

FedRAMP Initial Review
Standard Operating Procedure



Version 1.3

August 27, 2015

Revision History

Date	Version	Page(s)	Description	Author
08/07/2015	1.0	All	Initial Release	FedRAMP PMO
08/17/2015	1.1	All	Readability Corrections	FedRAMP PMO
08/21/2015	1.2	All	Readability Corrections; corrected Table 3 on page 10	FedRAMP PMO
08/27/2015	1.3	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.....	2
1.3. Roles and Responsibilities.....	2
1.4. Coordination Among Organizational Entities	2
1.5. Compliance	2
1.6. Prerequisites.....	2
2. Initial Security Documents Review	4
2.1. Part One: Showstopper Review	4
2.2. Part Two: Readability Review	5
2.3. Part Three: Prepare Review Results	5
3. Referenced FedRAMP Documents.....	7
4. Document Locations	8
Appendix A: Table of Acronyms.....	9
Appendix B: Required Authorization Package Documents.....	10

List of Tables

Table 1. Roles and Responsibilities.....	2
Table 2. Initial Review Results Actions	6
Table 3. Required Authorization Package Documents and Attachments.....	10

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 4 of this document 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 Standard Operating Procedure (SOP) is part of a larger SOP, the *FedRAMP Review and Approve SOP* which describes the entire Authorization Package Review and Approve process executed by the FedRAMP PMO. This Initial Review is the first review of the Authorization Package documents in this process.

1.1. PURPOSE

The Initial Review determines if the Authorization Package documents are complete, free of “showstoppers”, and readable (clear, concise, and consistent). Showstoppers are missing, incomplete, or weak critical security controls that must be addressed before the documents can continue through the FedRAMP review process. Initial Reviews also include a high-level security compliance review.

Upon completion of the Initial Review, the authorization package would be listed as FedRAMP Ready unless submitted as an Agency Authorization to Operate (ATO) Package. FedRAMP Ready is a milestone step in becoming FedRAMP Compliant, but it is not a final determination. FedRAMP Ready ensures that a CSP’s documentation meets the FedRAMP PMO’s minimum quality and security standards. To be listed as FedRAMP Ready, applicants must pass an Initial Review of their System Security Plan (SSP) and all SSP attachments (see Appendix C: Required Authorization Package Documents).

Once an applicant has been listed as FedRAMP Ready, they have one year to decide a path (if undecided), submit the remaining package documentation, and pass the Initial Review. If the completed authorization package does not pass an Initial Review within a year, the applicant will no longer be designated as FedRAMP Ready.

Poorly written documents detract from the reader’s understanding of the material, which delays the FedRAMP review process and reduces the value of the Authorization Package for reuse. Incomplete documents, documents with showstoppers, and/or documents with high-level security compliance concerns make it difficult or impossible to conduct vigorous Information

System Security Officer (ISSO) Detailed Reviews for documents on the JAB P-ATO review path. Documents that include showstoppers, high-level security concerns or incomplete and/or unreadable sections may be returned to the Applicant for completion or rework and resubmission, depending on the path. The FedRAMP PMO will perform an Initial Review on reworked and resubmitted documents again.

1.2. SCOPE

This SOP affects all three paths to achieving FedRAMP compliance: JAB P-ATO path, CSP Supplied path, and Agency 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 each 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. Roles and Responsibilities

Role	Responsibilities
Lead Reviewer	Assigns Authorization Packages and documents to be reviewed and their due date to Quality Control (QC) Technicians. Performs high-level security review of submitted documents.
QC Technician	Performs Initial Completeness, Showstopper, and Readability Reviews and submits completed checklists and reviews to the Lead Reviewer.

1.4. COORDINATION AMONG ORGANIZATIONAL ENTITIES

FedRAMP PMO Operations is responsible for managing the overall Initial Review process and performing a high-level security review on submitted documents. FedRAMP PMO Quality Management is responsible for performing the Initial completeness, Showstopper, and readability reviews and reporting their comments to Operations. See *FedRAMP Review and Approve SOP* for more information regarding their coordination.

1.5. COMPLIANCE

Documents must be clear, concise, consistent, complete, and free from showstoppers and high-level security concerns to comply with this review.

1.6. PREREQUISITES

The Lead Reviewer notifies the QC Technician via email that a document or Authorization Package is ready for review. The notification includes the document or Authorization Package's

location in the FedRAMP Secure Repository. The Lead Reviewer only assigns documents and Authorization Packages for reviews that are present in the Secure Repository, properly named, and can be opened. For more information on this repository, see the *FedRAMP Secure Repository Provisioning Standard Operating Procedure*.

The QC Technician must have successfully completed the *Initial Checklist and Readability* training module and have access to the following:

- The FedRAMP Secure Repository hosted on max.gov.
- The current version of the *FedRAMP Writing Standards and Conventions* reference document.
- The current version of the checklists described in Section 2 below.

The Lead Reviewer must have a cybersecurity and quality control background and access to the same repositories, reference documents, and checklists as the QC Technician.

2. INITIAL SECURITY DOCUMENTS REVIEW

In the interest of effectiveness and efficiency, this review is performed in two parts: the Showstopper Review and the Readability Review. The Showstopper Review includes a document-specific completeness review and is performed first to quickly determine whether or not further review is warranted. If the QC Technician determines the document is incomplete and/or there are showstoppers, the QC Technician terminates the review and reports their results to the Lead Reviewer. If the QC Technician determines there are no showstoppers, he or she completes the Initial Review by performing the Readability Review.

2.1. PART ONE: SHOWSTOPPER REVIEW

If there are two or more security documents in an Authorization Package, review them in the order listed in Step 2 below. Complete the following steps in sequential order.

- Step 1:** Logon to the FedRAMP Secure Repository and navigate to the *Quality Management Guides and Templates* folder.
- Step 2:** Select the appropriate review checklist template for the document as described below.
- 1) System Security Plan – *FedRAMP SSP Initial Review Checklist Template*
 - 2) Security Assessment Plan – *FedRAMP SAP Initial Review Checklist Template*
 - 3) Plan of Action and Milestones – *FedRAMP POA&M Initial Review Checklist Template*
 - 4) Security Assessment Report – *FedRAMP SAR Initial Review Checklist Template*
- Step 3:** Save the template in the Secure Repository folder described in the Lead Reviewer's notification with the proper naming convention for the document being reviewed in accordance with File Names Section of the *FedRAMP Writing Standards and Conventions*.
- Step 4:** Navigate to the folder where the document to be reviewed is stored and open the document. Do not modify the original document. Download a working copy to your local drive and write-protect it to prevent accidental modification.
- Step 5:** A) The QC Technician reviews the document for completeness and showstoppers in accordance with the *Initial Review Checklist* and documents their comments and recommended corrective actions in the checklist. The QC Technician does not enter data in the original document.
- B) The Lead Reviewer reviews the document(s) for high-level security concerns. If there are significant security findings, the Lead Reviewer discusses them with the ISSO.
- Step 6:** A) If the QC Technician finds showstoppers the QC Technician terminates the review. Otherwise he or she continues the review.

B) If the ISSO decides the high-level security findings are showstoppers, the review is terminated. Otherwise, the review is completed.

Step 7: A) If the review is terminated, the QC Technician notifies the Lead Reviewer via email and stops the review.

B) If the review is completed, the QC Technician notifies the Lead Reviewer via email and continues with the Readability Review.

2.2. PART TWO: READABILITY REVIEW

This review applies to Authorization Package documents without showstoppers, and their attachments, appendices, and other associated documents. When there are two or more documents associated with a security document, review them in the order presented in the security document. When there are two or more documents in an Authorization Package, review them in the order listed in the package.

Step 1: Logon to the FedRAMP Secure Repository and navigate to the *Quality Management Guides and Templates* folder.

Step 2: Select the *FedRAMP Readability Initial Review Template*.

Step 3: Save the template in the review folder with proper naming convention for the document being reviewed in accordance with the File Names and Folder Names Section of the *FedRAMP Writing Standards and Conventions*.

Step 4: Navigate to the folder where the document to be reviewed is stored and open the document. Do not modify the original document. Download a working copy to your local drive and write-protect it to prevent accidental modification.

Step 5: Review the document for readability in accordance with the *FedRAMP Readability Initial Review Template* and document your comments and recommended corrective actions in the template.

Step 6: When the review is finished, notify the Lead Reviewer via email.

2.3. PART THREE: PREPARE REVIEW RESULTS

The Lead Reviewer performs the following steps upon receipt the completed templates.

Step 1: Compile the comments and results from the completed checklist reviews and high-level security review, along with any evaluations of other documentation such as evidence, into the *Initial Review Results Template*.

Step 2: Prepare notification letter based on the review results and Applicant's Path. Table 2 below summarizes the possible actions.

Table 2. Initial Review Results Actions

Path	Results	Action
JAB P-ATO	Acceptable	Document/package submitted to Detailed Review
	Unacceptable	Authorization Package/Document returned to Applicant for defect repair
CSP Supplied	Acceptable	Authorization Package submitted to FedRAMP Director
	Unacceptable	Authorization Package returned to Applicant for defect repair
Agency ATO	Acceptable	Authorization Package submitted to FedRAMP Director
	Unacceptable	Submit Initial Review Results with package

Step 3: Send notification letter with attachments to the FedRAMP Director and FedRAMP Cybersecurity Manager for approval.

3. REFERENCED FEDRAMP DOCUMENTS

Title	Description
FedRAMP SSP Initial Review Checklist Template	<p>These Initial Review Checklist Templates are worksheets with entries for identifying completeness, showstoppers, and high-level security concerns within the document in review. A QC Technician and Lead Reviewer/Security Professional use these templates to document review results.</p>
FedRAMP SAP Initial Review Checklist Template	
FedRAMP POA&M Initial Checklist Template	
FedRAMP SAR Initial Review Checklist Template	
FedRAMP Readability Initial Review Template	<p>This Initial Review Template is a table with entries for identifying readability problems with the document being reviewed. A QC Technician uses this template to document completeness and Showstopper reviews.</p>
FedRAMP Initial Review Results Template	<p>This Initial Review Results Template is a document with a table for summarizing and rating the review results. The Lead Reviewer/Security Professional uses this document.</p>

4. DOCUMENT LOCATIONS

Document	Location
Guide to Understanding FedRAMP	https://www.fedramp.gov/resources/documents/
FedRAMP Review and Approve SOP	http://www.fedramp.gov/resources/standard-operating-procedures-sops/
FedRAMP Secure Repository Provisioning Standard Operating Procedure	Internal document
FedRAMP SSP Initial Review Checklist Template	https://www.fedramp.gov/resources/standard-operating-procedures-sops/
FedRAMP SAP Initial Review Checklist Template	https://www.fedramp.gov/resources/standard-operating-procedures-sops/
FedRAMP POA&M Initial Review Checklist Template	https://www.fedramp.gov/resources/standard-operating-procedures-sops/
FedRAMP SAR Initial Review Checklist Template	https://www.fedramp.gov/resources/standard-operating-procedures-sops/
FedRAMP Writing Standards and Conventions	Internal document
FedRAMP Readability Initial Review Template	https://www.fedramp.gov/resources/standard-operating-procedures-sops/
FedRAMP Initial Review Results Template	https://www.fedramp.gov/resources/standard-operating-procedures-sops/

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. 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 3. Required Authorization Package Documents and Attachments

Item No.	Document Title (attachments indented)	FedRAMP Template Available?	Agency Path	CSP Path	JAB Path	Undecided Path
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	Control Implementation Summary (CIS)	Yes	✓	✓	✓	✓
1.6	CIS Worksheet	Yes	✓	✓	✓	✓
1.7	IT Contingency Plan (CP) and CP Test	Yes	✓	✓	✓	✓
1.8	Incident Response Plan (IRP)	No	✓	✓	✓	✓
1.9	Privacy Threshold Analysis (PTA) / Privacy Impact Assessment (PIA)	Yes	✓	✓	✓	✓
1.10	User Guide	No	✓	✓	✓	✓
1.11	Rules of Behavior (ROB)	Yes	✓	✓	✓	✓
1.12	Signature Page	No	✓	✓	✓	✓
2.0	Security Assessment Plan (SAP)	Yes				
2.1	Rules of Engagement (ROE)	No	✓	✓	✓	✓
2.2	Security Assessment Test Cases	Yes	✓	✓	✓	✓
3.0	Security Assessment Report (SAR)	Yes				
3.1	Security Assessment Report	Yes	✓	✓	✓	✓
3.2	Security Test Cases	Yes	✓	✓	✓	✓
3.3	Vulnerability Scans	No	✓	✓	✓	✓
3.4	Ad Hoc Evidence	No	✓	✓	✓	✓
4.0	Plan of Action and Milestones (POA&M)	Yes	✓	✓	✓	✓
5.0	Agency ATO Letter (provided as PDF)	Yes	✓			
	[See Notes on Following Page]					

FedRAMP Initial Review SOP v1.3

Notes:

✓ = Required for initial package submission

✓ = Must be submitted eventually, but not with initial package submission. For undecided, CSPs have 12 months to select a path and submit missing documents. For JAB, missing documents are submitted based on a schedule developed by the CSP and ISSO. See section 2.2 for a description of the JAB path.