FedRAMP

FedRAMP System Security Plan (SSP) Required Documents

Presented by: FedRAMP PMO

GSA

info@fedramp.gov

fedramp.gov

What Does This Course Cover?

This course is divided into **three** main parts:

1 FedRAMP Initial Authorization Package Checklist

This is an Excel checklist that details the documents required for a complete FedRAMP initial authorization package.

2 SSP Overview

This section details the importance of the SSP with respect to the overall security package.

- The SSP Relationship with Other Documents
- The SSP Organization and System Authorization Package Attributes
- SSP Organization and Scope
- Sections 1 - 12 of the SSP

3 Course Recap and Quiz

Course Objectives

At the conclusion of this course, you should understand:

- What documents are required for the FedRAMP initial authorization package submission
- Why the system security plan is one of the essential documents in the security package
- How to organize a system security plan
- How to develop clear, concise, consistent, and complete information within each section of a system security plan

FedRAMP Initial Authorization Package Checklist

Documentation

FedRAMP is a documentation-heavy process

- The FedRAMP Program Management Office or PMO has created some templates for documents that the CSP must edit and modify based on the security controls implemented in its system. Please note that FedRAMP does not have templates for all documents. You should become familiar with theses templates by searching for them on www.fedramp.gov.
- The templates provided by the FedRAMP PMO are intended to:
  - Standardize the security assessment process for agency reviews
  - Enable CSPs to move through the assessment process quickly
  - Enable agencies to more easily recognize where they can find important aspects of the systems used by agencies (some of these documents may be considered attachments to others, but are listed separately to enable easier uploading and tracking)
- Please note that if no template is provided, cloud service providers should follow the proper NIST standard (Special Publication (SP) 800 Series) to ensure required information is captured appropriately.

FedRAMP Initial Authorization Package Checklist

Cloud Service Providers Documentation Responsibilities

System Security Plan (SSP) - Must be submitted in Word format and a PDF version

SSP ATTACHMENT 1 - Information Security Policies and Procedures (covering all control families)

SSP ATTACHMENT 2 - User Guide

SSP ATTACHMENT 3 - Digital Identity Worksheet

SSP ATTACHMENT 4 - Privacy Threshold Analysis (PTA)

SSP ATTACHMENT 4 - Privacy Impact Assessment (PIA) (if the answer to any of the qualifying questions in the PTA is “Yes”, complete the PIA template and submit it as an attachment to the SSP)

SSP ATTACHMENT 5 - Rules of Behavior (RoB)

SSP ATTACHMENT 6 - Information System Contingency Plan (ISCP) (be sure to include the Contingency Plan Test Report in Appendix G of the ISCP)

SSP ATTACHMENT 7 - Configuration Management Plan (CMP)

SSP ATTACHMENT 8 - Incident Response Plan (IRP)

SSP ATTACHMENT 9 - Control Implementation Summary (CIS) Workbook

SSP ATTACHMENT 10 - Federal Information Processing Standard (FIPS) 199

SSP ATTACHMENT 11 - Separation of Duties Matrix

SSP ATTACHMENT 12 - Laws and Regulations (if additional system-specific laws or regulations apply (e.g., HIPAA), include them)

SSP ATTACHMENT 13 - Integrated Inventory Workbook

Plan of Action and Milestones (POA&M)

Continuous Monitoring Strategy (required by CA-7)

Continuous Monitoring Monthly Executive Summary

FedRAMP Initial Authorization Package Checklist *(cont.)*

Third Party Assessment Organizations Documentation Responsibilities

Security Assessment Plan (SAP)

Must be submitted in Word format; final versions can be submitted in PDF, after a FedRAMP Authorized designation is achieved

- SAP APPENDIX A - Security Test Case Procedures
- SAP APPENDIX B - Penetration Testing Plan and Methodology
- SAP APPENDIX C - 3PAO Supplied Deliverables (e.g., Penetration Test Rules of Engagement, Sampling Methodology)

Security Assessment Report (SAR)

Must be submitted in Word format; final versions can be submitted in PDF, after a FedRAMP Authorized designation is achieved

- SAR APPENDIX A - Risk Exposure Table
- SAR APPENDIX B - Security Test Case Procedures
- SAR APPENDIX C - Infrastructure Scan Results
- SAR APPENDIX D - Database Scan Results
- SAR APPENDIX E - Web Scan Results

NOTE: Provide all fully authenticated infrastructure, database, and web scans results generated by the scanner in a readable format. Do not provide files that require a scan license to read the file. Bundle scan results into one zip file.

- SAR APPENDIX I - Auxiliary Documents (e.g., evidence artifacts)
- SAR APPENDIX J - Penetration Test Report

FedRAMP Initial Authorization Package Checklist *(cont.)*

The Authorizing Official or AO Documentation Responsibilities

- There are two approaches to obtaining a FedRAMP authorization:
  - A provisional authorization through the Joint Authorization Board (JAB)
  - An authorization through an agency
- Either the JAB or agency is responsible for the Authorization To Operate Letter (ATO) letter.
- In the agency authorization path, agencies may work directly with a cloud service provider (CSP) for authorization at any time. CSPs that make a business decision to work directly with an agency to pursue an Authority to Operate (ATO) will work with the agency throughout the FedRAMP authorization process.
- For a JAB authorization, cloud service providers must submit a business case through the FedRAMP Connect process.
- FedRAMP may prioritize up to 12 CSOs for a JAB authorization per year.
  - In the business case provided to the FedRAMP Connect Team, the most important prioritization criteria is to demonstrate government-wide demand for the cloud service offering. Second, cloud service offerings who are FedRAMP Ready have preference in prioritization.

SSP Overview

Objectives of the SSP

What is a System Security Plan or SSP?

- The system security plan provides an overview of the security requirements for a cloud service offering.
- The system security plan describes the controls in place, or planned for implementation, to provide a level of security appropriate for the information to be transmitted, processed, or stored by a system.
- The system security plan contains the:
  - Authorization boundary diagram
  - Data flow diagram
  - Types of inheritances from other FedRAMP leveraged systems
  - External services in use by the system (external services are other cloud services that are not FedRAMP authorized such as corporate services and external update services)
  - Federally noted pieces that should be adequately described and secured. For instance:
    - Development/test environments
    - Any transport services
    - Multi-factor authentication
    - All alternate storage and processing sites

System Security Plan Document Attachments

FedRAMP does add emphasis to these documents being carefully and thoughtfully created:

IT Contingency Plan; Incident Response Plan; Configuration Management Plan; Privacy Threshold Analysis/Privacy Impact Analysis; Control Implementation Summary

The SSP is aligned with the following attachments:

SSP ATTACHMENT 1	Information Security Policies and Procedures (covering all control families)
SSP ATTACHMENT 2	User Guide
SSP ATTACHMENT 3	Digital Identity Worksheet
SSP ATTACHMENT 4	Privacy Threshold Analysis (PTA)
SSP ATTACHMENT 4	Privacy Impact Assessment (PIA) (if the answer to any of the qualifying questions in the PTA is “Yes”, complete the PIA template and submit it as an attachment to the SSP)
SSP ATTACHMENT 5	Rules of Behavior (RoB)
SSP ATTACHMENT 6	Information System Contingency Plan (ISCP) (be sure to include the Contingency Plan Test Report in Appendix G of the ISCP)
SSP ATTACHMENT 7	Configuration Management Plan (CMP)
SSP ATTACHMENT 8	Incident Response Plan (IRP)
SSP ATTACHMENT 9	Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM) Workbook
SSP ATTACHMENT 10	Federal Information Processing Standard (FIPS) 199
SSP ATTACHMENT 11	Separation of Duties Matrix
SSP ATTACHMENT 12	Laws and Regulations (if additional system-specific laws or regulations apply (e.g., HIPAA), include them)
SSP ATTACHMENT 13	Integrated Inventory Workbook

Necessary Organization and System Attributes

The cloud service offering must be documented to demonstrate important aspects such as:

1. The system boundary and all data flows internally, externally, and traversing the system boundary
2. All dataflows that have FIPS 140 validated encryption internally, externally, and traversing the system boundary with the correct directional arrows
3. The customer responsibilities, for each security control, defined in the system baseline and what the leveraging partner must do to implement controls.
4. System diagrams that show the cloud service offering provides identification and two-factor authentication plus all authentication methods minimally for:
   a. Network access by privileged customer accounts
   b. Network access by non-privileged customer accounts
   c. Network access by the cloud service privileged administrators
   d. Local access by the cloud service privileged administrators (when applicable)
5. All scanning capabilities for operating systems, databases, and web applications
6. The CSP can remediate high risks within 30 days, moderate risks within 90 days, and low risks within 180 days
7. An inventory for all hardware, software, and firmware

FedRAMP Mindset for SSP Development

How to Write a System Security Plan

1. Writing Takes Time and Effort
2. Strongly and Clearly Articulate System Functionality
3. Tell a Story
4. Answer Who, What, When, and How
5. Answer 100% of the Controls
6. Be Clear, Concise, Consistent, and Complete
7. Adequately Reference all Documentation
8. Ensure Compliance with FedRAMP Policy

SSP Organization and Scope

Section 1:	Identifies information system name and title
Section 2:	Identifies the system categorization and digital identity determination
Section 3:	Identifies the system owner and contact information
Section 4:	Identifies the authorizing official
Section 5:	Identifies other designated contacts
Section 6:	Identifies the assignment of security responsibility
Section 7:	Identifies the information system operational status
Section 8:	Identifies the type of information system
Section 9:	Describes the function and purpose of the information system
Section 10:	Describes the information system environment and inventory
Section 11:	Identifies interconnections between other information systems
Section 12:	Laws, regulations, standards, and guidance
Section 13:	Minimum Security Controls

Sections 1-8: Identifying the System

Using the FedRAMP Templates

All tables in the SSP template should be populated with the most current information - the “as is” state.

- Since the SSP is a living document, it will change based on the system environment.
  - If something changes in the SSP, normally the change affects other documents (e.g., the Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM), the “dash “1” control documentation, etc.).
- The FedRAMP PMO has incorporated blue italicized text instructions throughout the front sections of the SSP.
  - Once the instructions are met, the instruction can be removed from the document.
- Consistency and accuracy are key.
  - The SSP tells a complete story from the beginning to end.
    - Inconsistencies and inaccuracies result in inconsistencies and inaccuracies in the security control implementation summaries.
- The authorization boundary is explicitly identified in the network diagram.
- The data flow diagram is aligned with the authorization boundary diagram.

If you have questions email info@fedramp.gov.

Section 9: General System Description

System Function/Purpose

Explain your system's technical function and purpose

Please refrain from including marketing language/material.

Information System Components & Boundaries

Describe the information system's major components, interconnections, and boundaries in sufficient detail that fully and accurately depicts the authorization boundary for the information system.

Types of Users

Include all roles and privileges, including system administrators, database administrators, customer end users, and customer administrators as role types.

Ensure that roles and privileges are specific and detailed enough to support 3PAO testing.

Network Architecture

Provide a legible and complete network diagram, which maps all system components.

If the authorization boundary shows sufficient detail regarding items like virtual private networks, subnets, ports and protocols, DNSSEC, the authorization boundary might also be able to be used as the network diagram.

Section 10: System Environment and Inventory

This section has the following components:

System Technical Environment

General description of the technical system environment

System Inventory

Directions for attaching the FedRAMP Inventory Workbook (Att. 13 – FedRAMP Inventory Workbook) can be found within the template

Data Flows

Describe all data flows and stores of data

Include data flows for privileged and non-privileged authentication/authorization to the system for internal and external users and encryption for all flows and stores internally, externally, and traversing the system boundary

Ports, Protocols, and Services

Indicates the components of the information system that make use of the ports, protocols and services

Section 11: System Interconnections

- Must be consistent with Table 13-3 - CA-3 Authorized Connections
- Lists each service provider IP address
- External Organization and IP address of the system
- External point of contact and phone number
- Connection security (IPSec, VPN, SSL Certificates, and Secure File Transfer)
- Data direction (incoming, outgoing, or both)
- Information being transmitted
- Port or circuit numbers

Section 12: Laws, Regulations, Standards and Guidance

Section 13: Minimum Security Controls

Security controls must meet the minimum security control baseline requirements for:

- Access Control (AC)
- Audit and Accountability (AU)
- Awareness and Training (AT)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Risk Assessment (RA)
- Security Assessment and Authorization (SA)
- Supply Chain Risk Management
- System and Communications Protection (SC)
- System and Information Integrity (SI)
- System and Services Acquisitions (SA)

Course Recap

Course Recap

As a recap to the course material, let's review a few key takeaways:

- When writing the SSP think of the 4 C's - Clear, Concise, Consistent and Complete.
- The SSP provides a global view of how the system is structured and is the focal point for all FedRAMP documentation but other documents that are provided along with the SSP have direct impact on the structure and content provided in the SSP.
- System boundary is a very critical concept for cloud security models and impacts the risk authorization levels for FedRAMP assessment. Security controls must meet minimum security control baseline requirements as defined by NIST 800-53A Rev 4.
- A high level of detail is required for writing FedRAMP control implementations and give a 3PAO solid evidence/artifacts when testing the control.

References

- Penetration Guidance
- NIST 800 53
- A2LA Website
- SAP Template
- Rev 4 Test Case Workbook
- 201 B Training

Learn more at **fedramp.gov**

Contact us at **info@fedramp.gov**

@FEDRAMP