged.

If an Agency decides to leverage a package, regardless of what level the security package meets as described in Section 3.1, the Agency will still need to issue its own ATO. The reason for this is the Federal Information Security Management Act (FISMA) requires Agencies to individually accept the risk of use of any IT system. As described in Section 3.3.3, Agencies may require additional controls to fit their individual circumstances and risk posture.

After reviewing the security authorization package of a CSP, Agencies must be aware that there are always customer responsibilities related to the use of a CSPs services. A key example of this is multi-factor authentication. CSPs can provide the ability to have multi-factor authentication, but Agencies must use and enforce this for the CSP system with its Agency users.

3.3.6. REVOKING AN AUTHORIZATION

CSPs with an authorization are required to implement continuous monitoring, continue to meet the FedRAMP requirements, and maintain an appropriate risk level associated with a Low or Moderate security impact level in order to maintain an authorization. If a CSP fails to maintain

its risk posture and comply with FedRAMP continuous monitoring requirements, the JAB AO or the Agency AO can choose to revoke the CSP's authorization. If an Agency revokes a CSP's FedRAMP Authorization it should notify the FedRAMP PMO by sending an email to info@fedramp.gov. The FedRAMP PMO will notify reliant stakeholders of changes to the status of any CSP authorizations.

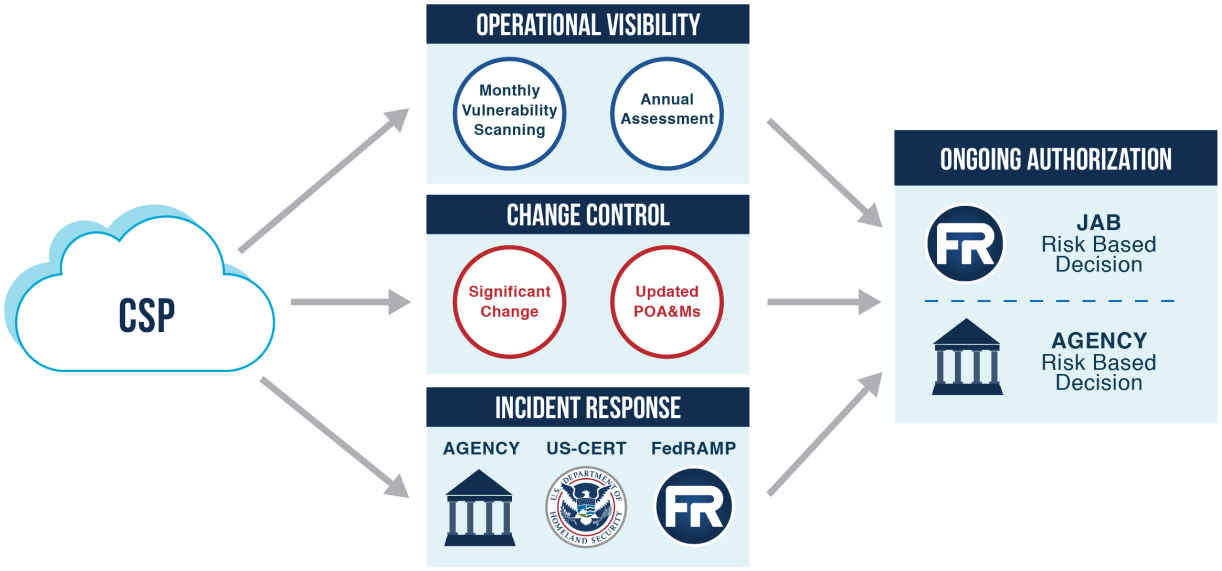
3.4. MONITOR

Ongoing assessment and authorization, hereinafter referred to as continuous monitoring, is the third and final process for cloud services in FedRAMP. Once a CSP receives a FedRAMP Authorization (JAB or Agency), it must implement a continuous monitoring capability to ensure the cloud system maintains an acceptable risk posture. 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.

For systems with a FedRAMP JAB P-ATO, the FedRAMP PMO manages both yearly and monthly continuous monitoring activities: these systems must conduct yearly assessments and must submit monthly continuous monitoring to the FedRAMP PMO. (See Continuous Monitoring Strategy Guide for requirements and details). For systems with an Agency FedRAMP ATO, the Agency must manage continuous monitoring activities and provide at minimum a yearly update to a CSP's security authorization package with the past year's continuous monitoring activities within the FedRAMP Secure Repository.

Continuous monitoring results in greater transparency of 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 continuous monitoring process for FedRAMP Authorizations is detailed in Figure 3, below.

Figure 3 – FedRAMP Continuous Monitoring



3.4.1. OPERATIONAL VISIBILITY

The goal of operational visibility is to reduce the administrative burden associated with demonstrating compliance and instead to shift toward real-time oversight monitoring through automated approaches in accordance with OMB 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 control artifacts, and annual re-assessments. For more information on periodic submission of evidentiary artifacts, refer to the *FedRAMP Continuous Monitoring Strategy Guide* available on www.fedramp.gov.

Annually, CSPs must re-assess a subset of the security controls and send results to the FedRAMP PMO and leveraging Agencies. The re-assessment of these controls must be completed by an IA in the same way testing was completed for the initial authorization. Essentially, the annual assessment is a mini-assessment. The *FedRAMP Continuous Monitoring Strategy Guide* identifies core controls which must be re-tested on an annual basis. The Authorizing Official and CSP must then agree on additional controls that will be tested based on control changes and identified risks in the previous year.

Templates for the annual SAP and SAR are available on www.fedramp.gov.

3.4.2. CHANGE CONTROL

CSPs may make periodic changes to the system according to the procedures found in the system's Configuration Management Plan. 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, significant changes as defined in the SSP and Configuration Management Plan, changes in the CSP's point of contact, changes in the CSP's risk posture, changes to any applications residing on the cloud system, and/or changes to the cloud system infrastructure.

CSPs must notify the AO of any impending change to the system that falls outside of the CSP's Configuration Management Plan to identify if the proposed change rises to the level of a significant change. The CSP must fill out a *FedRAMP Significant Change Security Impact Assessment Form,* which the CSP can download from www.fedramp.gov. The form must include a description of the change and a discussion of the impact of the change to the risk posture. CSPs are encouraged to discuss the change with the respective AO and review teams and the IA for guidance on assessing the risk of the change. CSPs must then submit the form to the AO for review.

A review of the *Security Impact Analysis Form* by the AO will dictate the course of action for the CSPs proposed change between allowing the change to occur within the normal course of a CSP's configuration management all the way to a re-authorization, depending on the severity of the impact.

After any proposed changes are made, any impacted security controls must be documented in the security authorization package and updated documentation must be provided to the AO.

3.4.3. INCIDENT RESPONSE

The shared tenant architecture of cloud services implies that a single incident may impact multiple Federal Agencies leveraging the cloud services. FedRAMP works with US-CERT to coordinate incident response activities in accordance with the *FedRAMP Incident Communications Procedure* published on www.fedramp.gov.

CSPs must have incident response plans in place for all FedRAMP compliant systems, and document it as part of the SSP in Section 3. Incident response plans are required by OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* and NIST SP 800-61, Revision 2*, Computer Security Incident Handling Guide*. In the event of a security incident, a CSP must follow the process and procedures found in the system Incident Response Plan in accordance with the *FedRAMP Incident Communications Procedure.*

AOs must ensure that CSPs report incidents according to the system's documented Incident Response Plan. Any Agencies impacted by a security incident must communicate incident information to US-CERT and the FedRAMP PMO according to procedures prescribed in this document.

Based on the severity and outcome of security incidents and the impact they have on the security posture of a CSP environment, AOs may initiate a review of a CSP's authorization. Failure to report incidents may also trigger a review of a CSP's authorization.

4. THIRD PARTY ASSESSMENT ORGANIZATIONS

FedRAMP requires the use of independent assessors for all FedRAMP compliant authorizations. For JAB provisional authorizations, a FedRAMP accredited 3PAO must be used. FedRAMP has established a conformity assessment process to accredit 3PAOs. 3PAOs, essentially, are the auditing firms that perform initial and periodic assessments of CSP systems per FedRAMP requirements, provide evidence of compliance, and play an ongoing role in ensuring that CSPs meet FedRAMP requirements. 3PAOs provide the independent assessment that assures AOs at Federal Agencies that a cloud computing service meets the security requirements outlined by FedRAMP and any risks or deficiencies are identified.

4.1. REQUIREMENTS FOR ACCREDITATION

FedRAMP requires accredited 3PAOs to meet the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17020 standards, as revised, for independence and managerial competence. In addition, accredited 3PAOs must meet FedRAMP requirements for technical FISMA competence through demonstrated expertise in assessing cloud-based solutions. FedRAMP bases its accreditation process for 3PAOs 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.

The specific 3PAO requirements can be found on www.fedramp.gov.

4.2. BECOMING AN ACCREDITED 3PAO

FedRAMP has transitioned the accreditation process for 3PAOs to the private sector and has selected American Association of Laboratory Accreditors (A2LA) to perform the assessment activities associated with becoming an accredited 3PAO. A2LA will use the 3PAO requirements available on FedRAMP.gov and coordinate with the FedRAMP PMO to accredit 3PAOs. The FedRAMP PMO will continue to be the only authority able to fully accredit FedRAMP 3PAOs.

Information regarding the process to obtain an A2LA FedRAMP 3PAO assessment can be found at www.A2LA.org/FedRAMP.

APPENDIX A: FedRAMP ACRONYMS

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

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

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

APPENDIX B: SUMMARY OF FedRAMP STAKEHOLDERS

Table 1: Summary of FedRAMP Stakeholders

ROLE	DUTIES AND RESPONSIBILITIES
JAB Members (CIOs 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 AO. ▪ Support the FedRAMP PMO in defining and implementing the joint authorization process. ▪ Recommend authorization decisions to the JAB AO. ▪ Escalate issues to the JAB AO as appropriate.
FedRAMP 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 and A2LA 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	▪ 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.