FedRAMP ANNUAL ASSESSMENT GUIDANCE

Version 2.0

November 24, 2017

FedRAMP

EXECUTIVE SUMMARY

The FedRAMP Joint Authorization Board (JAB) updated the FedRAMP security controls baseline to align with National Institutes of Standards and Technology (NIST) Special Publication 800-53 (SP 800-53), Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4. The FedRAMP Program Management Office (PMO) updated the FedRAMP baseline security controls, documentation, and templates to reflect the changes in NIST SP 800-53, revision 4.

This document provides guidance to assist Cloud Security Providers (CSPs), FedRAMP Third-Party Assessment Organizations (3PAOs), and Federal agencies in determining the scope of an annual assessment based on NIST SP 800-53, revision 4, FedRAMP baseline security requirements, and FedRAMP continuous monitoring requirements.

Cloud Service Providers (CSPs) and Federal Agencies with systems currently FedRAMP compliant based on NIST SP 800-53, revision 4 should use this document for guidance. This document is also intended to assist 3PAOs in planning and conducting security assessments and reports for those systems based on NIST SP 800-53, revision 4.

This document includes the security controls selection list. This list provides a structured approach and assists in development of the scope for conducting assessments based on FedRAMP NIST SP 800-53, revision 4, FedRAMP baseline security requirements, FedRAMP continuous monitoring requirements, and CSP-specific implementations.

DOCUMENT REVISION HISTORY

DATE	VERSION	PAGE(S)	DESCRIPTION	AUTHOR
04/05/2016	1.0	All	Initial draft guidance on completing annual assessments based on FedRAMP NIST SP 800 53 Revision 4, FedRAMP baseline security requirements, and FedRAMP continuous monitoring requirements.	FedRAMP PMO
06/06/2017	1.0	Cover	Updated logo	FedRAMP PMO
11/24/2017	2.0	All	Updated to the new template	FedRAMP PMO

HOW TO CONTACT US

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

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

TABLE OF CONTENTS

LIST OF TABLES

1. INTRODUCTION

The FedRAMP Program Management Office (PMO) published several documents and templates based on NIST SP 800-53, Revision 4, FedRAMP baseline security requirements, and FedRAMP continuous monitoring requirements to assist FedRAMP compliant Cloud Service Providers (CSPs) and Federal Agencies in becoming compliant with NIST SP 800-53, Revision 4. This document defines the FedRAMP process for determining the scope and selection of controls to be included as part of an annual assessment for those systems that have completed transition to Revision 4 requirements.

1.1. PURPOSE

The purpose of this document is to facilitate a structured approach to completing security assessments and reports required to meet FedRAMP compliance based on NIST SP 800-53, revision 4.

This document describes a recommended methodology for determining the scope of the annual assessments and reports including a recommended methodology for addressing risks associated with continuing to leverage cloud services (e.g., Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS)) that have not yet completed the transition FedRAMP NIST SP 800-53, revision 4.

1.2. SCOPE

The scope of this document includes completing annual assessments in compliance with NIST SP 800-53, revision 4, FedRAMP baseline security requirements, FedRAMP continuous monitoring requirements, and CSP-specific cloud service implementations.

1.3. ASSUMPTIONS

The guidance and recommendations in this document for CSPs, Federal Agencies, and 3PAOs is based on the following assumptions:

- The Cloud Service is currently compliant with FedRAMP based on NIST SP 800-53, revision 4
- The CSP, at a minimum, is conducting continuous monitoring in compliance with the current FedRAMP Continuous Monitoring and Strategy Guide
- All services and components included in the boundary for authorization will be assessed for compliance with applicable controls determined as in-scope for this assessment

- CSPs will be required to identify the impact and risks associated with leveraging systems that have not yet become FedRAMP NIST SP 800-53, revision 4, compliant

1.4. COMPLIANCE

FedRAMP approved CSPs (those with an existing P-ATO) must comply with this guidance for all annual assessments completed following transition from FedRAMP NIST SP 800-53, revision 3 to FedRAMP NIST SP 800-53, revision 4. Not doing so may be considered a failure to maintain an adequate risk management program and result in escalation actions as described in the *FedRAMP P-ATO Management and Revocation Guide*.

2. TASKS REQUIRED TO COMPLETE THE ASSESSMENT

2.1. DEVELOP SCHEDULE

Major milestone activities for a schedule to complete the annual assessment include the following:

- Review and update, as required, the System Security Plan (SSP) and attachments
- Conduct Incident Response Plan Test and provide the Incident Response Plan Test Report
- Conduct Contingency Plan functional test and include the Contingency Plan Test Report
- Complete the Annual Assessment Security Assessment Plan (SAP)
- Conduct testing
- Complete Annual Assessment Security Assessment Report (SAR)
- Complete the Plan of Action and Milestones (POA&M)
- Submit the complete Annual Assessment package, including the SAR and attachments, updated SSP and attachments, updated SAP, and POA&M to FedRAMP PMO or Agency AO

The schedule must include timeframes and resources to support technical and quality assurance reviews of all deliverables.

2.2. REVIEW AND UPDATE DOCUMENTATION

The CSP is required to review the SSP and all attachments and update as necessary at least annually to incorporate system changes and/or changes in processes and procedures. In particular, the CSP is required to review and update implementation details (e.g., who, what, how) as necessary for all controls that are “in-scope” for this assessment to ensure adequate details are provided.

In addition, the FedRAMP PMO periodically publishes updates to the document templates and the CSP should review these new templates to ensure significant changes either are incorporated into the CSP’s documents or new documents are created to address the changes prior to performing the updates.

2.3. DETERMINE SCOPE OF ASSESSMENT

The determination of the FedRAMP NIST SP 800-53 revision 4 “in-scope” set of controls for annual assessments is based on the following:

2.3.1. FEDRAMP-SELECTED CONTROLS

The determination of FedRAMP-selected list of core controls (as defined in the *FedRAMP Annual Assessment Control Selection Workbook,* see section 5), those controls required to be assessed annually by all CSPs, is based on the FedRAMP NIST SP 800-53 Rev3 to Rev4 Transition Control List, as follows:

- Core controls
  - Controls and enhancements (including parameters) that have an associated NIST SP 800-53, revision 4 and/or FedRAMP-defined operational frequency that is
    - CSP- defined
    - FedRAMP-defined
    - Less than 3 years, including those that are at varied timeframes (e.g. hourly, daily, monthly, quarterly) and continuous
  - Controls FedRAMP has determined are critical to protecting the information system.
  - Controls FedRAMP has determined necessary to ensure continued operation and implementation of the control as intended, based on the NIST definition of volatility:

Dan F
Form

Dan F
Delet

- *Security control volatility is a measure of how frequently a control is likely to change over time subsequent to its implementation. Special Publication 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations*
- Reference: NIST SP 800-137, dated September 2011, Section 3.2.2, Establish Monitoring and Assessment Frequencies, page 28.

2.3.2. FEDRAMP-SELECTED CONTROLS, NOT-INCLUDED FOR TESTING BY CSP

The FedRAMP-selected list of core controls that are not applicable to a CSP's implementation of cloud services are not required to be tested on an annual basis, based on the following criteria:

- Controls that are not applicable to the CSP's implementation (e.g., controls related to provision and management of wireless services when no wireless network capability is implemented). The 3PAO is required to validate that Not Applicable controls are not applicable.
- Controls that are fully "inherited" and entirely the responsibility of a leveraged provider are not required to be tested by the CSP leveraging those services. The 3PAO is required to validate that the inherited services and/or controls continue to the meet the terms of use in accordance with the FedRAMP P-ATO or Agency ATO.

2.3.3. CSP-SPECIFIC CONTROLS, SELECTED BY CSP

In addition to the FedRAMP-Selected List of Core Controls, the CSP is required to select additional controls for testing based on the following criteria:

- CSP-selected controls that may be required to address periodicity requirements (e.g., testing is required at least once every 3 years).
- CSP-selected controls required to address system changes that have been implemented by the CSP since the last annual assessment, (e.g., closed POA&M items, including Vendor Dependencies (VDs), Deviation Requests (DRs), and system changes).

2.3.4. ADDITIONAL TESTING REQUIREMENTS

In addition, the 3PAO must evaluate (review and/or test), as necessary, all items related to continuous monitoring activities. The 3PAO must evaluate all open POA&M items (including Vendor Dependencies); POA&M closures (to confirm adequate closure) and validate and confirm continued applicability of Deviation Requests (False Positives, Risk Adjustments and Operational Requirements).

2.3.5. CONTROL SELECTION PROCESS

CSPs must complete the *FedRAMP Annual Assessment Control Selection Workbook*, in Section 5, to determine the controls selected for testing in the annual assessment. The following sections provide guidance on completing the Worksheet.

The completed Worksheet must be included in the SAP and SAR prepared and submitted by the 3PAO.

2.3.6. WORKSHEET: LIST OF CONTROLS

The *FedRAMP Annual Assessment Control Selection Workbook* template has two sections. The top section of the template documents general system information as described in the table below:

Table 1 – FedRAMP Annual Assessment Control Selection Worksheet General Information Description

GENERAL INFORMATION	DETAILS
Date	Provide the date the template is completed.
CSP	The Vendor Name as supplied in any of the documents provided to the AO.
System Name	The Information System Name as supplied in any of the documents provided to the AO.
3PAO	The name of the 3PAO completing the assessment.

The next section of the worksheet has three sections: List of Core Controls, CSP-Specific Controls, and Comments. These sections are described in the tables below:

Table 2 – FedRAMP Annual Assessment Controls Selection Worksheet – Selected List of Core Controls

COLUMN HEADER	CONTENT DESCRIPTION
Column A – Item No.	This is the item number of the control all CSPs are required to test.
Column B – Control ID	This is the NIST SP 800-53 revision 4 unique control identifiers for the core controls all CSPs are required to test.
Column A – Totals	This row indicates the total controls listed in List of Core Controls (column B) and FedRAMP- Selected Controls Not Included for Testing by CSP (column D); and CSP-Specific, Selected controls (column G).

COLUMN HEADER	CONTENT DESCRIPTION
Column B – Number	This is the item number of the core controls required for testing
Column C – Divider	This column separates List of Core Controls (column B) from FedRAMP- Selected Controls Not Included for Testing by CSP (column D)

Table 3 – FedRAMP Annual Assessment Controls Selection Worksheet – Selected Controls Not Included for Testing by CSP

COLUMN HEADER	CONTENT DESCRIPTION
Column D – Indicate Rationale: Not Applicable/Not Implemented, Inherited from a Leveraged System	These are core controls that the CSP has selected to exclude from testing. The CSP is required to indicate the rationale for the determination for excluding this control from the scope of testing and the 3PAO must validate this rationale. For example, the control is not applicable because the requirement is related to a service or component that has not been implemented by the CSP (e.g., wireless access) or a control is fully inherited from a leveraged. The 3PAO is required to validate that Not Applicable controls are not applicable. The total number of controls in this column will be entered in the last row of the list.
Column E – Divider	The column separates FedRAMP- Selected Controls Not Included for Testing by CSP (column D) from CSP-Specific Controls, Selected by CSP (columns F-H).

Table 4 – FedRAMP Annual Assessment Controls Selection Worksheet – CSP: Specific Controls Selected by CSP

COLUMN HEADER	CONTENT DESCRIPTION
Column F – Item	This is the item number of the additional control selected for testing based on CSP-specific implementations and continuous monitoring activities.
Column G – Control ID	This is the list of NIST SP 800-53 Rev4 unique control identifiers for the additional controls selected for testing by the CSP for this annual assessment.
Column H – Indicate Rationale: POA&M Closure, DR, System Change, Periodic Testing Requirement	The CSP is required to indicate the rationale for the determination to test this control. For example, the control requirement is related to a Deviation Request for a False Positive, Risk Adjustment, and/or Operational Requirement, Vendor Dependencies, or a system change implemented by the CSP since the last annual assessment. The 3PAO is required to validate these items for continued applicability to the system.
Column I – Comments	Additional information related to the controls selected for testing may be provided in this column.
Column J – Divider	This column separates the CSP-Specific Controls from the Total Number of Controls Selected for This Assessment.

Table 5 – FedRAMP Annual Assessment Controls Selection Worksheet – Total Number of Controls Selected for This Assessment

COLUMN HEADER	CONTENT DESCRIPTION
Column K – Total Number of Controls Selected for This Assessment	This column provides a total number of controls selected for this assessment. The number is calculated in the last row of the table by subtracting the total in Column D from the total in Column B and adding the total in Column H.

2.4. COMPLETE SECURITY ASSESSMENT

3PAOs must complete all security assessments in accordance with the same processes and procedures required by FedRAMP. The scope of the assessment will be based on the results of the control selection process and the testing will utilize the FedRAMP Revision 4 Test Cases (Refer to Section 6, FedRAMP Revision 4 Test Cases) and the requirements specified in the FedRAMP Continuous Monitoring and Strategy Guide.

2.4.1. SECURITY ASSESSMENT PLAN (SAP)

The 3PAO prepares and submits the Security Assessment Plan (SAP) utilizing the FedRAMP revision 4 Security Assessment Plan Template for Annual Assessments located on the FedRAMP website (fedramp.gov). The SAP clearly defines the process, procedures, and methodologies for testing. The scope of controls to be tested is based on the control selection process defined in this document. Include only those test cases for selected controls. Some test cases may need to be modified to address CSP-specific implementations as described in the SSP and other supporting documentation. The test cases may need to be modified for those controls selected for validation of closed POA&M items, DRs, Vendor Dependencies, and system changes.

2.4.2. SECURITY ASSESSMENT REPORT (SAR)

The 3PAO prepares and submits the Security Assessment Report (SAR) utilizing the FedRAMP revision 4 Security Assessment Report Template for Annual Assessments. The SAR clearly defines the process, procedures, and methodologies utilized for testing as required and documents all the results of the testing conducted.

The SAR clearly identifies what was tested and what was not tested as part of this assessment, especially related to non-applicable controls and inherited controls from leveraged systems as may be applicable.

The SAR clearly identifies known risks associated with leveraged systems, if applicable.

2.4.2.1. THE JAB AND/OR AO DETERMINE WHETHER THE OVERALL RISK POSTURE OF THE SYSTEM, AS DEFINED IN THE SAR, IS ACCEPTABLE. SECURITY ASSESSMENT TEST CASES

The 3PAO prepares and submits the FedRAMP Security Assessment Test Cases and supporting documentation as part of the SAR. The test cases contain all the FedRAMP NIST SP 800-53, revision 4, control requirements with associated required test methods for each of the selected controls.

The 3PAO fully completes and documents the assessment information related to the controls selected for the assessment, e.g., detailed observations and evidence, implementation status, findings, and risk exposure information.

2.4.2.2. WORKSHEET 1: SYSTEM

This System worksheet provides system and CSP general information.

Table 6 – FedRAMP Security Assessment Test Cases – System Content Description

COLUMN A	COLUMN B
System Name	This is the name of the system.
CSP Name	This is the name of the CSP.
Sensitivity Level	This is the security impact level of the system (Moderate/Low).

2.4.2.3. WORKSHEET 2: CTRL SUMMARY

The CTRL Summary worksheet provides the test results summary of all the test cases for controls selected for this assessment.

Table 7 – FedRAMP Security Assessment Test Cases – Control Summary Column Content Description

COLUMN A	COLUMN B
Column B – CONTROL TITLE (NIST SP 800-53 Rev 4)	This is the NIST SP 800-53 revision 4 control title.
Column C – Control Baseline – Low	This lists the FedRAMP NIST SP 800-53 revision 4 baseline controls at the low impact level.
Column D – Control Baseline – Moderate	This lists the FedRAMP NIST SP 800-53 revision 4 baseline controls at the moderate impact level.

COLUMN A	COLUMN B
Column E – Implementation Status	Specify the implementation status of the control at the completion of testing [implemented/partially implemented/ planned/ alternative implementation/not applicable].
Column F – Findings	Specify the status of the control at the completion of testing [satisfied/other than satisfied].
Column G – Risk Exposure	Specify the risk exposure to the system if the vulnerability associated with this control is exploited [high/moderate/low].
Column H – Prior Findings	Specify the status of any prior finding associated with this control.
Column I – Prior Risk	Specify the risk exposure to the system if the vulnerability associated with this control is exploited [high/moderate/low].

2.4.2.4. WORKSHEET 3-19: CONTROLS “AC” THROUGH “SI”

The FedRAMP Security Assessment Test Cases workbook contains a separate worksheet for documenting the tests conducted for each of the 17 control families in the FedRAMP NIST SP 800-63 revision 4 baseline.

Table 8 – FedRAMP Security Assessment Test Cases – Controls “AC” through “SI” Column Content Description

COLUMN A	COLUMN B
Column A – Name	This is the NIST SP 800-53 revision 4 unique control identifier.
Column B – Title	This is the NIST SP 800-53 revision 4 control title.
Column C – Decision	This specifies each of the security control requirements to be tested.
Column D – Examine	This specifies what is required to be examined to determine the implementation of the control requirement.
Column E – Test	This specifies what is required to be tested to determine the implementation of the control requirement.
Column F – Interview	This specifies the interview requirements to determine the implementation of the control requirement.
Column G – Observations and Evidence	Specify and fully describe the testing and observations from the testing, including references to artifacts utilized as evidence to support the observations. Specify full document references [title, version, date, and page numbers] for all documentation artifacts. Specify full names, roles, and dates of interviews. Specify the tests conducted at a level of detail that enables them to be replicated.
Column I – Prior Risk	Specify the risk exposure to the system if the vulnerability associated with this control is exploited [high/moderate/low].

COLUMN A	COLUMN B
Column H – Implementation Status	Specify the implementation status of the control at the completion of testing [implemented/partially implemented/ planned/ alternative implementation/not applicable].
Column I – <date> Findings	Insert the date of the testing in the Column Header and specify the status of the control at the completion of testing for each test [satisfied/other than satisfied].
Column J – Likelihood	Specify the likelihood a threat will exploit the vulnerability identified [high/moderate/low].
Column K – Impact	Specify the impact to the system if the threat successfully exploits the vulnerability [high/moderate/low].
Column L – Risk Exposure	Specify the risk exposure to the system if the vulnerability associated with this control is exploited [high/moderate/low].
Column M – Risk Description	Fully describe the details of the risks to this specific system if the vulnerability is exploited.
Column N – Recommendation for Mitigation	Fully describe the recommendation for remediation of the risk associated with this control.
Column O – Assessor POC	Specify the assessor name and contact information [e.g., email, phone] for each test.
Column P – Divider	This column separates the results of the current assessments from results and findings from previous assessments.
Column Q – <Date> Prior Findings	Insert the date of the previous assessment and specify the status of a prior finding associated with this control. [satisfied/other than satisfied].
Column R – <Date> Prior Risk	Insert the date of the previous assessment and specify the risk exposure to the system if the vulnerability associated with this control is exploited. [High/Moderate/Low].

2.5. COMPLETE PLAN OF ACTION AND MILESTONES (POA&M)

The CSP prepares and submits the Plan of Action and Milestones (POA&M) utilizing the FedRAMP Plan of Action and Milestone (POA&M) Template Completion Guide. The CSP documents all residual risks identified in the SAR and defines a plan for remediation of those risks in the template provided and provides an inventory list of the system tested.

The CSP includes known risks identified by the 3PAO that are associated with leveraged systems in the POA&M.

3. METHODOLOGY FOR MANAGING RISKS ASSOCIATED WITH INHERITED CONTROLS

3.1. METHODOLOGY FOR TESTING INHERITED CONTROLS

The methodology for testing controls inherited from a FedRAMP compliant system (leveraged system) is explicitly based on how the requirement is described in the SSP. The SSP for the Cloud Service leveraging a system clearly defines the roles and responsibilities for every control requirement. The CSP must describe how the control is implemented and how it is using the inherited control in the leveraged system SSP. For example, a Physical and Environmental (PE) control might be fully inherited from the leveraged system. The CSP describes “how” the PE control requirement is implemented; including stating it is fully inherited from the leveraged system. There is a subsection in the control implementation description that states “what” the leveraged system is providing to meet the requirement but not “how” the leveraged system meets the requirement. The 3PAO must verify the CSP is using the control consistent with the SSP.

In another example, a control requirement might be a “shared” control, where the System and the leveraged system implement portions of a requirement to fully meet the requirement. In this case, the CSP would define “what” and “how” the CSP is implementing the portion they are responsible for, and there would be a subsection in the implementation description where the “what” being provided by the leveraged system is described. However, the description of “how” the leveraged system implements their portion of the control would be found in the leveraged system SSP.

The scope of testing for the CSP leveraging a FedRAMP compliant leveraged system includes only control requirements that the CSP is responsible for implementing, either wholly or partially. The 3PAO tests only the control requirement implemented by the CSP and assumes the leveraged system is compliant with the requirements based on their initial and continued P-ATO or ATO status. The scope of testing does not include “testing” of the implementation by the leveraged system. If the leveraged system provides a service such as auditing/logging or trouble ticketing, the 3PAO must collect evidence from only the CSP that the leveraged system is providing those services (e.g., audit logs/reports).

3.2. METHODOLOGY FOR REPORTING AND MANAGING RISKS ASSOCIATED WITH INHERITED CONTROLS

The 3PAO may have identified some known risks associated with the system leveraged by a CSP. These risks may be due to a “gap” in implementation of all the requirements in a control between the CSP and the leveraged system. These risks may result from the CSP not having fully implemented a requirement that they are responsible for implementing or the leveraged system may not have fully implemented and tested the FedRAMP NIST SP 800-53, revision 4baseline requirements.

The 3PAO must include these known risks in the SAR and the CSP must include these known risks in the POA&M (including Vendor Dependencies) and track and report the status of those risks as part of continuous monitoring activities. For example, the CSP indicates in the POA&M that they have communicated with the applicable POC of the leveraged system to determine the current status of remediation of those risks at least every 30 days.

Consider the following example: The IaaS CSP currently has only implemented FedRAMP NIST SP 800-53, revision 3 requirements. The SaaS leveraging the IaaS has implemented FedRAMP NIST SP 800-53, revision 4. During the assessment of the SaaS, it was determined that the leveraged IaaS had not transitioned to implementation of FedRAMP NIST SP 800-53, revision 4. To be compliant, the SaaS CSP must have the following:

- Have a SAR that identifies the gaps in the inherited controls (gaps from Rev. 3 to Rev. 4)
- The SaaS POA&M must track these deficiencies
- These findings are identified as “Vendor Dependencies”. The SaaS CSP must verify the status of these deficiencies every 30 days and document the status in the POA&M
- The SaaS SSP must reflect these inherited controls are partially implemented or planned based on the SAR findings
- The SaaS SSP text for these inherited controls must include “Pending full implementation and testing by <CSP/System Name>”
- Closure of these POA&Ms can occur once the leveraged IaaS CSP meets the FedRAMP NIST SP 800-53, revision 4 requirements and has fully and successfully tested the implementation of these controls

The preceding is only an example. It does not imply the requirements only apply to SaaS providers. Similar requirements apply whenever a CSP claims vendor dependency as the reason for an open POA&M item. During the annual assessment, the 3PAO verifies the applicable requirements are met.

4. GENERAL REQUIREMENTS

- Use latest version for all FedRAMP document templates located on the FedRAMP website, such as SSP, CP, SAP, and SAR.
- Ensure that all requirements are addressed and documented completely. Identify specifically what was included in the scope of the assessment and what was excluded, including the rationale for both.

- Ensure there are enough resources to complete the required tasks in the timeframes defined.
- Develop and implement a schedule that supports completion of the assessment prior to anniversary date of P-ATO or ATO.
- Develop and implement a schedule that provides for revisions and updates to draft documents based on FedRAMP and AO technical reviews.
- Ensure that all findings are included in the SAR and POA&M.

5. CONTROL SELECTION WORKBOOK

The FedRAMP Annual Assessment Control Selection Workbook is provided here.

FedRAMP Annual
Assessment Control S

6. FEDRAMP REVISION 4 TEST CASES

The *FedRAMP Revision 4 Test Cases v 1.0* workbook can be found on the FedRAMP website at the following URL: https://www.fedramp.gov/resources/templates-3/.

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.