



FedRAMP System Security Plan (SSP) Required Documents

6/5/2015

Presented by: Matt Strasburg

www.fedramp.gov



Today's Training

- Welcome! This training session is part 2 of the FedRAMP Training Series.
 1. Introduction to the Federal Risk and Authorization Program (FedRAMP) – 100A
 - 2. FedRAMP System Security Plan (SSP) Required Documents – 200A**
 3. FedRAMP Review and Approve Process
 4. Rev 3 to Rev 4 Transition
 5. Third Party Assessment Organization (3PAO) Specific Training
 6. Security Assessment Report (SAR) and Security Assessment Plan (SAP) Overview
 7. Significant Change Training for CSPs
- The goal of the FedRAMP Training Series is to provide a deeper understanding of the FedRAMP program and the level of effort required to satisfactorily complete a FedRAMP assessment.
- This is a mandatory course for Security Package submission.



What Does This Course Cover?

This course is divided into five main parts:

1. FedRAMP Required Documents for Package Submission
2. SSP Overview
 - a) Relationships to Other Documents
 - b) Necessary Organization and System Attributes
 - c) Organization and Scope
 - d) Sections 1-8
 - e) Section 9 – General System Description
 - f) Section 10 – Describing the System Boundary
 - g) Section 11 – System Interconnections
 - h) Section 12 – Minimum Security Controls
3. Tips for Writing the SSP
 - a) Control Example
4. Instructions for Submitting a Security Package
5. Course Recap and Quiz



Course Objectives

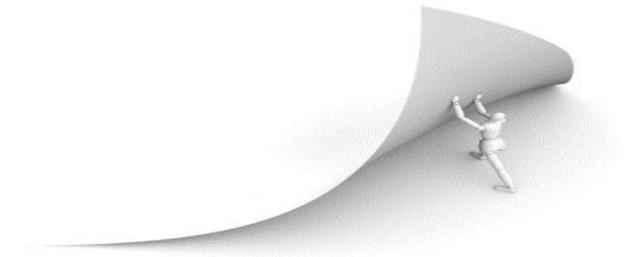
At the conclusion of this course, you should understand:

- What documents are required for initial package submission
- Why the SSP is one of the essential documents in the Security Package
- How to properly prepare for writing a SSP and submitting a Security Package
- How the SSP is organized and its relation to other documents included in the Security Package
- How to develop clear, concise, consistent, and complete information within each section of the SSP
- The appropriate level of detail to provide in the SSP



FedRAMP is a documentation-heavy process

- The FedRAMP PMO created templates for documents that the CSP must edit and modify based on the security controls implemented in its system.
- The templates provided by the FedRAMP PMO are intended to:
 - Standardize the security assessment process for Agency review
 - Enable CSPs to move through the assessment process quickly
- Some of these documents may be considered attachments to others, but are listed separately to enable easier uploading and tracking.
- Please note that there are FedRAMP templates for most of these documents, provided on our website at FedRAMP.gov. If no template is provided, follow the proper NIST Standard (SP 800 Series) to ensure required information is captured appropriately.





List of mandated documents for initial Security Package submission

Joint Authorization Board (JAB) Path Documents

- FIPS 199*
- E-Authentication Template**
- Information System Security Policies and Procedures
- Privacy Threshold Analysis (PTA) / Privacy Impact Analysis (PIA)**
- Configuration Management Plan (CM)
- Incident Response Plan (IR)
- IT Contingency Plan**
- System Security Plan (SSP)*
- Rules of Behavior (ROB)**
- Control Implementation Summary (CIS)*
- User Guide

Additional Documents for Agency Authorization to Operate (ATO) and CSP Supplied Path

- Agency ATO Letter** (Agency ATO Path Only)
- Security Assessment Plan (SAP)*
- Security Assessment Test Cases
- Security Assessment Report (SAR)*
- Plan of Action and Milestone (POA&M)**

* = Mandatory Documents
** = Highly Recommended



Objectives of the SSP

The SSP is the main document in which the CSP describes all the security controls in use on the information system and their implementation.

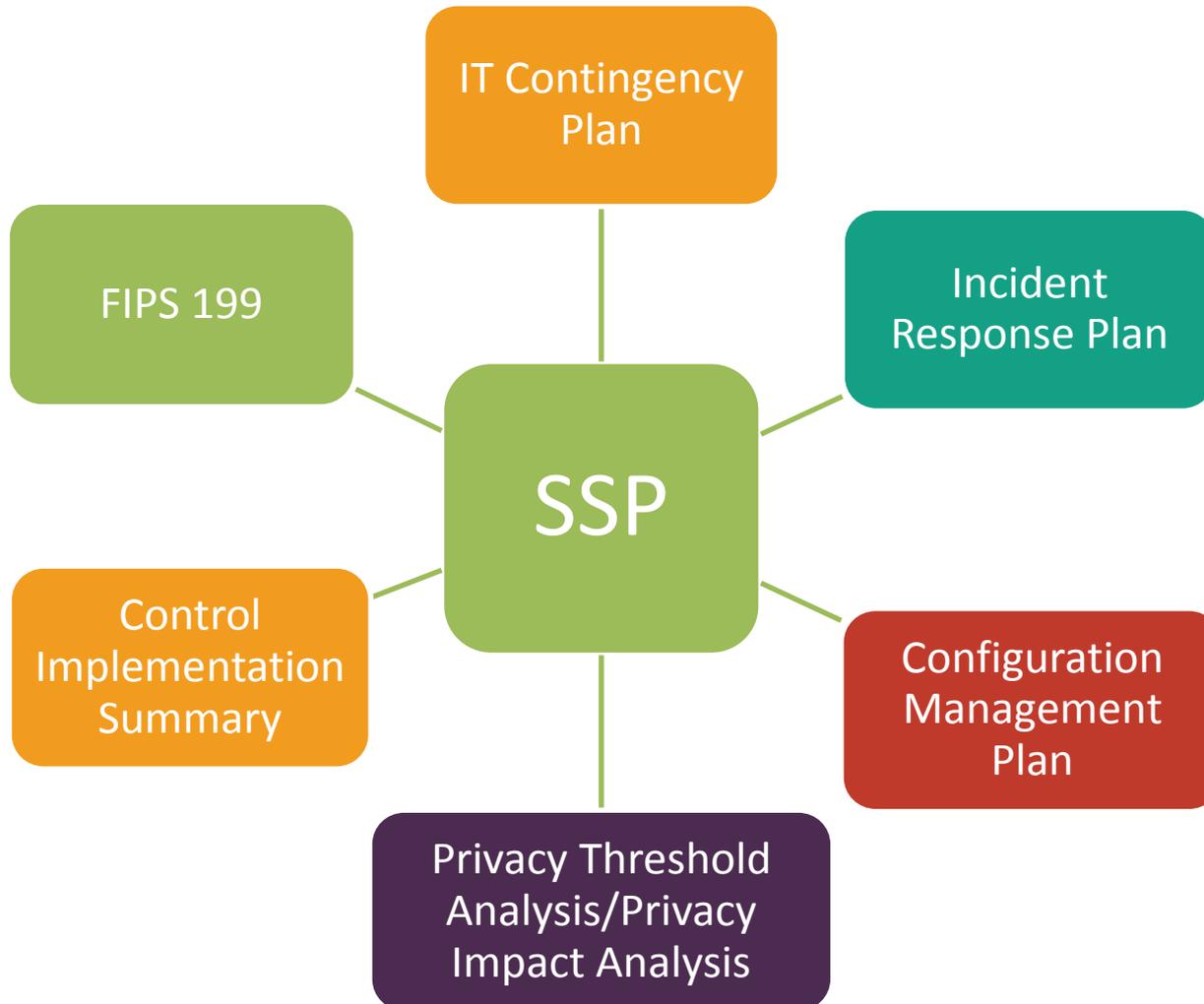
Provides a global view of how the system is structured

Identifies sub-organizations in the organization or point of contacts that are responsible for system security

Clearly delineates control responsibility between the customer and CSP



System Security Plan Document Attachments





Necessary Organization and System Attributes

The CSP and its Cloud service must be documented to show the following:

1. The CSP has the ability to process electronic discovery and litigation holds.
2. System boundaries are clearly defined and described.
3. Customer responsibilities and what they must do to implement controls are identified.
4. The system provides identification and two-factor authentication for:
 - a) network access by privileged accounts
 - b) network access by non-privileged accounts
 - c) local access by privileged accounts
5. The CSP can perform code analysis scans for code written in-house (non-COTS products).
6. The system has boundary protections with logical and physical isolation of assets.
7. The CSP can remediate high risk issues within 30 days, medium risk issues within 90 days.
8. An inventory and configuration build standards for all devices is provided.
9. The system has safeguards to prevent unauthorized information transfer via shared resources.
10. The system has cryptographic safeguards preserve confidentiality and integrity of data during transmission



FedRAMP Mindset for SSP Development

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

Consistency is Critical

- The information in Sections 1-11 of the CSP's SSP **MUST** be **100% ACCURATE** and **COMPLETE**.
- System Description, Roles and Responsibilities, Hardware, Software, and Network inventories, and boundary/architecture, network, and data flow diagrams are propagated across Contingency Plans, Configuration Management Plans, and other documentation.

Section 1	Identifies information system name and title
Section 2	Identifies the system categorization in accordance with FIPS 199
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 operational status of the information system
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
Section 11	Identifies interconnections between other information systems
Section 12	Provides an in-depth description of how each security control is implemented



Sections 1-8: Identifying the System

Fill in the blanks with the most accurate information.

The SSP is a living document and will change from time to time. If something changes in the SSP, chances are it will change in another document.

Make sure the information on the front page, the headers, and footers is consistent.

Read the instructions at the beginning of the document, as key details of information tend to be overlooked.

Pick an information system acronym and use it consistently throughout the document.

Do NOT manipulate the template in any way, shape, or form. You may add, but don't remove anything. If you have questions email info@fedramp.gov.



Section 9: General System Description

System Function/Purpose

Explain your system's function/purpose.

Information System Components and Boundaries

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

General System Description

Types of Users

Include all roles and privileges, including system administrators and database 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 the all system components.



Section 10: Information System Environment

Include information about all system environments that are used

- Production environment
- Test environment
- Staging or Quality Assurance (QA) environments
- Include alternate, backup and operational facilities.

System Inventory - This is a comprehensive inventory of all system components

- Hardware
- Software
- Network
- Port, Protocols, and Services



Section 11: System Interconnections





Section 12: Minimum Security Controls

Security controls must meet minimum security control baseline requirements

Access Control (AC)

Awareness and Training (AT)

Audit and Accountability (AU)

Security Assessment and Authorization (SA)

Configuration Management (CM)

Contingency Planning (CP)

Identification and Authentication (IA)

Incident Response (IR)

Maintenance (MA)

Media Protection (MP)

Physical and Environmental Protection (PE)

Planning (PL)

Personnel Security (PS)

Risk Assessment (RA)

System and Services Acquisitions (SA)

System and Communications Protection (SC)

System and Information Integrity (SI)



Tips for Writing the SSP

Clear

- Material is unambiguous, clear, and comprehensive
- Written in correct and consistent format
- Logical presentation of material

Concise

- Content and complexity is relevant to the audience
- No superfluous words or phrases

The 4 C's

Consistent

- Terms have the same meaning throughout the document
- Items are referred to by the same name or description throughout the document
- The level of detail and presentation style is the same throughout the document

Complete

- Responsive to all applicable FedRAMP requirements
- The Security Package Includes all appropriate sections of FedRAMP Template
- The Security Package Includes all attachments and appendices



Control Example: Account Management (AC-2)

The organization:

- a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];
- b) Assigns account managers for information system accounts;
- c) Establishes conditions for group and role membership;
- d) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- e) Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;
- f) Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];
- g) Monitors the use of information system accounts;
- h) Notifies account managers:
 - 1) When accounts are no longer required;
 - 2) When users are terminated or transferred; and
 - 3) When individual information system usage or need-to-know changes.
- i) Authorizes access to the information system based on:
 - 1) A valid access authorization;
 - 2) Intended system usage; and
 - 3) Other attributes as required by the organization or associated missions/business functions.
- j) Reviews accounts for compliance with account management requirements [*FedRAMP Assignment: at least annually*]; and
- k) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.



Control Definition

Each control objective (a-k) will need to be answered individually.

- As a guide to understanding the requirements for each control, the Rev 4 Test Cases may be reviewed.

Use the control as a cascading point to the rest of the definition (Example AC-2b)

- “The organization...” Assigns account managers for information system accounts.
- “The organization...” Establishes conditions for group and role membership.

Look at the verb in the control requirement: **Assigns**

- The verbs in each control explain the action to be implemented and must be used in the description.

Here is where the story-telling begins:

- Who (from your types of user list) assigns account managers?
- How and when are account managers assigned? Tell us how this is done. What is the process? Who is informed? When? How are they informed? What records are kept?
- Walk the reader through it like writing a story (beginning, middle, and end)

Keep in mind:

- ✓ If a 3PAO tests this control, is this implementation detailed enough for them to request solid evidence/artifacts?
- ✓ As a CSP, can I provide evidence for the 3PAO to examine or test, and can a CSP team member vouch for an implementation if interviewed?



Control Writing Tips

Organization Defined

- Organization-defined assignments are to be defined and documented by a CSP. Acceptable references may come from Standard Operating Procedures, Security Policy, or Concept of Operations guides.

Staying with AC-2, let's look at assessment objective (a):

Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];

- From the requirement, the control is asking the CSP to **identify** and **select** the following types of information system accounts to support organizational missions/business functions.
- The CSP can choose to include a reference to the policies where these accounts are identified, as long as the reference includes the **name**, **date**, and **version** of the policies, and the **section number** where these accounts can be located.



Control Writing Tips

FedRAMP Assignments

- These follow the same logic as organization-defined assignments and are to be treated as such. The assignments are also documented in the “Parameter” sections of the Control Summary Information following the requirements.

Requirements with multiple items (AC-2f)

The organization: Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];

- Each action needs to be addressed individually with the same level of detail to satisfy the control, so that it is testable.



Instructions for Submitting a Security Package

File Naming Convention and Package Upload

- Applicants are required to use FedRAMP's contact and inquiry email address (Info@FedRAMP.gov) to initiate contact with the FedRAMP team.
- The Applicant fills out and submits an application at FedRAMP.gov and attaches the required pre-application forms including the training certificate for this course. The name on the certificate must match the contact information on the SSP.
- Once provisioned access, Applicants are required to use the Office of Management and Budget's (OMB) MAX Secure Repository to send security packages to FedRAMP.
- When uploading the package to MAX:
 - All documents must be properly named in the following format
 - FedRAMP <document title> <version>.<date>.<file type>
 - File names should accurately reflect the contents of the document, not differing a great deal from the title of the document in the file.
- The PMO will validate that all documents have been received and notify the Applicant of acceptance.



Course Recap

- All available templates can be found on the FedRAMP website at [FedRAMP.gov](https://www.fedramp.gov) under the resources tab.
- All documentation must be clear, concise, consistent, and complete.
- Proper preparation prevents poor performance when it comes to writing the SSP.
- The SSP provides a global view of how the system is structured.
- System Description, Roles and Responsibilities, Hardware, Software, and Network inventories; and boundary/architecture, network, and data flow diagrams are propagated across the Security Package documentation.
- 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.



FedRAMP

Federal Risk Authorization Management Program

For more information, please contact us or visit us at any of the following websites:

<http://FedRAMP.gov>

<http://gsa.gov/FedRAMP>

Follow us on [twitter](#) @FederalCloud