

FedRAMP Detailed Review
Standard Operating Procedure



FedRAMP

Version 1.1

August 27, 2015

Revision History

Date	Version	Page(s)	Description	Author
08/14/2015	1.0	All	Initial Release	FedRAMP PMO
08/27/2015	1.1	All	Remove all links to version-specific documents and replace with non-version-specific links to the website pages where the documents are found.	FedRAMP PMO

How to Contact Us

For questions about FedRAMP or this document, email to info@fedramp.gov.

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

Table of Contents

1. Introduction.....	1
1.1. Purpose.....	1
1.2. Scope.....	1
1.3. Roles and Responsibilities.....	2
1.4. Coordination Among Organizational Entities	2
1.5. Compliance	2
1.6. Prerequisites.....	3
1.7. Detailed Security Documents Review	3
2. Phase One: SSP Detailed Review	5
3. Phase Two: SAP Review	9
4. Phase Three: SAR Review	11
5. Phase Four: POA&M Review.....	14
6. Prepare Review Results	15
7. Referenced FedRAMP Documents.....	16
8. Document Locations	17
Appendix A: Table of Acronyms.....	19
Appendix B: Required Authorization Package Documents.....	20

List of Tables

Table 1. PMO Roles and Responsibilities	2
Table 2. Roles and Responsibilities by Document	3
Table 3. Detailed Review Results Actions	15
Table 4. Authorization Package Documents and Attachments	20

1. INTRODUCTION

The Federal Risk and Authorization Management Program (FedRAMP) provides a cost-effective, risk-based approach for the adoption and use of cloud services by providing a repository of Authorization Packages for cloud services that are adaptable and reusable by Federal Agencies. The objective is to authorize a cloud service system once and reuse that authorization many times. For more information about FedRAMP, see the *Guide to Understanding FedRAMP*. See Section 0 for the location of referenced documents.

To obtain FedRAMP compliance, an Applicant must submit an Authorization Package for FedRAMP review and approval. Applicants are primarily Cloud Service Providers (CSPs) and Federal Agencies. Some documents are received directly from a Third-Party Assessment Organization (3PAO) contracted by a CSP. An Authorization Package contains the body of evidence needed by authorizing officials to make risk-based decisions regarding the information systems providing cloud services. The Applicant may submit these documents all at once or incrementally in order of completion or review, depending on the path and review level. Some documents may be updated and resubmitted throughout the FedRAMP review and approval process.

This SOP is part of a larger SOP, the *FedRAMP Review and Approve Process* (see Section 0), which describes the entire Authorization Package Review and Approve process executed by the FedRAMP PMO. This Detailed Review SOP describes the process of reviewing the Authorization Package documents submitted by CSPs applying for a FedRAMP Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO). The reviews are completed by the FedRAMP Information System Security Officer (ISSO) assigned to the review process for the CSP.

1.1. PURPOSE

Detailed Reviews determine whether the CSP is in compliance with the Information Technology (IT) security requirements defined by the Federal Information Security Management Act (FISMA), National Institutes of Standard and Technology (NIST) Special Publications (SP) 800-53 Revision 4, and FedRAMP. The Detailed Review determines if the Authorization Package documentation demonstrates the CSP's implementation of security controls.

To be listed as FedRAMP Compliant for JAB P-ATO Packages on the FedRAMP website (fedramp.gov), a CSP must pass the FedRAMP Detailed Review of the System Security Plan (SSP) and attachments, Security Assessment Plan (SAP), Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M). The successful completion of this Detailed Review signifies that the FedRAMP ISSO believes the documentation provided by a CSP meets the minimum security and quality standards in order to be submitted to the JAB for a P-ATO.

Documents that are incomplete or contain insufficient information to determine that the intent of the security controls is being met by the CSP's implementation are returned to the Applicant for completion or rework and resubmission. The FedRAMP ISSO will perform a Detailed Review on reworked and resubmitted documents.

1.2. SCOPE

This SOP affects only the path to achieving FedRAMP compliance: JAB P-ATO path.

This SOP affects all Authorization Package documents including their attachments, appendices, and other associated documents regardless of whether they are submitted individually or as part of an Authorization Package.

See *Appendix B: Required Authorization Package Documents* for a complete list of documentation included in the Authorization Package for a JAB P-ATO path.

1.3. ROLES AND RESPONSIBILITIES

Table 1 below describes the roles and responsibilities of the FedRAMP PMO staff involved in this SOP.

Table 1. PMO Roles and Responsibilities

Role	Responsibilities
Lead Quality Management (QM) Reviewer	Performs Initial Completeness, Showstopper, and Readability Reviews and submits completed checklists and reviews to the Primary ISSO.
ISSO Team Lead	Assigns Primary ISSO and Secondary ISSOs for Detailed Reviews.
Primary ISSO	Project lead for assisting the CSP through the review process, the lead reviewer for all documentation and coordinator of all activities related to completion of the review process with the FedRAMP PMO, CSP, and the JAB Technical Reviewers (TR).
Secondary ISSO(s)	Perform secondary reviews of the CSP documentation as assigned by ISSO Team Lead.
Continuous Monitoring Team	Analyzes the automated scan tool results files.

1.4. COORDINATION AMONG ORGANIZATIONAL ENTITIES

The FedRAMP Cybersecurity Team (the ISSOs) is responsible for managing the overall detailed review process and performing detailed security reviews on submitted documents. FedRAMP PMO QM is responsible for performing the initial completeness, showstopper, and readability reviews and providing their reports to the Cybersecurity Team. See *FedRAMP Review and Approve Process* (see Section 0) for more information regarding their coordination.

1.5. COMPLIANCE

Documentation must address specified security requirements at a level of detail sufficient to demonstrate if the requirements have been correctly implemented and will operate as intended.

1.6. PREREQUISITES

The Lead Reviewer notifies the ISSO Team Lead via email that a CSP SSP, including attachments, has successfully completed the Initial Review process and is ready for a Detailed Review for the JAB P-ATO path. The notification includes the location of the CSP documentation and Initial Review Report in the FedRAMP Secure Repository (MAX).

The ISSO Team Lead will designate a FedRAMP ISSO as the Primary ISSO, who will coordinate reviews with the Secondary ISSOs. All ISSOs must have successfully completed the *Detailed Checklist and Review* training module (see Section 0) and have access to the following:

- The FedRAMP Secure Repository (MAX) hosted on by Office of Management and Budget (OMB) at max.gov.
- FedRAMP Review automation tool
- The current version of the *FedRAMP Writing Standards and Conventions* reference document (see Section 0).
- The current versions of the checklists described in the sections below.

1.7. DETAILED SECURITY DOCUMENTS REVIEW

Detailed Reviews are performed in four phases, based on the document associated with each phase: SSP, SAP, SAR, and POA&M. The phases may be completed sequentially or “overlapping,” with one phase beginning before the previous phase has been completed. For example, the SAP Detailed Review phase may begin immediately following JAB TR approval of the SSP or may begin while the SSP is being reviewed by the JAB TRs prior to approval. The Primary ISSO manages this phase in coordination with the CSP.

In the interest of effectiveness and efficiency, the Primary ISSO and Secondary ISSO reviews of all documents are performed in parallel as show in Table 2 below.

Table 2. Roles and Responsibilities by Document

Role	SSP Detailed Review	SAP Detailed Review	SAR Detailed Review	POA&M Detailed Review
Primary ISSO	Performs detailed review of SSP and all attachments	Performs detailed review of SAP and all attachments	Performs detailed review of SAR and all attachments	Performs detailed review of POA&M and all attachments
Secondary ISSOs	All Secondary ISSOs perform detailed reviews of a subset of controls and attachments as assigned by Primary ISSO	One Secondary ISSO will perform detailed review of the SAP and all attachments	One or more Secondary ISSOs will perform detailed reviews of the SAR and all attachments	One Secondary ISSO will perform detailed review of the POA&M and all attachments

FedRAMP Detailed Review SOP v1.1

Continu us Monitori ng Team			Performs detailed analysis of the automated scanning tool results files.	
--------------------------------------	--	--	---	--

The FedRAMP ISSO Team Lead assigns Primary and Secondary ISSO reviewers for all detailed reviews.

2. PHASE ONE: SSP DETAILED REVIEW

Review the SSP and attachments as listed in Step 1: below. The SSP is the authoritative source for the security requirement implementations and references to attachments. Specific attachment references are reviewed both as part of the implementation details in the SSP and individually as standalone documents. For example, a reference to an attachment in the SSP must be verified for correctness and applicability to the requirement and also reviewed according to a document-specific checklist. Complete the following steps in sequential order.

Primary ISSO:

Step 1: Use the appropriate review checklist templates for the SSP and all attachments as described below.

- 1) System Security Plan – *FedRAMP SSP Detailed Review Checklist Template*
- 2) Control Implementation Summary (CIS and Worksheet) – *FedRAMP CIS Detailed Checklist Template*
- 3) Configuration Management Plan – *FedRAMP CM Plan Detailed Checklist Template*
- 4) e-Authentication - *FedRAMP e-Authentication Detailed Checklist Template*
- 5) FIPS Publication 199 Categorization – *FedRAMP FIPS 199 Detailed Checklist Template*
- 6) Incident Response Plan – *FedRAMP IR Plan Detailed Checklist Template*
- 7) IT Contingency Plan – *FedRAMP IT Contingency Plan Detailed Checklist Template*
- 8) PTA-PIA – *FedRAMP PTA-PIA Detailed Checklist Template*
- 9) Rules of Behavior – *FedRAMP ROB Detailed Checklist Template*
- 10) Security Policies and Procedures – *FedRAMP Security P&P Detailed Checklist Template*
- 11) User Guide – *FedRAMP User Guide Detailed Checklist Template*
- 12) Continuous Monitoring Plan – *FedRAMP Continuous Monitoring Plan Detailed Checklist Template*

Note: These templates are prepopulated in automation tool used by the FedRAMP PMO to conduct Security Document Reviews.

Step 2: In MAX navigate to the CSP-specific folder where the document to be reviewed is stored. Do not modify the original document. Download a working copy to your local drive.

Step 3: Logon on to Google Docs and locate the *SSP Red Team Review Template* and prepare it as follows for Secondary ISSO review:

- a. Make a copy of the template in Google Docs.
- b. Rename the copy of the template as <CSP Name><System Name> Red Team Review Template.
- c. Complete the required information at the top of the first worksheet with CSP-specific information as follows:

- i. CSP Name/System Name
 - ii. Assigned ISSO Name
 - iii. Red Team Due Date
 - iv. NIST 800-53 Revision 4
 - v. Location of Files – hyperlink to file location
- d. Share the template with Secondary ISSOs and the ISSO Team Lead. The Secondary ISSO will receive automatic notification of the availability of the template for completion.

NOTE: The ISSO Team Lead will adjust Secondary ISSO assignments as necessary.

Step 4: Perform the detailed review of the SSP and all attachments in accordance with the Detailed Review Checklists, and document all comments and recommended corrective actions as follows:

- a. For SSP Detailed Review Checklist Items related to SSP Sections 1-12, complete the detailed review and provide comments in the Detailed Review Checklist Tab named 1-12. Insert or add rows as may be necessary to provide a single review comment per row.
- b. For SSP Detailed Review Checklist Items related to the SSP Minimum Security Controls (AC through SI):
 - i. Perform each of the detailed review items for each control as required in the checklist.
 - ii. Provide review comments directly within the FedRAMP Review automation tool for all controls. Insert or add an entry as may be necessary to provide a single review comment.
- c. For SSP Attachments Detailed Review Checklists, provide review comments in the applicable checklist. Insert or add an entry as may be necessary to provide a single review comment.

NOTE: The Primary ISSO may also enter review comments in a copy of the documents to assist the CSP in addressing the comments but the completed checklists are the authoritative source for all comments and responses.

Step 5: A) Perform a review of the Secondary ISSO review comments to determine whether they are additional or duplicate comments to the Primary ISSO review comments and that they are applicable to be added to the review checklist.

B) Add the Secondary ISSO review comments to the review checklists based on the results of the review in Step 8(A).

Step 6: Provide all completed Detailed Review Checklists and Detailed Review Report to the CSP by posting the documents to MAX in the CSP-specific location in the JAB In-Process folder.

Step 7: Notify the CSP that the results of the Detailed Review are available on MAX for their review and response, if necessary.

Step 8: When the SSP and all attachments are updated and/or complete, post the documentation on MAX in the CSP-Specific Ready for JAB TR Review location and provide notification to the JAB TRs that the documents are ready for their review.

Secondary ISSOs:

The Secondary ISSOs perform a comprehensive review of the documents and Primary ISSO comments to ensure they are accurate, appropriate, and complete. This review is referred to as a “Red Team Review.”

Step 1: Logon to Google Docs and locate the CSP-Specific *SSP Red Team Review Template* based on the information provided by Google Docs or the Primary ISSO.

Step 2: Determine which controls have been assigned for review.

Step 3: Logon to MAX and navigate to the CSP-Specific location as provided in the CSP-Specific Red Team Review Template.

Step 4: Navigate to the CSP-specific folder where the documents to be reviewed are stored and download a working copy of the SSP and applicable SSP attachments to your local drive.

Step 5: A) Navigate to the CSP-specific folder for the appropriate review checklist template(s) for the SSP and attachments as required for review of the ISSO-specific assigned controls:

- 1) System Security Plan – *FedRAMP SSP Detailed Review Checklist Template*
- 2) Control Implementation Summary – *CIS Attachment Checklist Template*
- 3) Configuration/Change Management – *CM Plan Attachment Checklist Template*
- 4) e-Authentication – *e-Authentication Attachment Checklist Template*
- 5) FIPS 199 Categorization – *FIPS 199 Attachment Checklist Template*
- 6) Incident Response Plan – *IR Plan Attachment Checklist Template*
- 7) IT Contingency Plan – *IT Contingency Plan Attachment Checklist Template*
- 8) PTA-PIA – *PTA-PIA Attachment Checklist Template*
- 9) Rules of Behavior – *ROB Attachment Checklist Template*
- 10) Security Policies and Procedures – *Security Policies and Procedures Attachment Checklist Template*
- 11) User Guide – *User Guide Checklist Template*
- 12) Continuous Monitoring Plan – *Continuous Monitoring Plan Checklist Template*

B) Download working copies to your local drive.

- Step 6:** Perform the Detailed Review of the applicable ISSO-specific assigned controls and applicable attachments in accordance with the Detailed Review Checklists and document all comments and recommended corrective actions in the CSP-Specific *SSP Red Team Review Template* as follows:
- a. For SSP Detailed Review Checklist Items related to SSP Sections 1-12, complete the detailed review and provide comments in the Detailed Review Checklist Tab named 1-12. Insert or add rows as may be necessary to provide a single review comment per row.
 - b. For SSP Detailed Review Checklist Items related to the SSP Minimum Security Controls (AC through SI):
 - i. Perform each of the detailed review items for each control as required in the checklist.
 - ii. Provide review comments on the SSP “Comments” Control Tab for all controls. Insert or add rows as may be necessary to provide a single review comment per row.
 - c. For SSP Attachments Detailed Review Checklists, provide review comments in the applicable checklist. Insert or add rows as may be necessary to provide a single review comment per row.
- Step 7:** Rename the completed checklists in accordance with the *FedRAMP Writing Standards and Conventions*.
- Step 8:** Upload the completed checklists in the CSP-Specific MAX folder.
- Step 9:** Notify the Primary ISSO via email that the reviews are completed.

3. PHASE TWO: SAP REVIEW

This review applies to the Detailed Review of the SAP and associated attachments and documents. Specific attachment references are reviewed both as part of the detailed review of the SAP and individually as standalone documents. For example, a reference to an attachment in the SAP must be verified for correctness and applicability to the description in the SAP and also reviewed according to a document-specific checklist items.

SAP attachments include the following:

- Security Assessment Test Cases Workbook – at least one of these will be in every SAP
- Security Assessment Test Cases for Alternative Implementations – if test cases need to be modified to test alternative implementations, a separate workbook of test cases may be provided
- Rules of Engagement
- Penetration Test Plan
- Inventory List

The SAP is the authoritative planning document for the assessment of the CSP implementation of the FedRAMP baseline security requirements as described in the SSP and attachments. The SAP is prepared and submitted by the FedRAMP Third-Party Assessment Organization (3PAO) selected by the CSP.

Complete the following steps in sequential order.

Primary ISSO:

- Step 1:** Logon to MAX and navigate to the *Quality Management Guides and Templates* folder.
- Step 2:** Select the *FedRAMP SAP Detailed Review Checklist Template*.
- Step 3:** Save a working copy of the template in the MAX CSP-specific folder with proper naming convention for the document being reviewed in accordance with the File Names Section of the *FedRAMP Writing Standards and Conventions*.
- Step 4:** Navigate to the CSP-specific folder where the *CSP-Specific FedRAMP SAP Detailed Review Checklist Template* is located and download a copy to your local drive.
- Step 5:** Navigate to the CSP-specific folder where the SAP and attachments to be reviewed are stored and download a working copy to your local drive.
- Step 6:** Review the SAP and attachments in accordance with the *CSP-Specific FedRAMP SAP Detailed Review Checklist Template* and document your comments and recommended corrective actions in the template. Insert or add rows as may be necessary to provide a single review comment per row.
- Step 7:** A) Perform a review of the Secondary ISSO review comments to determine whether they are additional or duplicate comments to the Primary ISSO review comments and that they are applicable to be added to the review checklist.

B) Add the Secondary ISSO review comments to the review checklists based on the results of the review in Step 6.

- Step 8:** Provide all completed Detailed Review Checklists and Detailed Review Report to the CSP by posting the documents to MAX in the CSP-specific location in the JAB In-Process folder.
- Step 9:** Notify the CSP that the results of the Detailed Review are available on MAX for their review and response, if necessary. The CSP is responsible for coordinating review comments with the 3PAO.
- Step 10:** When the SAP and all attachments are updated and/or complete, post the documentation on MAX in the CSP-Specific Ready for JAB TR Review location and provide notification to the JAB TRs that the documents are ready for their review.

Secondary ISSO:

- Step 1:** Navigate to the CSP-specific folder where the CSP-Specific *FedRAMP SAP Detailed Review Checklist Template* is located and download a copy to your local drive. This information is provided by the Primary ISSO.
- Step 2:** Navigate to the CSP-specific folder where the SAP and attachments to be reviewed are stored and download a working copy to your local drive.
- Step 3:** Review the SAP and attachments in accordance with the CSP-Specific *FedRAMP SAP Detailed Review Checklist Template* and document your comments and recommended corrective actions in the template. Insert or add rows as may be necessary to provide a single review comment per row.
- Step 4:** Rename the completed checklist in accordance with the *FedRAMP Writing Standards and Conventions*.
- Step 5:** Upload the completed checklist in the CSP-Specific MAX folder.
- Step 6:** Notify the Primary ISSO via email that the reviews are completed.

4. PHASE THREE: SAR REVIEW

This review applies to the Detailed Review of the SAR and associated attachments and documents. Specific attachment references are reviewed both as part of the detailed review of the SAR and individually as standalone documents. For example, a reference to an attachment in the SAR must be verified for correctness and applicability to the description in the SAR and also reviewed according to a document-specific checklist items.

SAR attachments include the following:

- Test Cases Workbook(s)
- Penetration Test Report
- Inventory Lists
- Vulnerability Scan Files
- Evidence/Artifact Files
- Table 4-1, Risk Exposure

The SAR is the authoritative document for the results of the assessment of the CSP implementation of the FedRAMP baseline security requirements as described in the SSP and attachments. The SAR is prepared submitted by the FedRAMP 3PAO selected by the CSP.

Complete the following steps in sequential order.

Primary ISSO:

- Step 1:** Logon to MAX and navigate to the *Quality Management Guides and Templates* folder.
- Step 2:** Select the *FedRAMP SAR Detailed Review Checklist Template*.
- Step 3:** Save the template in the MAX CSP-specific review folder with proper naming convention for the document being reviewed in accordance with the File Names Section of the *FedRAMP Writing Standards and Conventions*.
- Step 4:** Navigate to the CSP-specific folder where the CSP-Specific *FedRAMP SAR Detailed Review Checklist Template* is located and download a copy to your local drive.
- Step 5:** Navigate to the CSP-specific folder where the SAR and attachments to be reviewed are stored and download a working copy to your local drive.
- Step 6:** Review the SAR and attachments in accordance with the CSP-Specific *FedRAMP SAR Detailed Review Checklist Template* and document your comments and recommended corrective actions in the template. Insert or add rows as may be necessary to provide a single review comment per row.
- Step 7:**
 - A) Perform a review of the Secondary ISSO review comments to determine whether they are additional or duplicate comments to the Primary ISSO review comments and that they are applicable to be added to the review checklist.
 - B) Add the Secondary ISSO review comments to the review checklists based on the results of the review in Step 6.

- Step 8:** Perform a review of the Continuous Monitoring Team review comments and add the applicable review comments to the *FedRAMP SAR Detailed Review Checklist*.
- Step 9:** Provide all completed Detailed Review Checklists and Detailed Review Report to the CSP by posting the documents to MAX in the CSP-specific location in the JAB In-Process folder.
- Step 10:** Notify the CSP that the results of the Detailed Review are available on MAX for their review and response, if necessary. The CSP is responsible for coordinating review comments with the 3PAO.
- Step 11:** When the SAR and all attachments are updated and/or complete, post the documentation on MAX in the CSP-Specific Ready for JAB TR Review location and provide notification to the JAB TRs that the documents are ready for their review.

Secondary ISSO(s):

- Step 1:** Navigate to the CSP-specific folder where the CSP-Specific FedRAMP SAR Detailed Review Checklist Template is located and download a copy to your local drive. This information is provided by the Primary ISSO.
- Step 2:** Navigate to the CSP-specific folder where the SAR and attachments to be reviewed are stored and download a working copy to your local drive.
- Step 3:** Review the SAR and attachments in accordance with the CSP-Specific *FedRAMP SAR Detailed Review Checklist Template* and document your comments and recommended corrective actions in the template. Insert or add rows as may be necessary to provide a single review comment per row.

NOTE: If there are multiple Secondary ISSO reviewers, the ISSO Team Lead will assign specific SAR components to be reviewed by each. For example, one ISSO may review the text and another ISSO may review the test cases. Rename the completed checklist in accordance with the *FedRAMP Writing Standards and Conventions*.

- Step 1:** Upload the completed checklist in the CSP-Specific MAX folder.
- Step 2:** Notify the Primary ISSO via email that the reviews are complete.

Continuous Monitoring Team:

- Step 1:** Navigate to the CSP-specific folder where the CSP-Specific *FedRAMP SAR Detailed Review Checklist Template* is located and download a copy to your local drive. This information is provided by the Primary ISSO.
- Step 2:** Navigate to the CSP-specific folder where the SAR and attachments to be reviewed are stored and download a working copy to your local drive.
- Step 3:** Extract the embedded vulnerability scans files from the SAR or download the files from the CSP-specific folder in MAX.

- Step 4:** Perform the vulnerability scan reviews and document the comments in the FedRAMP SAR Detailed Review Checklist Template. Insert or add more rows as may be necessary.
- Step 5:** Upload the completed checklist in the CSP-Specific MAX folder.
- Step 6:** Notify the Primary ISSO via email that the reviews are complete.

5. PHASE FOUR: POA&M REVIEW

Primary ISSO:

- Step 1:** Logon to MAX and navigate to the *Quality Management Guides and Templates* folder.
- Step 2:** Select the *FedRAMP POA&M Detailed Review Checklist Template*.
- Step 3:** Save the template in the MAX CSP-specific review folder with proper naming convention for the document being reviewed in accordance with the File Names Section of the *FedRAMP Writing Standards and Conventions*.
- Step 4:** Navigate to the CSP-specific folder where the CSP-Specific *FedRAMP POA&M Detailed Review Checklist Template* is located and download a copy to your local drive.
- Step 5:** Navigate to the CSP-specific folder where the POA&M to be reviewed is stored and download a working copy to your local drive.
- Step 6:** Review the POA&M in accordance with the CSP-Specific *FedRAMP POA&M Detailed Review Checklist Template* and document your comments and recommended corrective actions in the template. Insert or add rows as may be necessary to provide a single review comment per row.
- Step 7:** Provide the completed *POA&M Detailed Review Checklist Template* and *POA&M Detailed Review Report* to the CSP by posting the documents to MAX in the CSP-specific location in the JAB In-Process folder.
- Step 8:** Notify the CSP that the results of the POA&M Detailed Review are available on MAX for their review and response, if necessary.
- Step 9:** When the POA&M is updated and/or complete, post the document on MAX in the CSP-Specific Ready for JAB TR Review location and provide notification to the JAB TRs that the document is ready for their review.

6. PREPARE REVIEW RESULTS

The Primary ISSO performs the following steps upon receipt the completed templates.

- Step 1:** Compile the comments and results from the all completed checklist reviews into the *Detailed Review Results Template*.
- Step 2:** Prepare notifications based on the review results for each phase of the JAB P-ATO path. Table 3 below summarizes the possible actions.

Table 3. Detailed Review Results Actions

Path	Results	Action
SSP and Attachment Review	Acceptable	Document package submitted for Detailed Review and status is eligible to be submitted to JAB TRs for review
	Unacceptable	Documents returned to Applicant for defect repair
SAP Review	Acceptable	Document submitted to JAB TRs for review
	Unacceptable	Document returned to Applicant for defect repair
SAR Review ATO	Acceptable	Document package submitted to JAB TRs for review
	Unacceptable	Document package returned to Applicant for defect repair
POA&M Review	Acceptable	Document submitted to JAB TRs for review
	Unacceptable	Document returned to Applicant for defect repair

- Step 3:** Send notifications to CSP and JAB TRs as applicable.

7. REFERENCED FEDRAMP DOCUMENTS

Title	Description
FedRAMP SSP and Attachment Detailed Review Checklist Template	<p>These Detailed Review Checklist Templates are worksheets with entries for identifying defects in the documents provided. For example, the SSP may have defects in the control implementation descriptions and the SAR may have defects in the descriptions of the assessment of those controls. The Primary ISSO, Secondary ISSOs, and Continuous Monitoring Team members use these checklists.</p>
FedRAMP SAP Detailed Review Checklist Template	
FedRAMP SAR Detailed Review Checklist Template	
FedRAMP POA&M Detailed Review Checklist Template	
FedRAMP Detailed Review Results Template	<p>This Detailed Review Results Template is a document with a table for summarizing the review results. The Primary ISSO uses this document.</p>

8. DOCUMENT LOCATIONS

Reference Document	Location
Guide to Understanding FedRAMP	https://www.fedramp.gov/resources/documents/
FedRAMP Review and Approve Process SOP	https://www.fedramp.gov/resources/standard-operating-procedures-sops/
FedRAMP Secure Repository Provisioning Standard Operating Procedure.	Internal document
FedRAMP Writing Standards and Conventions	Internal document
FedRAMP SSP Detailed Review Checklist Template	Internal documents
FedRAMP CIS Detailed Checklist Template	
FedRAMP CM Plan Detailed Checklist Template	
FedRAMP e-Authentication Detailed Checklist Template	
FedRAMP FIPS 199 Detailed Checklist Template	
FedRAMP IR Plan Detailed Checklist Template	
FedRAMP IT Contingency Plan Detailed Checklist Template	
FedRAMP PTA-PIA Detailed Checklist Template	
FedRAMP ROB Detailed Checklist Template	
FedRAMP Security P&P Detailed Checklist Template	
FedRAMP User Guide Detailed Checklist Template	
FedRAMP Continuous Monitoring Plan Detailed Checklist Template	
FedRAMP SAP Detailed Review Checklist Template	
FedRAMP SAR Detailed Review	

Reference Document	Location
Checklist Template	
FedRAMP POA&M Detailed Review Checklist Template	
FedRAMP Detailed Review Results Template	Internal document
SSP Red Team Review Template	Internal document
All Secondary ISSO Attachment Checklist Templates	Internal documents

APPENDIX A: TABLE OF ACRONYMS

Acronym	Meaning
3PAO	Third-Party Assessment Organization
ATO	Authorization to Operate
CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
ISSO	Information System Security Officer
JAB	Joint Authorization Board
JAB TR	JAB Technical Representative
P-ATO	Provisional Authorization to Operate
PMO	Program Management Office
POA&M	Plan of Action and Milestones
QC	Quality Control
SAP	Security Assessment Plan
SAR	Security Assessment Report
SOP	Standard Operating Procedure
SSP	System Security Plan

APPENDIX B: REQUIRED AUTHORIZATION PACKAGE DOCUMENTS

The following documents are required regardless of path, except for the Agency ATO Letter, which is only required for the Agency ATO path. Some of these documents may be embedded or included in sections in other documents. When a FedRAMP template is not available, NIST Special Publication 800 series guidance should be followed. Applicants on the JAB P-ATO path will submit the SSP first, followed by the SAP, SAR, and POA&M in sequence as the previous documents are completed and approved by the JAB TRs.

Table 4. Authorization Package Documents and Attachments

Item No.	Document Title (attachments indented)	FedRAMP Template
1.0	System Security Plan (SSP)	Yes
1.1	FIPS Pub 199	Yes
1.2	e-Authentication	Yes
1.3	Information System Security Policies & Procedures	No
1.4	Configuration Management Plan (CM) Plan	No
1.5	Continuous Monitoring (ConMon) Plan	No
1.6	Control Implementation Summary (CIS) and Worksheet	Yes
1.7	IT Contingency Plan (CP)	Yes
1.8	Incident Response Plan (IRP)	No
1.9	Privacy Threshold Analysis (PTA) / Privacy Impact Analysis (PIA)	Yes
1.10	User Guide	No
1.10	Rules of Behavior (ROB)	Yes
2.0	Security Assessment Plan (SAP)	Yes
2.1	Rules of Engagement (ROE)	No
2.2	Security Assessment Test Cases	Yes
2.3	Penetration Testing Plan	No
3.0	Security Assessment Report (SAR)	Yes
3.1	Completed Security Assessment Test Cases	N/A
3.2	Vulnerability Scans	N/A
4.0	Plan of Action and Milestones (POA&M) – If outstanding Issues in SAR	Yes
5.0	Agency ATO Letter– Agency ATO path only	No