FedRAMP™

FedRAMP Baseline Revision 5 Transition Plan

Transition to the FedRAMP Baselines based on NIST SP 800-53 Revision 5

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 (SP) 800-53 (SP 800-53), Security and Privacy Controls for Federal Information Systems and Organizations, Revision 5 (Rev. 5). The FedRAMP Program Management Office (PMO) updated the FedRAMP baseline security controls, documentation, and templates to reflect the changes in NIST SP 800-53, Rev. 5. 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 Rev. 5, and to the new FedRAMP requirements.

Document Revision History

Date	Version	Page(s)	Description	Author
5/30/2023	1.0	All	Transition Guide - Major revision for SP 800-53 Revision 5, includes new baselines, test cases and guidance on completing security assessments and reporting	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.

Introduction

NIST released SP 800-53 Rev. 5 in September 2020 (and updated on December 10, 2020). This document provides guidance, references updated documentation, and clarifies the transition timelines and the FedRAMP's expectations for migration to the FedRAMP baselines based on NIST SP 800-53 Rev. 5.

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, Rev. 5. In addition, it defines the required deadlines for transitioning from Revision 4 (Rev. 4) to Rev. 5.

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.

Scope

The scope of this document is to provide guidance specifically related to completing the transition from compliance with FedRAMP security requirements based on NIST SP 800-53, Rev. 4, to FedRAMP security requirements based on NIST SP 80-53, Rev. 5. The scope of the guidance is to assist CSPs, Federal Agencies, and 3PAOs/Assessors, based on the following assumptions:

- The CSP is currently compliant with, or working towards compliance with, FedRAMP based on NIST SP 800-53, Rev. 4.
- CSPs providing IaaS services will be transitioning all services and components included in the boundary for authorization for NIST SP 80-53, Rev. 5 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, Rev. 5, compliant.

FedRAMP Baseline Rev. 5 Transition Schedule

The Rev. 5 transition strategy went into effect May 30, 2023.

The requirements and timeline for CSPs to transition to the FedRAMP Rev. 5 baseline and templates depend on the CSP's current FedRAMP authorization phase. In order to determine a CSP's proper timeline, please first determine which phase the CSP is currently in using the guidance below:

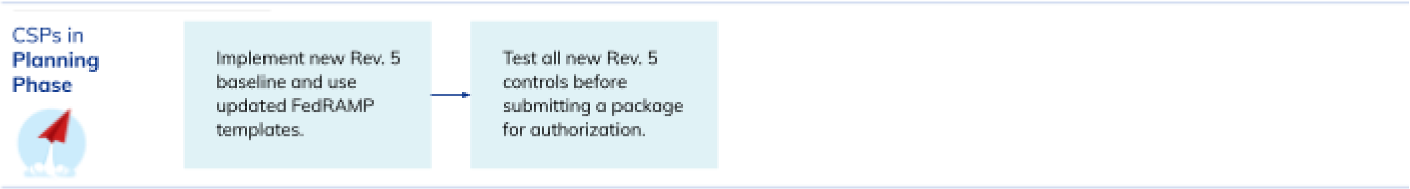
PLANNING

CSPs are in the "Planning" phase and will implement and have an assessor test the new Rev. 5 baseline and use the updated FedRAMP templates prior to submitting a package for authorization if **any** of the below applies:

- CSPs that are applying to FedRAMP or are in the readiness review process.
- CSPs that have not partnered with a federal agency (i.e., the Agency AO has not submitted a formal In Process Request to the PMO) prior to **May 30, 2023**.
- CSPs that have not contracted with a 3PAO for a Rev. 4 assessment prior to **May 30, 2023**.
- CSPs with a JAB prioritization that have not begun an assessment after release of the Rev. 5 baseline and templates.

CSPs in the planning phase will:

- Implement new Rev. 5 baseline and use updated FedRAMP templates.
- Test all new Rev. 5 controls before submitting a package for authorization.



CSPs in **Planning Phase**

Implement new Rev. 5 baseline and use updated FedRAMP templates.

Test all new Rev. 5 controls before submitting a package for authorization.

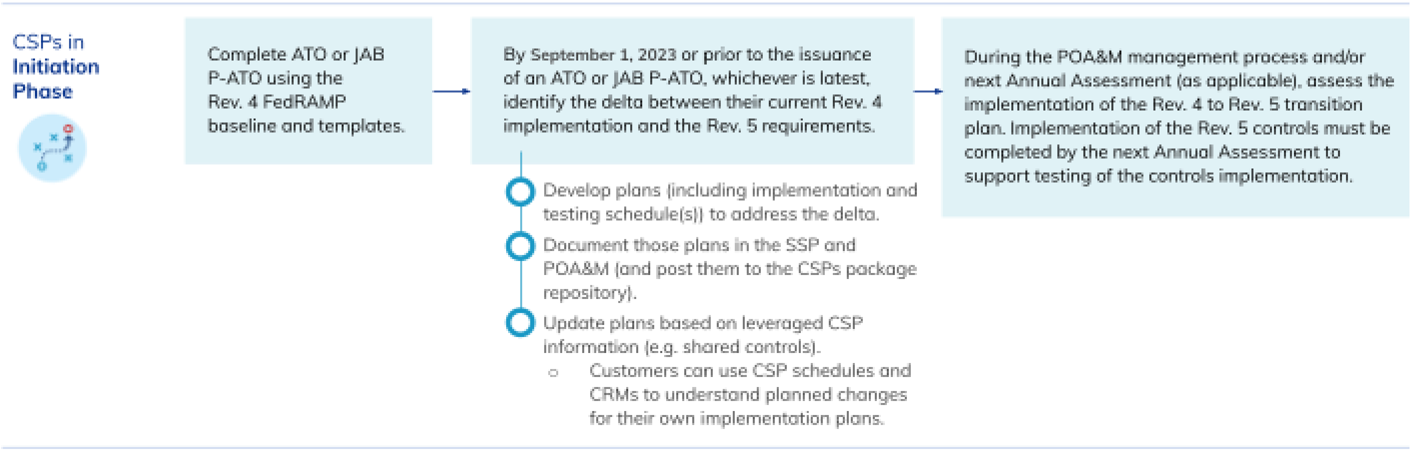
INITIATION

CSPs are in the “Initiation” phase if **any** of the below applies:

- CSPs that are currently prioritized for the JAB and are currently under contract with a 3PAO or in 3PAO assessment, have been assessed and are working toward P-ATO package submission, or have kicked off the JAB P-ATO review process prior to **May 30, 2023**.
- CSPs who have partnered with a federal agency and are currently under contract with a 3PAO, are undergoing a 3PAO assessment, or have been assessed and have submitted the package for Agency ATO review prior to **May 30, 2023**.

CSPs in the initiation phases will:

- Complete ATO or JAB P-ATO using the Rev. 4 FedRAMP baseline and templates.
- By **September 1, 2023** or prior to the issuance of an ATO or JAB P-ATO, whichever is latest, identify the delta between their current Rev. 4 implementation and the Rev. 5 requirements.
    - Develop plans (including implementation and testing schedule(s)) to address the delta.
    - Document those plans in the SSP and POA&M (and post them to the CSP’s package repository).
    - Update plans based on leveraged CSP information (e.g. shared controls).
        - Customers can use CSP schedules and CRMs to understand planned changes for their own implementation plans.
- During the POA&M management process and/or next Annual Assessment (as applicable), assess the implementation of the Rev. 4 to Rev. 5 transition plan. Implementation of the Rev. 5 controls must be completed by the next Annual Assessment to support testing of the controls implementation.



CSPs in Initiation Phase

Complete ATO or JAB P-ATO using the Rev. 4 FedRAMP baseline and templates.

By September 1, 2023 or prior to the issuance of an ATO or JAB P-ATO, whichever is latest, identify the delta between their current Rev. 4 implementation and the Rev. 5 requirements.

- Develop plans (including implementation and testing schedule(s)) to address the delta.
- Document those plans in the SSP and POA&M (and post them to the CSPs package repository).
- Update plans based on leveraged CSP information (e.g. shared controls).
    - Customers can use CSP schedules and CRMs to understand planned changes for their own implementation plans.

During the POA&M management process and/or next Annual Assessment (as applicable), assess the implementation of the Rev. 4 to Rev. 5 transition plan. Implementation of the Rev. 5 controls must be completed by the next Annual Assessment to support testing of the controls implementation.

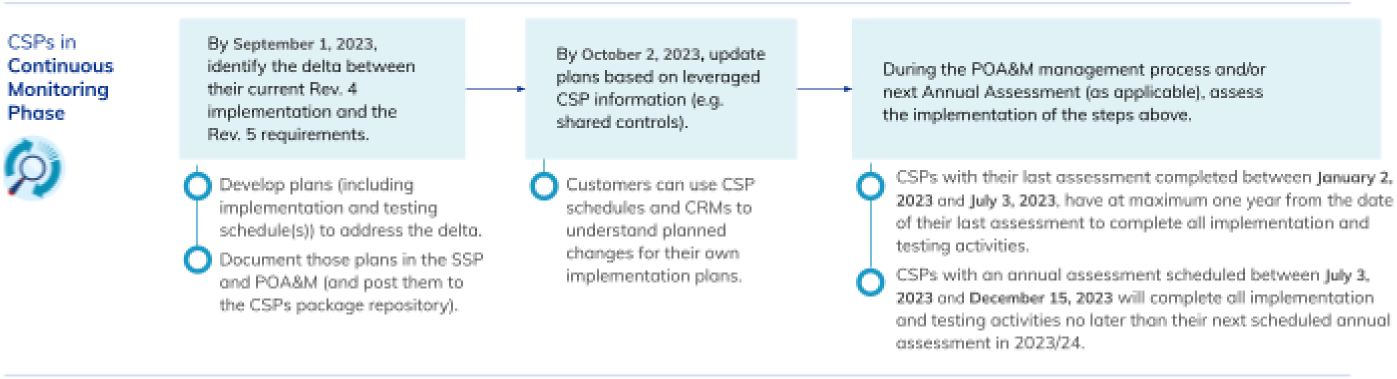
CONTINUOUS MONITORING

CSPs are in the “Continuous Monitoring” phase if **any** of the below applies:

- CSPs who are in continuous monitoring with a current FedRAMP authorization.

CSPs in the continuous monitoring phase will:

- By **September 1, 2023**, identify the delta between their current Rev. 4 implementation and the Rev. 5 requirements.
  - Develop plans (including implementation and testing schedule(s)) to address the delta.
  - Document those plans in the SSP and POA&M (and post them to the CSP’s package repository).
- By **October 2, 2023**, update plans based on leveraged CSP information (e.g. shared controls).
  - Customers can use CSP schedules and CRMs to understand planned changes for their own implementation plans.
- During the POA&M management process and/or next Annual Assessment (as applicable), assess the implementation of the steps above.
  - CSPs with their last assessment completed between **January 2, 2023** and **July 3, 2023**, have at maximum one year from the date of their last assessment to complete all implementation and testing activities.
  - CSPs with an annual assessment scheduled between **July 3, 2023** and **December 15, 2023** will complete all implementation and testing activities no later than their next scheduled annual assessment in 2023/24.


CSPs in Continuous Monitoring Phase

By September 1, 2023, identify the delta between their current Rev. 4 implementation and the Rev. 5 requirements.

Develop plans (including implementation and testing schedule(s)) to address the delta.

Document those plans in the SSP and POA&M (and post them to the CSPs package repository).

By October 2, 2023, update plans based on leveraged CSP information (e.g. shared controls).

Customers can use CSP schedules and CRMs to understand planned changes for their own implementation plans.

During the POA&M management process and/or next Annual Assessment (as applicable), assess the implementation of the steps above.

CSPs with their last assessment completed between January 2, 2023 and July 3, 2023, have at maximum one year from the date of their last assessment to complete all implementation and testing activities.

CSPs with an annual assessment scheduled between July 3, 2023 and December 15, 2023 will complete all implementation and testing activities no later than their next scheduled annual assessment in 2023/24.

Timeline for CSPs

CSPs in Planning Phase

Implement new Rev. 5 baseline and use updated FedRAMP templates.

→ Test all new Rev. 5 controls before submitting a package for authorization.

CSPs in Initiation Phase

Complete ATO or JAB P-ATO using the Rev. 4 FedRAMP baseline and templates.

→ By **September 1, 2023** or prior to the issuance of an ATO or JAB P-ATO, whichever is latest, identify the delta between their current Rev. 4 implementation and the Rev. 5 requirements.

- Develop plans (including implementation and testing schedule(s)) to address the delta.
- Document those plans in the SSP and POA&M (and post them to the CSPs package repository).
- Update plans based on leveraged CSP information (e.g. shared controls)
  - Customers can use CSP schedules and CRMs to understand planned changes for their own implementation plans.

→ During the POA&M management process and/or next Annual Assessment (as applicable), assess the implementation of the Rev. 4 to Rev. 5 transition plan. Implementation of the Rev. 5 controls must be completed by the next Annual Assessment to support testing of the controls implementation.

CSPs in Continuous Monitoring Phase

By **September 1, 2023**, identify the delta between their current Rev. 4 implementation and the Rev. 5 requirements.

- Develop plans (including implementation and testing schedule(s)) to address the delta.
- Document those plans in the SSP and POA&M (and post them to the CSPs package repository).

→ By **October 2, 2023**, update plans based on leveraged CSP information (e.g. shared controls).

- Customers can use CSP schedules and CRMs to understand planned changes for their own implementation plans.

→ During the POA&M management process and/or next Annual Assessment (as applicable), assess the implementation of the steps above.

- CSPs with their last assessment completed between **January 2, 2023** and **July 3, 2023**, have at maximum one year from the date of their last assessment to complete all implementation and testing activities.
- CSPs with an annual assessment scheduled between **July 3, 2023** and **December 15, 2023** will complete all implementation and testing activities no later than their next scheduled annual assessment in 2023/24.

Tasks Required to Complete the Transition

Develop Schedule

The CSP, with assistance from their assessor, will develop a schedule that shows their planned transition from Rev. 4 to Rev. 5. Major milestone activities for a schedule to complete the transition include the following:

- CSP: Complete new Rev. 5 System Security Plan (SSP) and attachments.
- Assessor: Complete the *Security Assessment Plan (SAP) Template*. This template is available on this FedRAMP website page: https://www.fedramp.gov/documents-templates/.
- CSP/Assessor: Submit SSP and SAP to FedRAMP JAB POC or Agency Authorizing Official (AO) for approval.
- Assessor: Conduct testing.
- Assessor: Complete the *Security Assessment Report (SAR) Template*. This template is available on this FedRAMP website page: https://www.fedramp.gov/documents-templates/.
- CSP/Assessor: Submit SAR, POA&M, attachments, and updated SSP to FedRAMP JAB POC or Agency AO.

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

Update Documentation to FedRAMP Rev. 5 Templates

The FedRAMP PMO has published updated templates for the SSP and attachments. CSPs must complete an entirely new authorization package based on the updated templates (see https://www.fedramp.gov/documents-templates/ for updated templates).

Determine Scope of Assessment

The scope of the assessment is based on determining the specific FedRAMP NIST SP 800-53 Rev. 5 controls that require testing by the assessor. All new or modified requirements introduced in Rev. 5 must be tested and other control testing may need to be required based on CSP-specific implementations and continuous monitoring activities.

Control Selection Process

CSPs will utilize the appropriate *FedRAMP Rev. 4 to Rev. 5 Assessment Controls Selection Template* (High, Moderate or Low) to determine which controls are in scope for testing. The template is an Excel Workbook containing four worksheets: the Rev. 5 List of Controls 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 Rev. 5 controls have been addressed.

Worksheet 1: Rev. 5 List of Controls

The Rev. 5 List of Controls worksheet has two sections. The top section of the worksheet documents basic system information described in Table 1 below:

Table 1. ***FedRAMP CSP Rev. 4 to Rev. 5 Controls Selection Worksheet 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 Rev. 5 List of Controls worksheet is the list of all controls identified for testing for this assessment and contains the information in Table 2 below:

Table 2. ***FedRAMP-Selected List of Core Controls - Column Content Description***

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 Rev. 5 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 *Continuous Monitoring Strategy Guide* that are required to be tested by all CSPs.
Column D - New	This column indicates the additional new FedRAMP NIST SP 800-53 Rev. 5 baseline controls that all CSPs are required to test.
Column E - Conditional- Refer to "Conditional Controls" Worksheet for further details	Ths 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. Columns A and B must be appended to include these additional NIST SP 800-53 Rev. 5 unique control identifiers.

Column Header	Content Description
Columns F, G - Divider	These columns divide 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 H - Item No.	This is the item number of the control selected for testing based on CSP-specific implementations and continuous monitoring activities.
Column I - Control ID - CSP-Specific-Refer to "CSP-Specific Controls" Worksheet for further details	Specify the NIST SP 800-53 Rev. 5 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 Rev. 5 unique control identifier for the controls selected for testing based on the rationale defined in Worksheet 4: Inherited Controls.
Column K - Comments	Provide any necessary comments related to the control.
Column L - 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 M - Total Number of Controls Selected for This Assessment	This column indicates the total number of controls in the assessment.

Worksheet 2: Conditional Controls

The Conditional Controls worksheet lists the FedRAMP NIST SP 800-53 Rev. 5 controls that all CSPs are required to consider for testing. The 3PAO performs an analysis to determine whether all the requirements in the Rev. 5 control have been tested as part of the Rev. 4 assessment completed for the initial P-ATO or ATO or tested within the required timeframes specified in the *Continuous Monitoring Strategy 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 Rev. 4 to Rev. 5 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 Header	Content Description
Column B - Control ID	This is the NIST SP 800-53 Rev. 5 unique control identifier for the control all CSPs are required to consider for testing.
Column C - Change	This column specifies criteria (control changes) to assist in determining whether the control is required to be included for testing in this assessment or whether previous testing activities are sufficient.
Column D - Answers (Yes/No) - **A "Yes" answer indicates that the control was tested.**	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 *Continuous Monitoring Strategy Guide*. Specify "No" in this column if the answer to any of the criteria (conditions) or any control requirements have not been tested as required.
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_2-4-2021.xls Row 100")	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 *Continuous Monitoring Strategy Guide*. Include a description of all artifacts that support the analysis and provide the artifacts as applicable.

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 Rev. 4 to Rev. 5 Assessment Controls – CSP-Specific Controls Column Content Description***

Column Header	Content Description
Column A - Item	This is the item number of the control selected for testing by the CSP.
Column B - Control ID	This is the NIST SP 800-53 Rev. 5 unique control identifier for the control selected for testing by the CSP.

Column Header	Content Description
Column C - Indicate Rationale: POA&M Closure, DR, System Change, Periodic Testing Requirement, Selected by CSP	Specify the rationale for selecting this control for testing in this assessment. Indicate one of the following rationale and provide applicable descriptive information: • POA&M closure. • DR (Deviation Request). • System Change. • Periodic Testing Requirement – Testing required as specified in the *Continuous Monitoring Strategy Guide*. Specify applicable requirements. • Selected by CSP – Controls selected by CSP for testing in this assessment. Specify rationale for selection.

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 Rev. 4 to Rev. 5 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 Rev. 5 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 Rev. 4/ NIST SP 800-53 Rev. 5	Specify if the inherited control is a FedRAMP NIST SP 800-53, Rev. 4, control or a FedRAMP NIST SP 800-53, Rev. 5, control.
Column D - Inherited Control – Rev. 4 to Rev. 5 Transition (Yes/No)	Specify whether the inherited control is required for testing as part of the FedRAMP Rev. 4 to Rev. 5 transition. Indicate "Yes" or "No."
Column E - Indicate Partially/Fully Inherited	Specify if the control requirements are fully inherited or partially inherited.

Column Header	Content Description
Column F - Required for Testing in this Assessment (Yes/No)	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. 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.

Complete Security Assessment

Assessors perform a FedRAMP Rev. 5 Transition security assessment using the same processes and procedures as performing a FedRAMP assessment. The scope of the assessment will be based on the results of the control selection process, the testing will utilize the FedRAMP Rev. 5 Test Cases (Refer to Section 6, FedRAMP Rev. 5 Test Cases) and the requirements specified in the *Continuous Monitoring Strategy Guide*.

Security Assessment Plan (SAP)

The Assessor prepares and submits the Security Assessment Plan (SAP) utilizing the *Security Assessment Plan Template*. 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.

Security Assessment Report (SAR)

The Assessor prepares and submits the Security Assessment Report (SAR) utilizing the *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.

Security Assessment Test Cases

The Assessor 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, Rev. 5, control requirements with associated required test methods.

The Assessor completes the observations and evidence, implementation status, findings, and risk exposure information. Worksheet 1 “Instructions” of the Test Case Workbook provides detailed instructions for the documentation of 3PAO assessment test results.

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.

Methodology for Managing Risks Associated with Inherited Controls

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 authorized 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 Assessor must collect evidence from only the CSP that the leveraged cloud system is providing those services (e.g., audit logs/reports).

Methodology for Reporting and Managing Risks Associated with Inherited Controls

The Assessor 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, Rev. 5, baseline requirements.

The Assessor must include these known risks in the SAR and the CSP must 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, Rev. 4 requirements. The SaaS leveraging the IaaS implements FedRAMP NIST SP 800-53, Rev. 5. During the assessment of the SaaS, the 3PAO identified the leveraged IaaS controls do not meet FedRAMP NIST SP 800-53, Rev. 5. To be compliant, the SaaS CSP must have the following:

- A SAR that identifies the gaps in the inherited controls (gaps from Rev. 4 to Rev. 5).
- 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, Rev. 5 requirements and has fully and successfully tested the implementation of these controls.

General Requirements

- Use the latest version for all FedRAMP document templates, such as SSP, SAP, SAR, POA&M, 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 the anniversary date of the P-ATO or ATO.
- Develop and implement a schedule that provides for revisions and updates to draft documents based on JAB POC or Agency AO technical reviews.
- Ensure that all findings are included in the SAR and POA&M.

Control Selection Workbook

The *FedRAMP Rev. 4 to Rev. 5 Assessment Controls Selection Template* workbook may be found on the following FedRAMP website page: https://www.fedramp.gov/documents-templates/.

FedRAMP Rev. 5 Test Cases

The *FedRAMP Rev. 5 Test Cases* workbook may be found on the following FedRAMP website page: https://www.fedramp.gov/documents-templates/.

FedRAMP Rev. 5 Updates, Contract Language and Information

All updated FedRAMP documents and templates are available at https://FedRAMP.gov.

Send questions to: Info@FedRAMP.gov.

NOTE: CSPs can transition to the new FedRAMP Rev. 5 baseline and templates sooner than the timelines provided in this guidance document. Agencies must issue contract language requiring CSPs to comply with FedRAMP security authorization requirements in accordance with the Office of Management and Budget FedRAMP memo dated Dec 8, 2011.

Frequently Asked Questions

When will the last Rev. 4 testing be accepted for an authorization package submitted for FedRAMP review?

- For CSPs in the Planning Phase the last Rev. 4 testing that will be accepted as part of an authorization package submission is May 30, 2023.
- For CSPs in the Initiation Phase, the last Rev. 4 testing that will be accepted as part of an authorization package submission is based on the 3PAO SAR testing date. For example, a CSP currently under contract for a 3PAO to perform SAR testing in May 2023 may submit an ATO/P-ATO package for FedRAMP review in August or September 2023. Therefore, the last Rev. 4 testing that will be accepted as part of an authorization package submission would be August or September 2023 for that CSP.
- For CSPs in the Continuous Monitoring Phase, the last Rev. 4 testing that will be accepted as part of an annual assessment package submission is December 2023.

We leverage an IaaS or PaaS, are we responsible for the Rev. 5 transition of controls that we inherit?

- CSPs are responsible for the customer defined responsibilities of those Rev. 5 controls once the IaaS or PaaS has implemented the applicable Rev. 5 control. Please see section “Methodology for Reporting and Managing Risks Associated with Inherited Controls” for detailed requirements.

My AO has stated that we must transition to Rev. 5 earlier than the transition date that FedRAMP requires. Which date should we follow?

- CSPs should follow whichever Rev. 5 transition date is earliest between the AO and FedRAMP transition guide requirements.

My AO requires additional Rev. 5 controls not specified in the FedRAMP Rev. 5 baseline. How do those controls fit into the transition time frame?

- CSPs should work with their AO to determine if there is an Agency specific transition requirement for the additional controls. CSPs should follow the transition guidance within this document if there are no specific Agency transition requirements.

When should I start working with my assessor to test our Rev. 5 implementation?

- While assessor engagement is up to the CSP, we suggest engaging with your assessor as soon as possible to ensure that CSPs are able to work through the timing and scope with their assessor to avoid potential delays due to scheduling or other issues.

What is a Rev. 5 “conditional control” and do we need to test them?

- Conditional controls are controls where the delta between the Rev. 4 and Rev. 5 versions are small and may have been tested during the Rev. 4 testing. If the different “conditions” were tested as part of the Rev. 4 testing and the testing data and analysis supporting that the applicable testing was performed is available then additional testing is not required.

What should I do if my system has unique circumstances and my situation does not match the phases defined above for any reason?

- Please work with your Authorizing Official to discuss your unique circumstances and determine a path forward.