

FedRAMP Revision 4 Transition
Guide



FedRAMP

Version 3.0

September 22, 2015

Executive Summary

The Federal Risk and Authorization Management Program (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 (Rev4). 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, and published the *FedRAMP Revision 4 Transition Guide*, Version 2.0, dated June 6, 2014.

This document provides guidance to assist Cloud Service Providers (CSP), FedRAMP Third-Party Assessment Organizations (3PAO), and Federal agencies in transitioning to NIST SP 800-53 Revision 4, and to the new FedRAMP requirements.

Document Revision History

Date	Version	Page(s)	Description	Author
06/06/2014	2.0	All	Transition Guide - Major revision for SP800-53 Revision 4, includes new template and formatting changes	FedRAMP PMO
03/11/2015	1.0	All	Additional Guidance - Transitioning to FedRAMP NIST SP 800 53 Revision 4, including test cases and guidance on completing security assessments and reporting	FedRAMP PMO
9/22/2015	3.0	All	Combined Transition Guide and Additional Guidance, clarification and simplification of required transition date and Clarification for leveraging CSPs not meeting Rev4	FedRAMP PMO

HOW TO CONTACT US

Send questions about FedRAMP or this document to info@fedramp.gov.

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

Table of Contents

Executive Summary	ii
Document Revision History	iii
How to contact us	iii
1. Introduction	1
1.1 Purpose	1
1.2 Scope.....	1
2. FedRAMP Revision 4 Transition Schedule	2
3. Tasks Required to Complete the Transition.....	2
3.1 Develop Schedule	2
3.2 Update Documentation to FedRAMP Revision 4 Templates.....	2
3.3 Determine Scope of Assessment	3
3.3.1 Control Selection Process.....	3
3.3.1.1 Worksheet 1: Rev4 Controls Summary.....	3
3.3.1.2 Worksheet 2: Conditional Controls.....	4
3.3.1.3 Worksheet 3: CSP-Specific Controls	5
3.3.1.4 Worksheet 4: Inherited Controls	6
3.4 Complete Security Assessment.....	6
3.4.1 Security Assessment Plan (SAP).....	6
3.4.2 Security Assessment Report (SAR)	7
3.4.2.1 SECURITY ASSESSMENT Test Cases.....	7
3.4.2.1.1 Worksheet 1: System.....	7
3.4.2.1.2 Worksheet 2: CTRLSummary.....	7
3.4.2.1.3 Worksheets 3 -19: Controls “AC” through “SI”	8
3.5 Complete Plan of Action and Milestones (POA&M).....	9
4. Methodology for Managing Risks associated with Inherited Controls.....	9
4.1 Methodology for Testing Inherited Controls	9
4.2 Methodology for Reporting and Managing Risks Associated with Inherited Controls	10
5. General Requirements.....	11
6. Control Selection Workbook	11
7. FedRAMP Revision 4 Test Cases	11
Appendix A – FedRAMP Acronyms	12

List of Tables

Table 1. FedRAMP Rev3 to Rev4 Annual Assessment Controls Template Header Information Description	3
Table 2. FedRAMP Rev3 to Rev4 Annual Assessment Controls - Column Content Description	3
Table 3. FedRAMP Rev3 to Rev4 Annual Assessment Controls – Conditional Controls Column Content Description.....	4
Table 4. FedRAMP Rev3 to Rev4 Annual Assessment Controls – CSP-Specific Controls Column Content Description.....	5
Table 5. FedRAMP Rev3 to Rev4 Annual Assessment Controls – CSP Inherited Controls Column Content Description.....	6
Table 6. FedRAMP Security Assessment Test Cases – System Content Description.....	7
Table 7. FedRAMP Security Assessment Test Cases – Control Summary Column Content Description	8
Table 8. FedRAMP Security Assessment Test Cases – Controls “AC” through “SI” Column Content Description.....	8

1. INTRODUCTION

The Federal Risk and Management Program (FedRAMP) Program Management Office (PMO) published the *FedRAMP Revision 4 Transition Guide*, Version 2.0, dated June 6, 2014, and additional guidance on March 11, 2015 to assist FedRAMP compliant Cloud Service Providers (CSP) and Federal Agencies in becoming compliant with NIST SP 800-53, Revision 4. This document combines the guidance and additional guidance documents and clarifies the transition timelines and the FedRAMP PMO's expectations for migration.

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. In addition, it defines the required deadlines for transitioning from Revision 3 (Rev3) to Revision 4 (Rev4). NIST released SP 800-53 Revision 4 in April 2013. NIST recommends incorporating the new publication within twelve months of release. FedRAMP released updated control requirements incorporating Revision 4 in June 2014.

This document identifies: (i) the timeline required for transition, (ii) the tasks required to transition, including a recommended methodology for determining the scope of the assessments and reports, and (iii) a recommended methodology for addressing risks associated with continuing to leverage CSPs (e.g., Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) that have not yet completed the transition.

1.2 SCOPE

The scope of this document is to provide guidance specifically related to completing transition from compliance with FedRAMP security requirements based on NIST SP 800-53, Revision 3, to FedRAMP security requirements based on NIST SP 80-53, Revision 4. The scope of the guidance is to assist CSPs, Federal Agencies, and 3PAOs, based on the following assumptions:

- The CSP is currently compliant with FedRAMP based on NIST SP 800-53, Revision 3.
- The CSP, at a minimum, is conducting continuous monitoring in compliance with the current *FedRAMP Continuous Monitoring and Strategy Guide (ConMon Guide)*, Version 2.0, dated June 6, 2014.
- CSPs providing IaaS services will be transitioning all services and components included in the boundary for authorization for NIST SP 80-53, Revision 4 compliance.
- CSPs will be required to identify the impact and risks associated with leveraging IaaS and/or PaaS services that have not yet become FedRAMP NIST SP 800-53, Revision 4, compliant.

2. FEDRAMP REVISION 4 TRANSITION SCHEDULE

NIST recommends adoption of new guidance within twelve months of issuance. FedRAMP issued the Revision 4 requirements in June 2014 along with an implementation schedule that provided flexibility for transitioning existing authorized or provisionally authorized systems at their next annual assessment. FedRAMP also provided additional time for systems that were engaged in activities leading up to the annual assessment, allowing those systems twelve months to transition, starting after the next annual assessment date.

FedRAMP requires all CSPs to transition to the FedRAMP Revision 4 requirements by the end of the 2015 calendar year. As of January 1, 2016, the FedRAMP PMO will not accept Revision 3 system documentation as FedRAMP compliant.

3. TASKS REQUIRED TO COMPLETE THE TRANSITION

3.1 DEVELOP SCHEDULE

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

- Complete a new System Security Plan (SSP) and attachments.
- Complete the *Security Assessment Plan (SAP) Template for Annual Assessment*. This template is available in the Monitor Phase section of this FedRAMP website page: <https://www.fedramp.gov/resources/templates-3/>.
- Submit SSP and SAP to FedRAMP PMO or Agency Authorizing Official (AO) for approval.
- Conduct testing.
- Complete the *Annual Security Assessment Report (SAR) Template*. This template is available in the Monitor Phase section of this FedRAMP website page: <https://www.fedramp.gov/resources/templates-3/>.
- Submit Annual Assessment SAR, attachments, and updated SSP to FedRAMP PMO or Agency AO.

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

3.2 UPDATE DOCUMENTATION TO FEDRAMP REVISION 4 TEMPLATES

The FedRAMP PMO has published updated templates for the SSP and attachments. CSPs must complete an entirely new SSP based on the updated template. CSPs should review the website for updated templates and revise the affected documents as required to address the changes in the template documents.

3.3 DETERMINE SCOPE OF ASSESSMENT

The scope of the assessment is based on determining the specific FedRAMP NIST SP 800-53 Revision 4 controls that require testing by the assessor. All CSPs are required to test some controls, and other controls may need to be required based on CSP-specific implementations and continuous monitoring activities.

3.3.1 CONTROL SELECTION PROCESS

CSPs utilize the *FedRAMP Rev3 to Rev4 Annual Assessment Controls Template* to determine which controls are in scope for testing. The template is an Excel Workbook containing four worksheets: the Rev4 Controls Summary worksheet, the Conditional Controls worksheet, the CSP-Specific Controls worksheet, and the Inherited Controls worksheet. The CSPs should complete the Conditional Controls worksheet first, to ensure that all required Rev4 controls have been addressed.

3.3.1.1 WORKSHEET 1: REV4 CONTROLS SUMMARY

The Rev4 Controls Summary worksheet has two sections. The top section of the worksheet documents basic system information tracks the headers described in Table 1 below:

Table 1. FedRAMP Rev3 to Rev4 Annual Assessment Controls Template Header Information Description

Header	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 bottom section of the Rev4 Controls Summary worksheet is the summary of all controls identified for testing for this assessment and contains the information in Table 2 below:

Table 2. FedRAMP Rev3 to Rev4 Annual Assessment Controls - Column Content Description

Column Header	Content Description
Column A - Item	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 identifier for the control all CSPs are required to test.
Column C - Core	This column indicates the controls specified for periodic testing in the <i>ConMon Guide</i> that are required to be tested by all CSPs.
Column D - New	This column indicates the additional new FedRAMP NIST SP 800-53 Revision 4 baseline controls that all CSPs are required to test.

Column Header	Content Description
Column E - Conditional- Refer to "Conditional Controls" Worksheet for further details	This column indicates the additional controls that are required to be considered for testing by all CSPs based on the responses to the criteria provided in Worksheet 2: Conditional Controls.
Column F – Divider	This column divides the group of controls required to be tested or considered for testing by all CSPs from the group of controls that are to be included based on CSP-specific implementations and continuous monitoring activities.
Column G - Item	This is the item number of the control selected for testing based on CSP-specific implementations and continuous monitoring activities.
Column H - Control ID - CSP-Specific - Refer to "Conditional Controls" Worksheet for further details	Specify the NIST SP 800-53 Revision 4 unique control identifier for the controls listed in Worksheet 2 with a final determination of "No" based on the analysis performed by the 3PAO.
Column I – Control ID - CSP-Specific-Refer to "CSP-Specific Controls" Worksheet for further details	Specify the NIST SP 800-53 Revision 4 unique control identifier for the controls selected for testing based on the rationale defined in Worksheet 3: CSP-Specific Controls.
Column J - Control ID - CSP Specific - Refer to "Inherited Controls" Worksheet for further details	Specify the NIST SP 800-53 Revision 4 unique control identifier for the controls selected for testing based on the rationale defined in Worksheet 4: Inherited Controls.

3.3.1.2 WORKSHEET 2: CONDITIONAL CONTROLS

The Conditional Controls worksheet lists the FedRAMP NIST SP 800-53 Revision 4 controls that all CSPs are required to consider for testing. The 3PAO performs an analysis to determine whether all the requirements in the control have been tested as part of the assessment completed for the initial P-ATO or ATO or tested within the required timeframes specified in the *ConMon Guide*. The 3PAO provides a description of the analysis performed and provides the artifacts that support the analysis, as described in Table 3 below.

Table 3. FedRAMP Rev3 to Rev4 Annual Assessment Controls – Conditional Controls Column Content Description

Column Header	Content Description
Column A - Item	This is the item number of the control all CSPs are required to consider for testing.
Column B – Control ID	This is the NIST SP 800-53 Revision 4 unique control identifier for the control all CSPs are required to consider for testing.
Column C - Condition	This column specifies some criteria (conditions) to assist in determining whether the control is required to be included for testing in this assessment.

Column Header	Content Description
<p>Column D - Answers (Yes/No) - A "Yes" answer indicates that the control was tested.</p>	<p>This column indicates the results of the analysis performed by the 3PAO based on the criteria (conditions) provided in Column C and a complete analysis of all the requirements specified in the control. Specify "Yes" in this column if the control has been tested as part of the assessment completed for the initial P-ATO or ATO or within the required timeframes specified in the <i>ConMon Guide</i>. Specify "No" in this column if the answer to any of the criteria (conditions) or any control requirements have not been tested as required.</p>
<p>Column E - Analysis - Describe how the 3PAO determined that the control was previously assessed (E.g. "Reviewed ABC.doc section 1.2.3 and XYZ_2-4-2013.xls Row 100")</p>	<p>If "Yes" is specified in Column D, fully describe the analysis performed by the 3PAO that supports a determination that the control has been as part of the assessment completed for the initial P-ATO or ATO or tested within the required timeframes specified in the <i>ConMon Guide</i>. Include a description of all artifacts that support the analysis and provide the artifacts as applicable.</p>

3.3.1.3 WORKSHEET 3: CSP-SPECIFIC CONTROLS

The CSP-Specific worksheet is a list of controls selected by the CSP for testing in this assessment based on CSP implementations and continuous monitoring activities, as described in Table 4 below.

Table 4. FedRAMP Rev3 to Rev4 Annual Assessment Controls – CSP-Specific Controls Column Content Description

Column Header	Content Description
<p>Column A - Item</p>	<p>This is the item number of the control selected for testing by the CSP.</p>
<p>Column B – Control ID</p>	<p>This is the NIST SP 800-53 Revision 4 unique control identifier for the control selected for testing by the CSP.</p>
<p>Column C - Indicate Rationale: POA&M Closure, DR, System Change, Periodic Testing Requirement, Selected by CSP</p>	<p>Specify the rationale for selecting this control for testing in this assessment. Indicate one of the following rationale and provide applicable descriptive information:</p> <ul style="list-style-type: none"> • POA&M closure. • DR (Deviation Request). • System Change. • Periodic Testing Requirement – Testing required as specified in the <i>ConMon Guide</i>. Specify applicable requirement. • Selected by CSP – Controls selected by CSP for testing in this assessment. Specify rationale for selection.

3.3.1.4 WORKSHEET 4: INHERITED CONTROLS

The Inherited Controls worksheet lists controls that the CSP fully or partially inherited from a leveraged FedRAMP compliant PaaS or IaaS service provider, as described in Table 5 below.

Table 5. FedRAMP Rev3 to Rev4 Annual Assessment Controls – CSP Inherited Controls Column Content Description

Column Header	Content Description
Column A - Item	This is the item number of the control that is fully or partially inherited from a leveraged FedRAMP compliant PaaS or IaaS service provider.
Column B – Control ID	This is the NIST SP 800-53 Revision 4 unique control identifier for the control that is fully or partially inherited from a leveraged FedRAMP compliant PaaS or IaaS service provider.
Column C - Inherited Control - Indicate NIST SP 800-53 Revision 3/ NIST SP 800-53 Revision 4	Specify if the inherited control is a FedRAMP NIST SP 800-53, Revision 3, control or a FedRAMP NIST SP 800-53, Revision 4, control.
Column D – Inherited Control – Rev3 to Rev4 Transition (Yes/No)	Specify whether the inherited control is required for testing as part of the FedRAMP Rev3 to Rev4 transition. Indicate “Yes” or “No.”
Column E - Indicate Partially/Fully Inherited	Specify if the control requirements are fully inherited or partially inherited.
Column F - Required for Testing in this Assessment (Yes/No)	<p>If the control is partially inherited and the results of Column D indicate “Yes,” the CSP is required to include the control in this assessment for testing of those portions of the control that are provided by the CSP.</p> <p>If the control is partially inherited and results of Column D indicate “No,” the CSP determines whether the control is required for testing based on the CSP-Specific rationale defined in Worksheet 3.</p>

3.4 COMPLETE SECURITY ASSESSMENT

CSPs perform a FedRAMP Revision 4 Transition security assessment using the same processes and procedures as performing a FedRAMP annual assessment. The scope of the assessment will be based on the results of the control selection process, 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 *ConMon Guide*.

3.4.1 SECURITY ASSESSMENT PLAN (SAP)

The 3PAO prepares and submits the Security Assessment Plan (SAP) utilizing the *Security Assessment Plan Template for Annual Assessments*. 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 modification to address CSP-specific implementations as described in the SSP and other supporting documentation.

3.4.2 SECURITY ASSESSMENT REPORT (SAR)

The 3PAO prepares and submits the Security Assessment Report (SAR) utilizing the *Annual Security Assessment Report Template*. 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 inherited controls from leveraged PaaS and IaaS systems as applicable.

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

The JAB and/or AO determine whether the overall risk posture of the system, as defined in the SAR, is acceptable.

3.4.2.1 SECURITY ASSESSMENT TEST CASES

The 3PAO prepares and submits the *FedRAMP Security Assessment Test Cases* 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.

The 3PAO completes the observations and evidence, implementation status, findings, and risk exposure information.

3.4.2.1.1 WORKSHEET 1: SYSTEM

This System worksheet provides system and CSP general information, as described in Table 6 below.

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

Column A	Column B
System	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).

3.4.2.1.2 WORKSHEET 2: CTRLSUMMARY

The CtrlSummary worksheet provides the test results summary of all the test cases, as described in Table 7 below.

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

Column Header	Content Description
Column A - ID	This is the NIST SP 800-53 Revision 4 unique control identifier.
Column B – CONTROL TITLE (NIST SP 800-53 Rev4)	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 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 the 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].

3.4.2.1.3 WORKSHEETS 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, as described in Table 8 below.

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

Column Header	Content Description
Column A - ID	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 Header	Content Description
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, 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 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 – Findings	Specify the status of the control at the completion of testing [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 – Prior Findings	Specify the status of a prior finding associated with this control. [satisfied/other than satisfied].
Column Q – Prior Risk	Specify the risk exposure to the system if the vulnerability associated with this control is exploited. [high/moderate/low].

3.5 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.

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

4. METHODOLOGY FOR MANAGING RISKS ASSOCIATED WITH INHERITED CONTROLS

4.1 METHODOLOGY FOR TESTING INHERITED CONTROLS

The methodology for testing controls inherited from a FedRAMP compliant PaaS or IaaS service (Leveraged CSP) is explicitly based on how the requirement is described in the SSP.

The SSP for the CSP leveraging another (leveraged) cloud system clearly defines the roles and responsibilities for each and every control requirement. For example, a Physical and Environmental (PE) control might be fully inherited from the Leveraged cloud system. The CSP describes “how” the PE control requirement is implemented by stating it is fully inherited from the leveraged cloud system. There is a subsection in the control implementation description that states “what” the leveraged CSP or cloud system is providing to meet the requirement but not “how” the leveraged cloud system meets the requirement. The leveraged cloud system’s SSP will describe “how” the control is implemented.

In another example, a control requirement might be a “shared” control, where the CSP and the leveraged CSP implement portions of a requirement in order to meet the entire 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” provided by the leveraged CSP is described. However, the description of “how” the leveraged CSP implements their portion of the control would be found in the leveraged CSP SSP.

The scope of testing for the CSP leveraging a FedRAMP compliant leveraged CSP includes only control requirements that the CSP is responsible for implementing. The 3PAO tests only the control requirements implemented by the CSP and assumes that the leveraged cloud 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 cloud system. If the leveraged cloud system provides a service such as auditing/logging or trouble ticketing, the 3PAO must collect evidence from only the CSP that the leveraged cloud system is providing those services (e.g., audit logs/reports).

4.2 METHODOLOGY FOR REPORTING AND MANAGING RISKS ASSOCIATED WITH INHERITED CONTROLS

The 3PAO may have identified some known risks associated with the PaaS or IaaS system leveraged by the 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 be due to 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 4, baseline requirements.

The 3PAO must include these known risks in the SAR and the CSP must to include these known risks in the POA&M 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 leveraged CSP to determine the status of remediation of those risks at least every 30 days and/or provides evidence of the leveraged system’s timeline for remediation.

Consider the following example: The IaaS CSP has only implemented FedRAMP NIST SP 800-53, Revision 3 requirements. The Software-as-a-Service (SaaS) leveraging the IaaS implements FedRAMP NIST SP 800-53, Revision 4. During the assessment of the SaaS, the 3PAO

identified the leveraged IaaS controls do not meet FedRAMP NIST SP 800-53, Revision 4. To be compliant, the SaaS CSP must have the following:

- 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.

5. GENERAL REQUIREMENTS

- Use latest version for all FedRAMP document templates, such as SSP, SAP, SAR and Contingency Plan.
- Ensure that all transition requirements are addressed and documented completely. Identify specifically what was included in the scope of the transition 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 testing 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 ISSO and JAB technical reviews.
- Ensure that all findings are included in the SAR and POA&M.

6. CONTROL SELECTION WORKBOOK

The *FedRAMP Rev4 Annual Assessment Controls* workbook may be found on the following FedRAMP website page: <https://www.fedramp.gov/resources/templates-3/>.

7. FEDRAMP REVISION 4 TEST CASES

The *FedRAMP Revision 4 Test Cases v 1.0* workbook may be found on the following FedRAMP website page: <https://www.fedramp.gov/resources/templates-3/>.

Appendix A – FedRAMP Acronyms

Acronym	Description
3PAO	Third Party Assessment Organization
AO	Authorizing Official
<i>ConMon Guide</i>	<i>FedRAMP Continuous Monitoring and Strategy Guide</i>
CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
IaaS	Infrastructure-as-a-Service
JAB	Joint Authorization Board
NIST	National Institute of Standards and Technology
PaaS	Platform-as-a-Service
PE	Physical Environment
PMO	Program Management Office
Rev3	Revision 3
Rev4	Revision 4
SaaS	Software-as-a-Service
SAP	Security Assessment Plan
SAR	Security Assessment Report
SSP	System Security Plan