FedRAMP System Security Plan (SSP) Required Documents

1. FedRAMP_Training_SSP v9_508

1.1 FedRAMP SSP Online Training Splash Screen

FedRAMP System Security Plan (SSP) Required Documents

1/22/2016

Presented by: FedRAMP PMO

www.fedramp.gov

Select the Next button to begin

Notes:

Transcript

Title <N/A>

Image

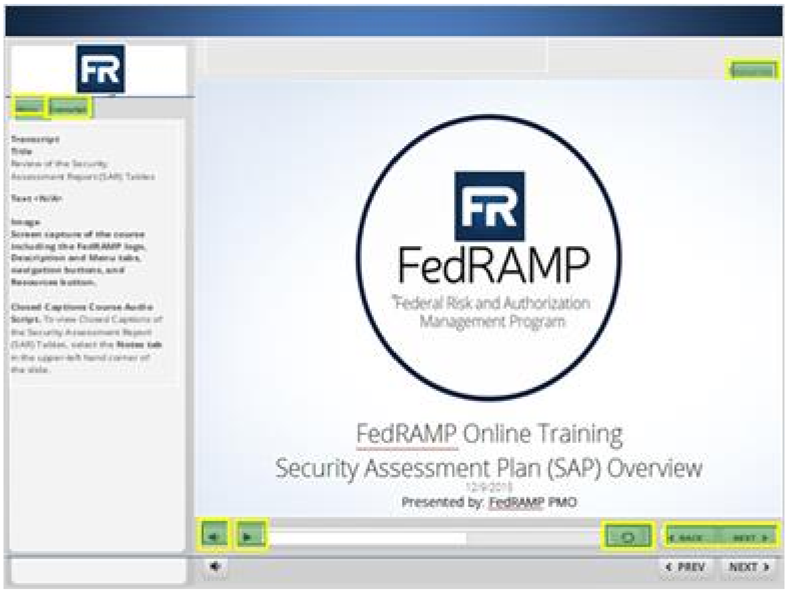
Image of FedRAMP logo.

Text

FedRAMP System Security Plan (SSP) Required Documents. Presented by: FedRAMP PMO.

Select the Next button to begin.

1.2 Course Navigation



Transcript

Title

Review of the Security Assessment Report (SAR) Tables

Text <N/A>

Image

Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

Closed Captions Course Audio Script. To view Closed Captions of the Security Assessment Report (SAR) Tables, select the Notes tab in the upper-left hand corner of the slide.

FedRAMP

"Federal Risk and Authorization Management Program

FedRAMP Online Training

Security Assessment Plan (SAP) Overview

12/9/2016

Presented by: FedRAMP PMO

Notes:

Transcript

Title

Course Features and Functions

Text

<N/A>

Image

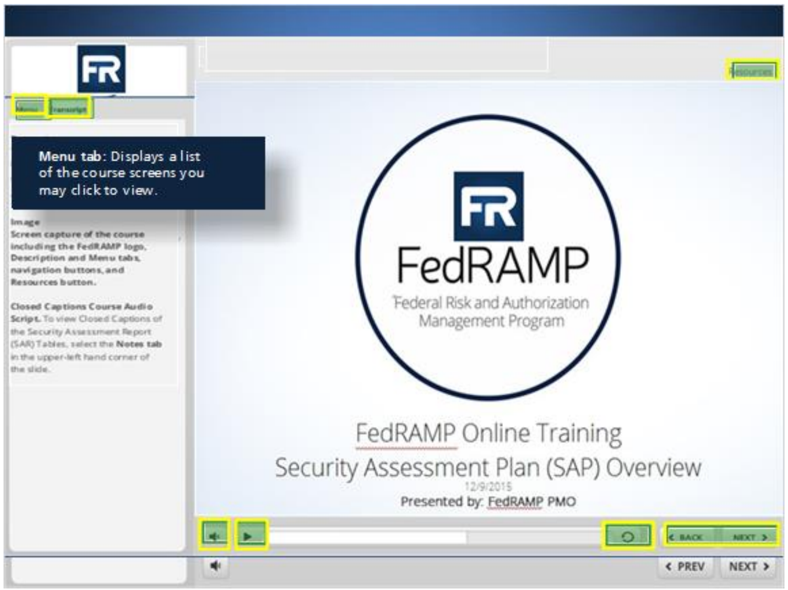
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

Audio

Let’s take a moment to familiarize ourselves with the features and functions of this course. To navigate the course, you may select the Back and Next buttons located at the bottom of the screen, or you may use the Menu tab located on the left side of the screen to select the screen you'd like to view. Use the Play and Pause buttons located at the bottom of the screen to start and stop the screen content. You may also select the replay button to view the content again. Use the Description tab on the left side of the screen to read a detailed description of the screen elements including the image descriptions, screen text, and audio script. You may also access the Resources button at the top right corner of the screen to open additional course resources.

When you are finished, click the Next arrow to continue.

Menu (Slide Layer)



Menu tab: Displays a list of the course screens you may click to view.

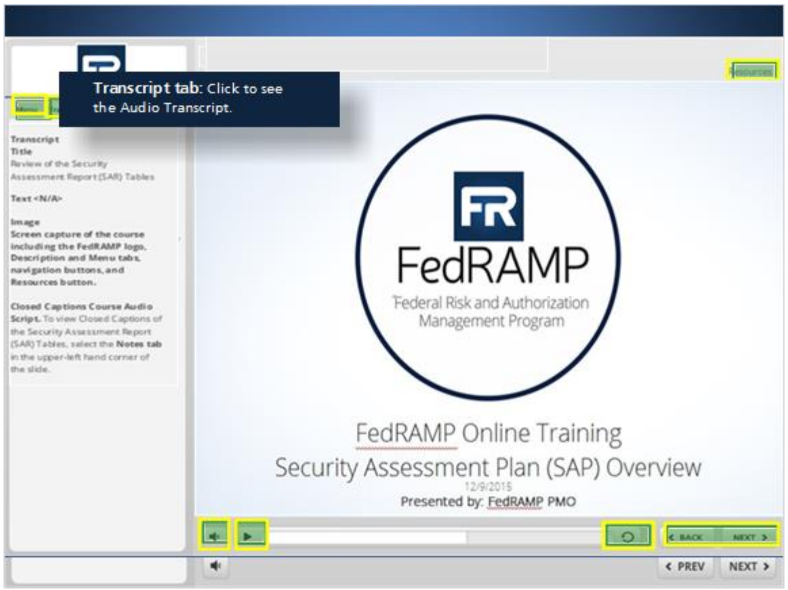
Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

Closed Captions Course Audio Script. To view Closed Captions of the Security Assessment Report (SAR) Tables, select the **Notes tab** in the upper-left hand corner of the slide.

FedRAMP
Federal Risk and Authorization Management Program

FedRAMP Online Training
Security Assessment Plan (SAP) Overview
12/9/2015
Presented by: FedRAMP PMO

Transcript (Slide Layer)



Transcript tab: Click to see the Audio Transcript.

Transcript
Title
Review of the Security Assessment Report (SAR) Tables

Text <N/A>

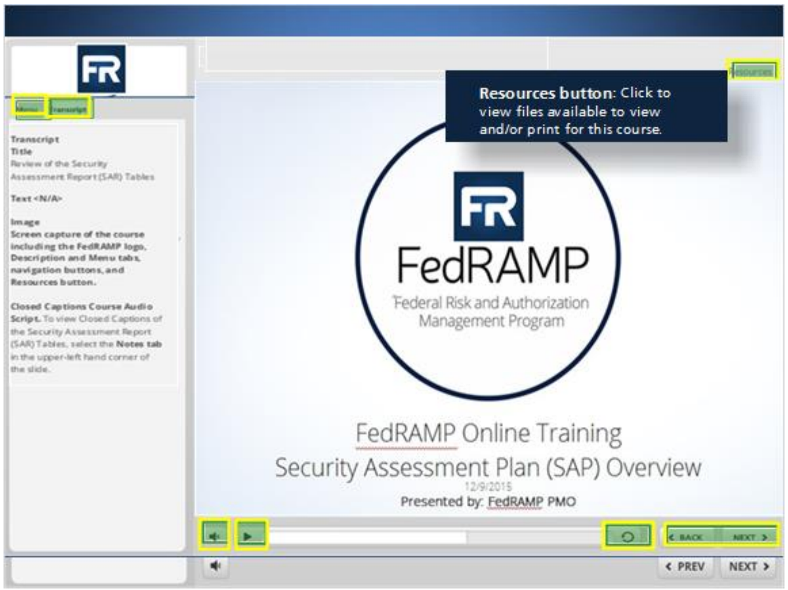
Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

Closed Captions Course Audio Script. To view Closed Captions of the Security Assessment Report (SAR) Tables, select the **Notes tab** in the upper-left hand corner of the slide.

FedRAMP
Federal Risk and Authorization Management Program

FedRAMP Online Training
Security Assessment Plan (SAP) Overview
12/9/2015
Presented by: FedRAMP PMO

Resources (Slide Layer)



Transcript
Title
Review of the Security Assessment Report (SAR) Tables

Text <N/A>

Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

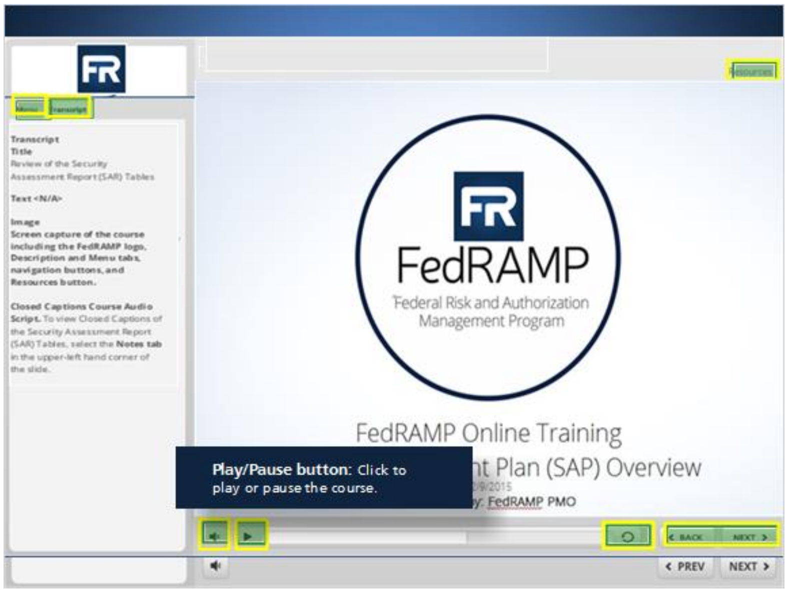
Closed Captions Course Audio Script. To view Closed Captions of the Security Assessment Report (SAR) Tables, select the **Notes tab** in the upper-left hand corner of the slide.

Resources button: Click to view files available to view and/or print for this course.

FedRAMP
Federal Risk and Authorization Management Program

FedRAMP Online Training
Security Assessment Plan (SAP) Overview
12/9/2015
Presented by: FedRAMP PMO

Play/Pause (Slide Layer)



Transcript
Title
Review of the Security Assessment Report (SAR) Tables

Text <N/A>

Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

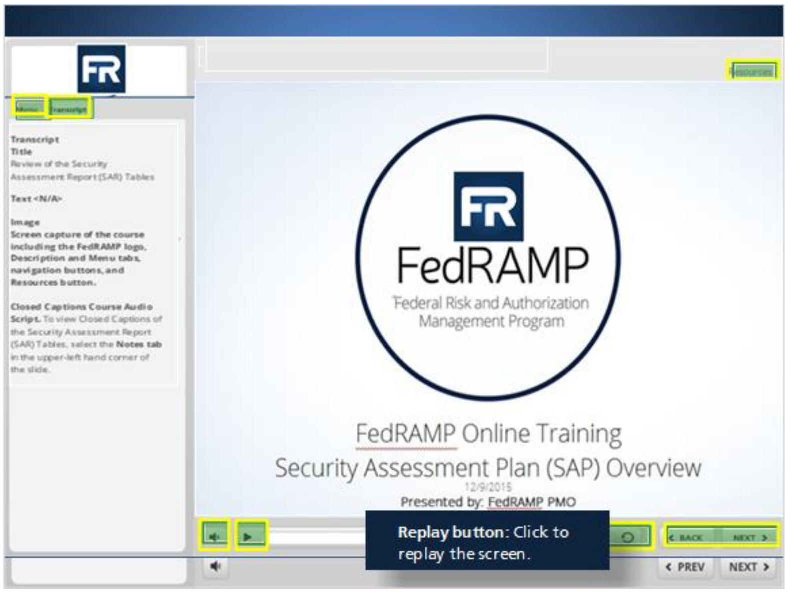
Closed Captions Course Audio Script. To view Closed Captions of the Security Assessment Report (SAR) Tables, select the **Notes tab** in the upper-left hand corner of the slide.

FedRAMP
Federal Risk and Authorization Management Program

FedRAMP Online Training
nt Plan (SAP) Overview
/9/2015
y: FedRAMP PMO

Play/Pause button: Click to play or pause the course.

Replay (Slide Layer)



Transcript
Title
Review of the Security Assessment Report (SAR) Tables

Text <N/A>

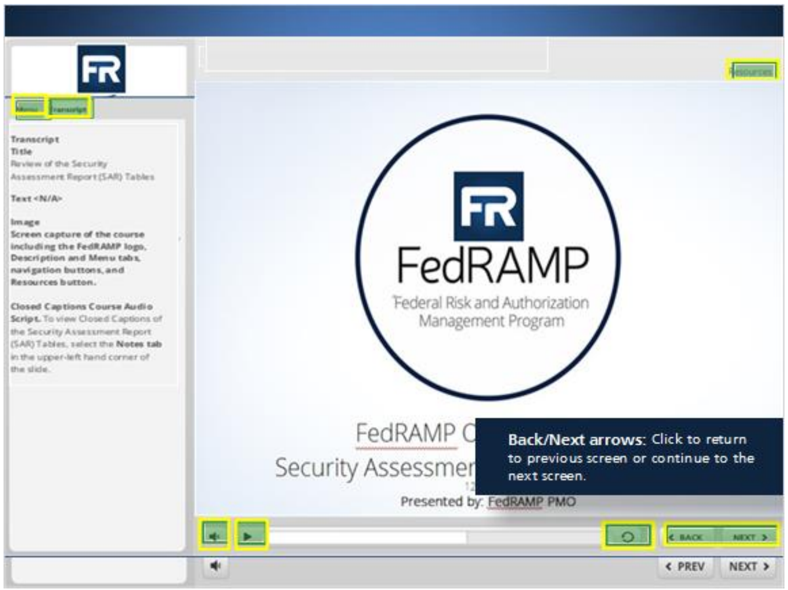
Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

Closed Captions Course Audio Script. To view Closed Captions of the Security Assessment Report (SAR) Tables, select the **Notes tab** in the upper-left hand corner of the slide.

FedRAMP Online Training
Security Assessment Plan (SAP) Overview
12/9/2015
Presented by: FedRAMP PMO

Replay button: Click to replay the screen.

Back/Next (Slide Layer)



Transcript
Title
Review of the Security Assessment Report (SAR) Tables

Text <N/A>

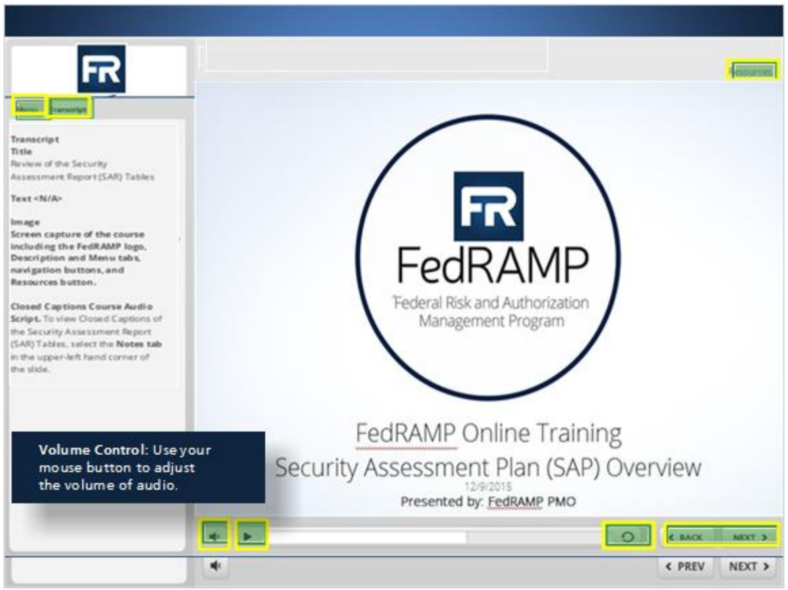
Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

Closed Captions Course Audio Script. To view Closed Captions of the Security Assessment Report (SAR) Tables, select the **Notes tab** in the upper-left hand corner of the slide.

FedRAMP O
Security Assessmer
Presented by: FedRAMP PMO

Back/Next arrows: Click to return to previous screen or continue to the next screen.

Volume Control (Slide Layer)



Transcript
Title
Review of the Security Assessment Report (SAR) Tables

Text <N/A>

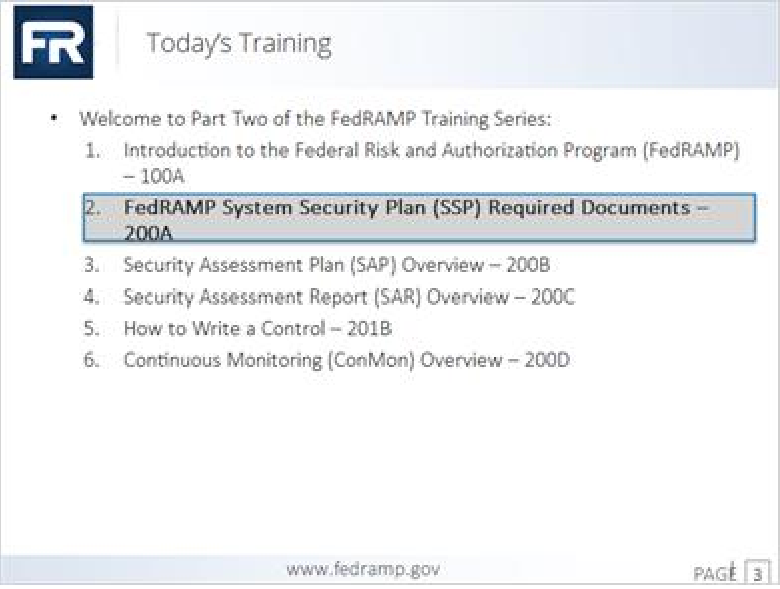
Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

Closed Captions Course Audio Script. To view Closed Captions of the Security Assessment Report (SAR) Tables, select the **Notes tab** in the upper-left hand corner of the slide.

Volume Control: Use your mouse button to adjust the volume of audio.

FedRAMP Online Training
Security Assessment Plan (SAP) Overview
12/9/2015
Presented by: FedRAMP PMO

1.3 Today's Training



Today's Training

- Welcome to Part Two 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. Security Assessment Plan (SAP) Overview – 200B
  4. Security Assessment Report (SAR) Overview – 200C
  5. How to Write a Control – 201B
  6. Continuous Monitoring (ConMon) Overview – 200D

www.fedramp.gov

PAGE 3

Notes:

Transcript

Today's Training

Image

<N/A>

Text

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.Security Assessment Plan (SAP) Overview - 200B
4.Security Assessment Report (SAR) Overview - 200C
5.How to Write a Control - 201B

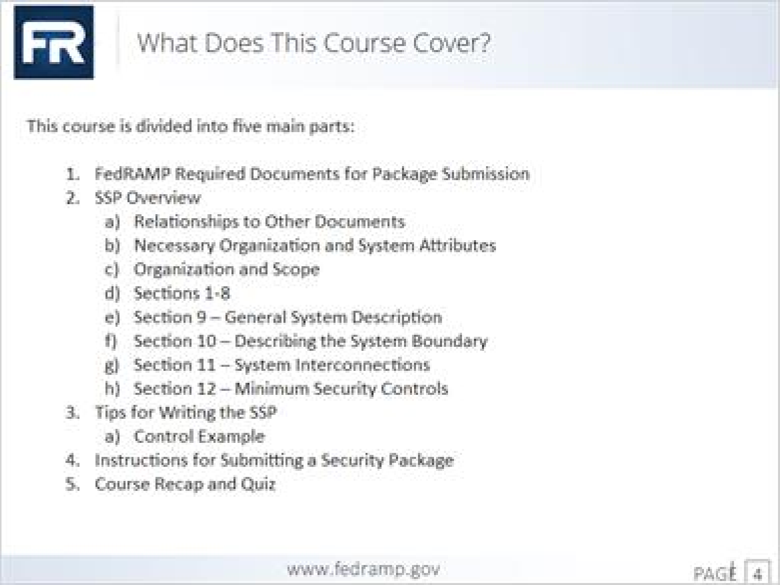
- Continuous Monitoring (ConMon) Overview - 200D
  The goal of the FedRAMP Training Series is to provide a deeper understanding of the FedRAMP program and the level of effort required to satisfactorily complete a FedRAMP assessment.
  This is a mandatory course for Security Package submission.

Audio

Welcome to part 2 of the FedRAMP Training Series, FedRAMP System Security Plan Required Documents, I am your host <name>. The FedRAMP Training Series strives to provide our Stakeholders with guidance and tips on the FedRAMP Program.

As an important note: While this is an open course for anyone to participate in, this course is mandatory for package submission regardless of intended path. This training module contains an online test of the material covered in this course and the training certificate, which is available after completion of this course and completing the customer satisfaction survey, must be presented to the FedRAMP PMO when applying to FedRAMP. In addition, the name on the training certificate must match the contact information on the System Security Plan.

1.4 What Does This Course Cover?



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

www.fedramp.gov PAGE 4

Notes:

Transcript

What Does This Course Cover?

Image

<N/A>

Text

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

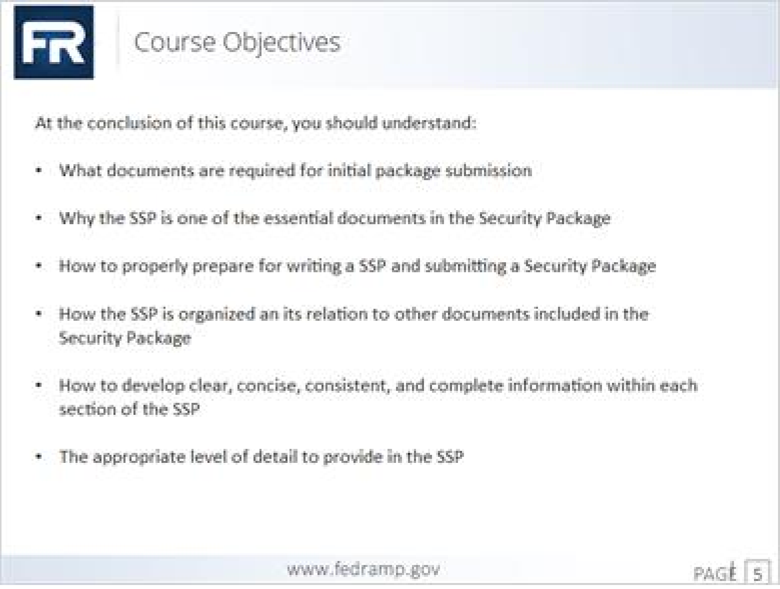
5.Course Recap and Quiz

Audio

The goal of this course is to familiarize you with required documentation for initial package submission and give a detailed overview of FedRAMP's System Security Plan template and its supporting documents. This will give you an understanding of the detail and rigor required by the FedRAMP PMO. In addition, we will review the System Security Plan or SSP for a cloud system and provide the information and guidelines that you need to accurately document the FedRAMP security controls for the cloud system.

We hope that this course will assist you in assembling a strong SSP that will meet FedRAMP requirements.

1.5 Course Objectives



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 an 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

www.fedramp.gov

PAGE 5

Notes:

Transcript

Course Objectives

Image

<N/A>

Text

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 an 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

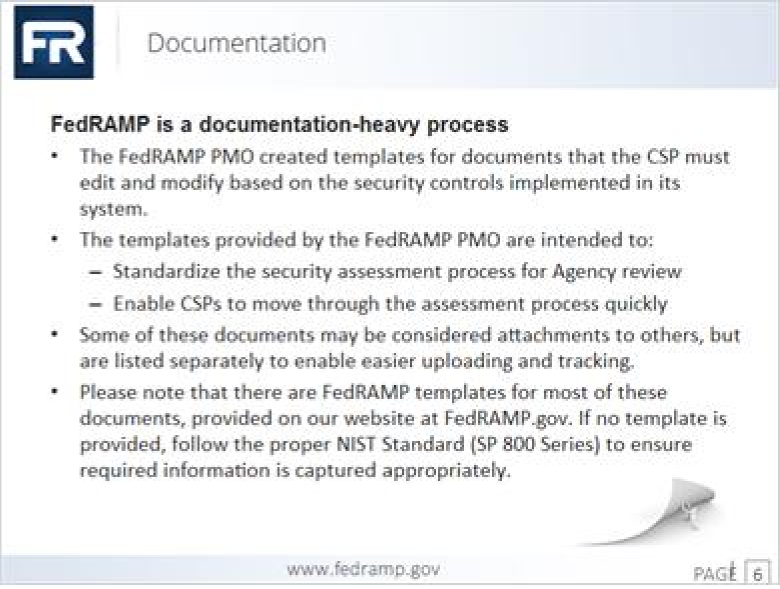
•

Audio

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 an 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

1.6 Documentation



Documentation

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.

www.fedramp.gov PAGE 6

Notes:

Transcript

Documentation

Image

Image of individual holding up paper

Text

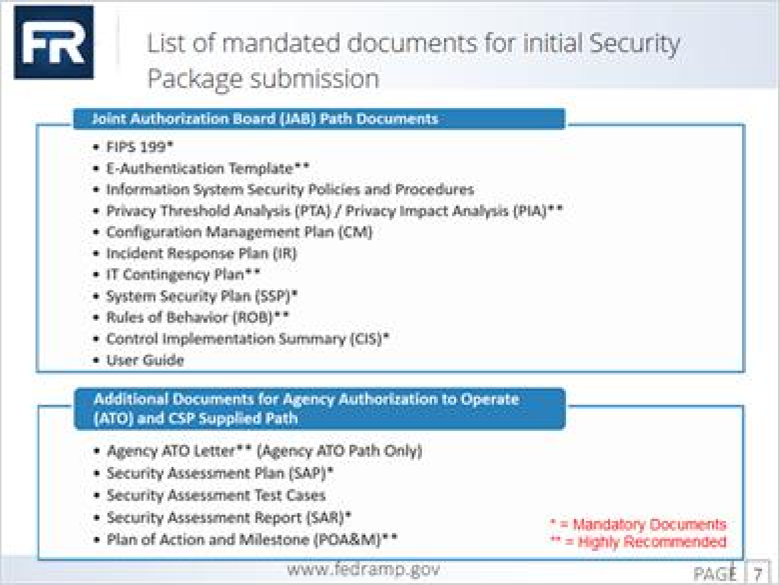
FedRAMP is a documentation-heavy process

- 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.

Audio

FedRAMP is a documentation heavy process and at the first glance of 400 plus page SSP the task of beginning to document your cloud system can seem pretty daunting. However, FedRAMP has created templates that are a great starting point. Using these templates are a critical aspect of the FedRAMP process because it standardizes the security assessment process for Agencies and enables the CSP to move through the assessment process quickly. All templates that FedRAMP provides are located on our website at FedRAMP.gov. However, there are some documents that are required for initial package submission that FedRAMP does not provide a template for. In these cases, please follow the NIST Special Publication 800 series standard and ensure that the required information is captured appropriately. As a note, all references used through out this training can be found in the top right hand portion of the presentation tab including the two just mentioned FedRAMP.gov and NIST.

1.7 List of mandated documents for initial Security Package submission



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

www.fedramp.gov

PAGE 7

Notes:

Transcript

List of mandated documents for initial Security Package submission

Image

<N/A>

Text

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)**

A**udio**

Now, a little bit more on the templates. For each Path the list of mandated documents for initial Security Package is slightly different. As a baseline, the following documents are required for all paths. They include:

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

Now, if a CSP is working with an Agency on an Authorization or if a CSP is self submitting to the FedRAMP Program, the CSP must also provide:

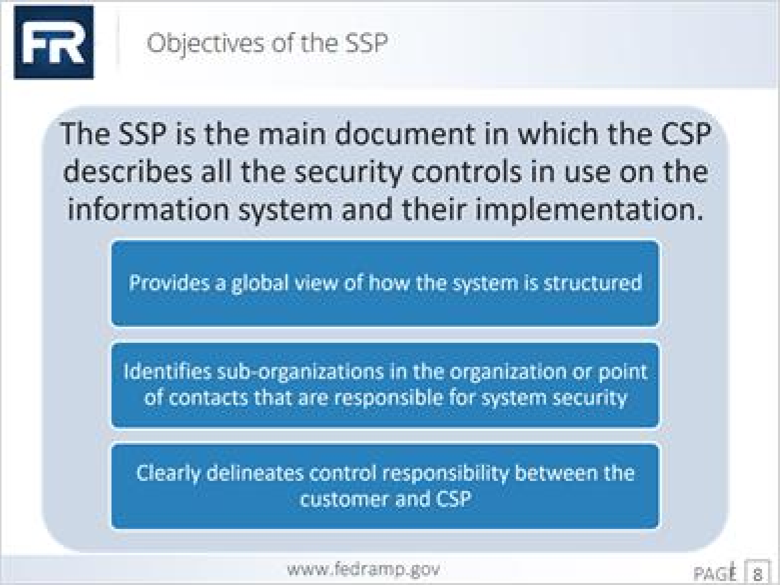
Security Assessment Plan (SAP)*
Security Assessment Test Cases
Security Assessment Report (SAR)*
Plan of Action and Milestone (POA&M)**

An Agency ATO Letter is only provided for Agency ATO Paths. As noted, The templates for documents marked with an asterisk* are mandatory that you use. The ones marked with a double asterisk** are highly recommended; You may use your own templates or follow the NIST standard as long as all required information is provided. If required information is not applicable or omitted for any reason, please clearly state the justification as to why that information is not provided.

Prior to submitting these documents please contact the FedRAMP PMO at info@fedramp.gov. At this time the FedRAMP PMO will ask for the training certificate and instruct the CSP to submit a FedRAMP Initiation Request at www.fedramp.gov. Once the initiation request is received by the FedRAMP PMO the PMO will set up access to the Secure Repository so that the CSP can upload these documents.

A little bit more on the FedRAMP Secure Repository, it provides a collaboration and document management solution for uploading, tracking, evaluating, reviewing, and managing CSP security authorization documents. The Secure Repository is housed within the Office of Management and Budget’s (OMB) MAX portal, a shared service utilized by agencies government-wide. MAX is recognized as the primary government-wide, government-managed collaboration tool.

1.8 Objectives of the SSP



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

www.fedramp.gov

PAGE 8

Notes:

Transcript

Objectives of the SSP

Image

<N/A>

Text

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

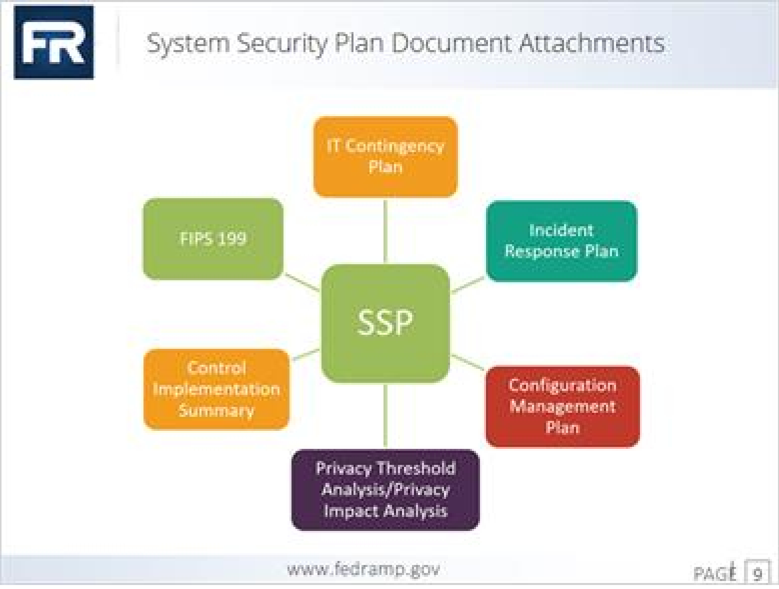
- Provides a global view of how the system is structured
- Identifies sub-organizations in the organization or point of contacts that are responsible for system security

Clearly delineates control responsibility between the customer and CSP

Audio

We are now going to transition into our detailed review of The System Security Plan or SSP. This document provides an overview of the security requirements for the Cloud System and 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 the system. The SSP:
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 and
Clearly delineates control responsibility between the customer and CSP

1.9 System Security Plan Document Attachments



System Security Plan Document Attachments

IT Contingency Plan

FIPS 199

Incident Response Plan

SSP

Control Implementation Summary

Configuration Management Plan

Privacy Threshold Analysis/Privacy Impact Analysis

www.fedramp.gov

PAGE 9

Notes:

Transcript

System Security Plan Document Attachments

Image

Image of SSP aligned to IT Contingency Plan; Incident Response Plan; Configuration Management Plan; Privacy Threshold Analysis/Privacy Impact Analysis; Control Implementation Summary

Text

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

Audio

In relation to the other documents provided in the System Security Package, The System Security Plan (SSP) is one of the most, if not the most, important document in the FedRAMP document set. The SSP provides a "big picture" view of a CSP's system security posture.

IT Contingency Plan

This document is used to define and test interim measures to recover information system services after a disruption. The ability to prove that system data can be routinely backed up and restored within agency specified parameters is necessary to limit the effects of any disaster and the subsequent recovery efforts.

Incident Response Plan

This plan documents how incidents are detected, reported, and escalated and should include timeframes, points of contact, and how incidents are handled and remediated. The Incident Response Plan should be consistent with NIST Special Publication 800-61 and the FedRAMP Incident Communication Plan.

Configuration Management Plan

This plan describes how changes to the system are managed and tracked. The Configuration Management Plan should be consistent with NIST SP 800-128

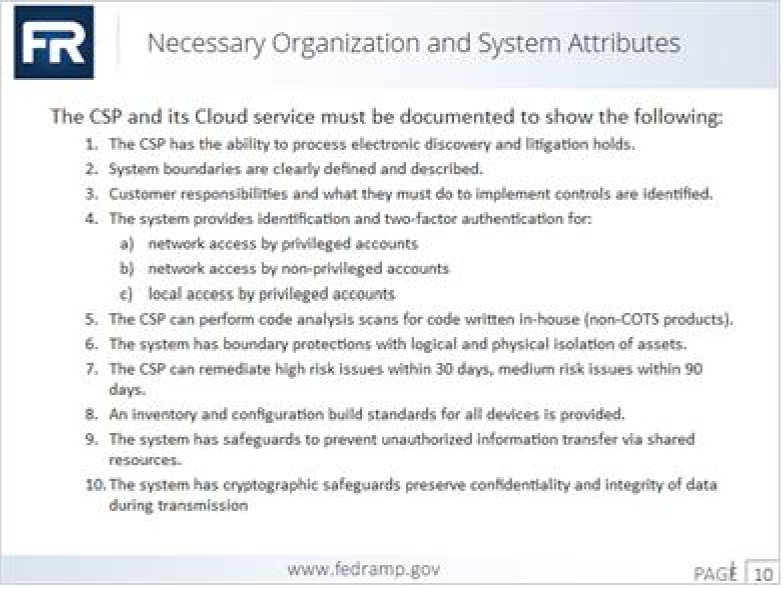
PTA/PIA
PTA This form is used to determine whether a Privacy Impact Analysis is required. A Privacy Impact Analysis is used to identify and mitigate privacy risks centered around Personally Identifiable Information or PII.

CONTROL IMPLEMENTATION SUMMARY
This document delineates the control responsibilities of the CSPs and customer agencies. In addition, the CIS provides a summary of all the required controls and enhancements across the system.

FIPS199
FIPS 199 document establishes the security categories to help determine the sensitivity of the cloud platform system.

FOR INFORMATION ABOUT OTHER DOCUMENTS, CHECK OUT OUR WEBSITE AT FEDRAMP.GOV

1.10 Necessary Organization and System Attributes



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

www.fedramp.gov

PAGE 10

Notes:

Transcript

System Security Plan Document Attachments

Image

N/A

Text

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

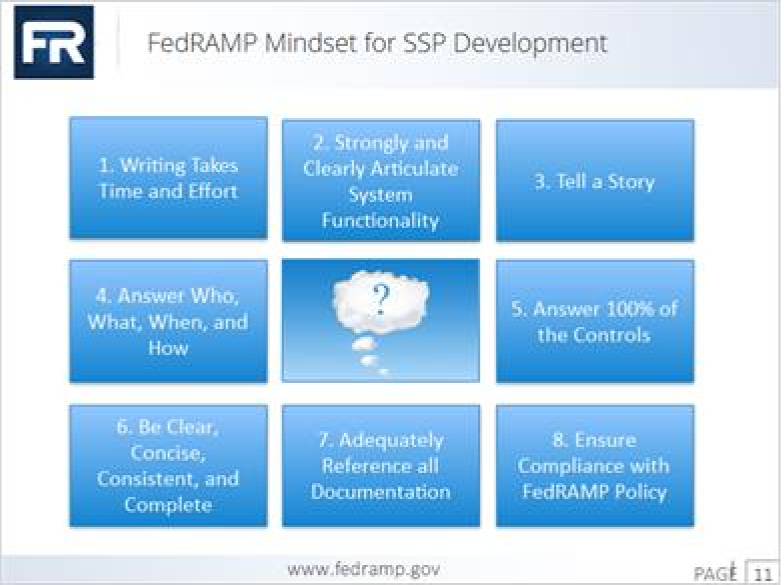
Audio

In relation

Audio

Now that we are aware of the documents that make up a FedRAMP Security Package let's prepare to document our Cloud System, in this case we can refer to the 5 P's … proper preparation prevents poor performance. It is essential that the CSP be able to document key characteristics of their Cloud system. You can even treat this as a checklist but ask yourself…
Can our system process electronic discovery and litigation holds?
Have we clearly defined our boundaries?
Have we identified customer responsibilities?
Can we remediate high risk issues within 30 days and medium risk issues within 90 days?
Do we have inventory and configuration build standards?
There are others too but the key is to first be able to answer yes to all of these questions and then be able to properly document them.

1.11 FedRAMP Mindset for SSP Development



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

www.fedramp.gov

PAGE 11

Notes:

Transcript Title

FedRAMP Mindset for SSP Development

Image

Images of nine showing the following:

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

Text

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

Audio

The System Security Plan is a document that requires an eye for detail. A few small mistakes can create a lot of questions following the review by the FedRAMP PMO, Agency, or JAB and slow down the assessment process. Before beginning documentation, it is important to understand the full scope of creating the SSP and level of effort required to make it good.

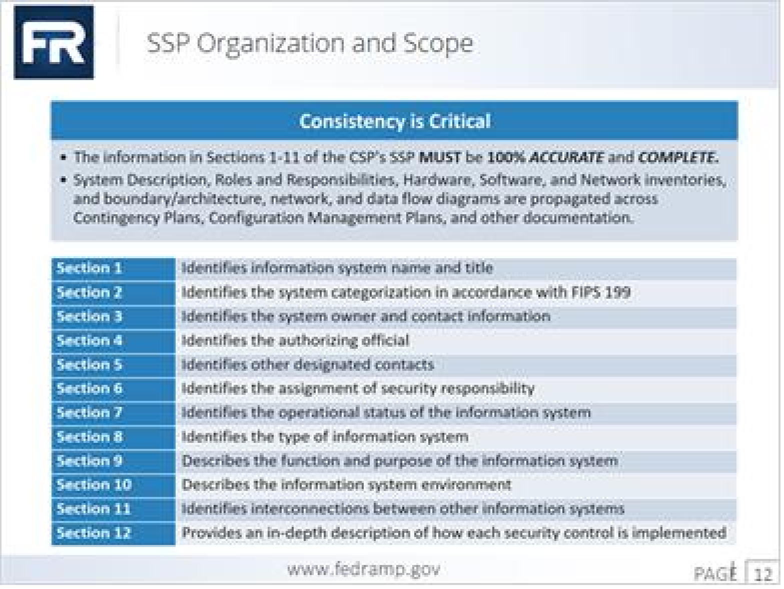
It is important to understand:

- Writing the SSP takes time, effort, careful thinking, and strong, clear articulation of your system's functionality The SSP is required to be complete and well-structured,
- Make sure that you have the required expertise and knowledge of NIST and FedRAMP security controls.
- Make sure you have enough resources - often one writer is not enough and you may have to allocate additional resources and subject matter experts to complete the SSP
- Make sure that the writers have technical knowledge of the system or can obtain the information from the System Owners

For the writers, we want you to tell your story and present the who, what, when, and how of the system.

- When filling out the SSP, be sure to answer 100% of the controls but, keep in mind that a strong SSP is tailored to fit the mission and system environment. If a specific control is inherited or not applicable provide a risk based justification as to why.
- We will touch more on these next points in a later slide but be clear, concise, consistent, and complete when writing and make sure you adequately reference all documentation and that your system is compliant with FedRAMP Requirements

1.12 SSP Organization and Scope



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

www.fedramp.gov

PAGE 12

Notes:

Transcript

SSP Organization and Scope

Image

Table listing Sections 1 through 11 of the SSP

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

Text

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
-

Table listing Sections 1 through 12 of the SSP

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

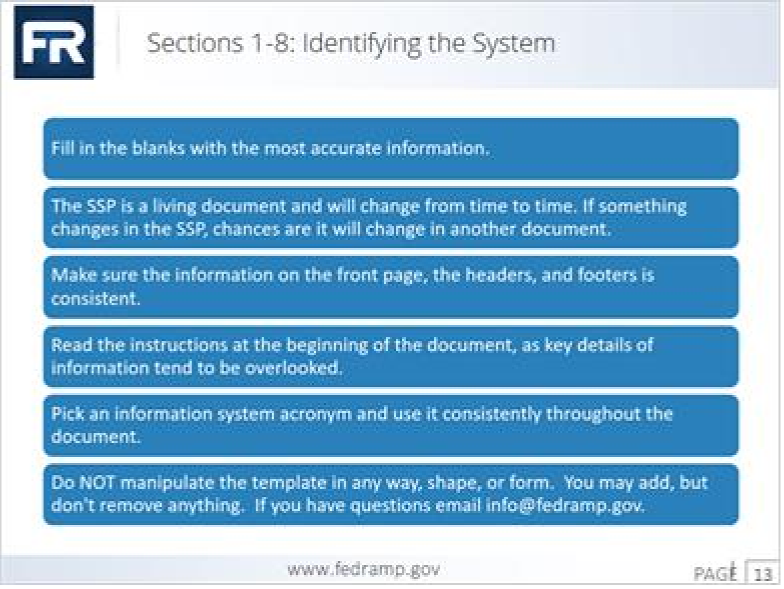
Section 12: Provides an in-depth description of how each security control is implemented

Audio

Moving on to the SSP there are 12 sections that need to be documented. You will find that these section are logically organized. In sections 1 through 8 you will be identifying the system. Who owns it, who is using it, and how is it classified. Sections 9 through 12 will be much more detailed and get into the systems security and describe how the system operates.

A CSP's SSP **MUST** be **100% accurate** because information such as System Description and Inventories, Roles and Responsibilities, boundaries and architectures, network and data flow diagrams are propagated across the other documents that we previously reviewed such as the IT Contingency Plans, Configuration Management Plans, and Incident Response Plans. Because of this relationship, consistency is critical.

1.13 Sections 1-8: Identifying the System



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.

www.fedramp.gov

PAGE 13

Notes:

Transcript

Sections 1-8: Identifying the System

Image

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.

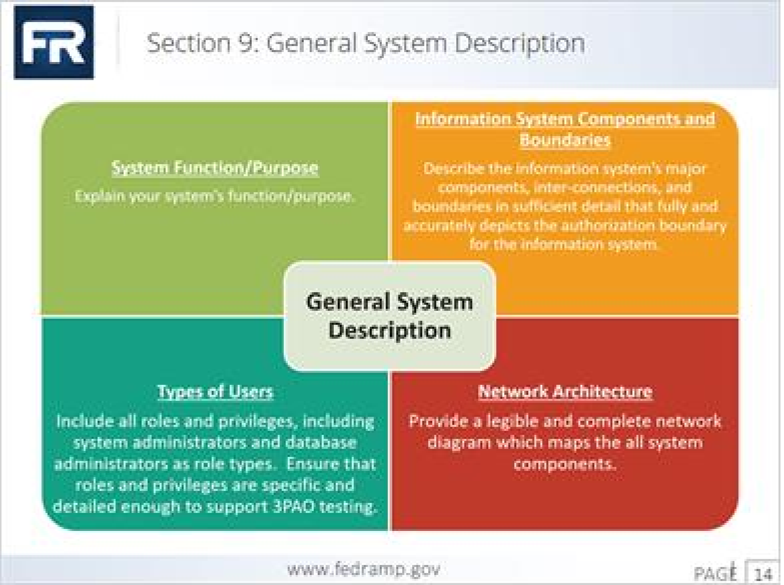
Pick an information system acronym and use it consistently throughout the document.

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
T**ext**
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

- **Audio**
  In Sections 1 through 8 you are responsible for Identifying the system. Who owns it and what does it do. Fill in the blanks with the most accurate information.
  Keep in mind though that the SSP is a living document and will change from time to time. However, 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.
  Before you begin to fill out any section of the SSP, read the instructions, as key details tend to be overlooked.
  Pick an information system acronym and use it consistently throughout the document.
  And, lastly, Do NOT manipulate the template in any way, shape, or form. You may add sections if you feel it better helps tell your story or highlight important information, but don't remove anything. If you have questions email info@fedramp.gov.

1.14 Section 9: General System Description



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.

www.fedramp.gov

PAGE 14

Notes:

Transcript

Section 9: General System Description

Image
General System Description quad graphic: System Function/Purpose; Information System Components and Boundaries; Network Architecture; Types of Users
Text
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.
Network Architecture: Provide a legible and complete network diagram which maps the all system components.
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.
System Function/Purpose: Explain your system's function/purpose
Au**dio**
The general System Description section contains some of the most important parts of the SSP in terms of defining the roles of the system's users, defining the system boundary, and describing the system architecture.

Sy**stem Function/Purpose**
Pretty straight forward but here, focus on providing specific details. What does it do? Who does it serve? What is it all about? The more information that you can provide here will help provide context behind the next three subsections.

S**ystem Components and Boundaries**
System boundary is a very critical concept for cloud security models and impacts the risk authorization levels for FedRAMP assessment.
Here provide a walk through of the system boundary in your environment that you are seeking authorization for. Think of it as giving a tour and explaining what the system components do to perform all intended functions securely, this is the place to explain that in detail.
Provide an understanding of which IT assets fit within the boundary.
Interconnections: indicate and label interconnections and interfaces to other systems
Make sure the components within the defined boundary is consistent with hardware & software inventory. You can name it whatever you want but keep it the same throughout.
Make sure the diagrams are consistent with boundary descriptions
Keep in mind, the components, interconnections, and boundaries described here must be consistent with other hardware, software, network, and interconnection inventories below and throughout the SSP.
Critical components supporting the cloud system must be included in the boundary if they protect the confidentiality, integrity and availability of the system and data
Access points such as jump servers or entry/exit points must be defined and accounted within the boundary.

In addition to the authorization boundary, there are spaces for network diagrams, data flow diagrams, and other graphical depictions of your system.
It is absolutely imperative that the components (hardware, software, network, and data flow) documented in your CSP's diagrams be documented in the corresponding lists and in your system description. The system description, architecture diagram, authorization boundary diagram, network diagram, and data flow diagram are e**x**amined and scrutinized carefully to ensure consistency throughout the SSP and other documents to which this information is propagated. If an error is found, the documents will be returned to the CSP to be corrected. To recap, the system description must be consistent with the CSPs system detailing the same components documented in the hardware, software, and network inventories. The information here will also be preceded in applicable controls for testing.

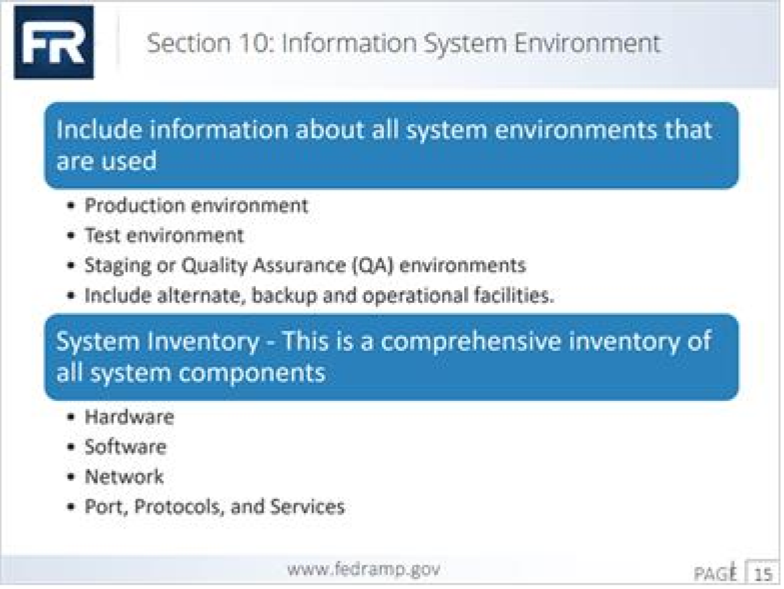
Ty**pes of Users**
This portion of the SSP focuses on the types of users involved with your CSP's system. This section needs to reflect those members of your team with particular roles and responsibilities for the system.

A few tips:
The responsibilities must be detailed.
The roles documented in the table must be the same roles documented in the 'Control Summary Information' section. There can be more than one role in the 'Control Summary Information' section, if applicable.
The roles documented in the table with the corresponding responsibilities must be consistent within the implementation statements.
Identify teams before addressing Types of Users; for example Change Control Board and Incident Response/Contingency Plan Teams
Also, include roles outside of direct access to the system, for example ISSOs and CIOs

Ne**twork Architecture**
The description of the boundary is continued in the Network Architecture section of the SSP. This section asks for network diagrams to describe of the system's architecture. Make sure the diagrams include an example of all components named in the description of the boundary and that naming conventions are

consistent. Ensure that the following items are labeled on the diagram: hostnames, DNS servers, authentication and access control servers, directory servers, firewalls, routers, switches, database servers, major applications, Internet connectivity providers, telecom circuit numbers, and network numbers/VLANs. Major security components should also be represented. If necessary, include multiple network diagrams. Assessors should be able to easily map hardware, software, and network inventories back to this diagram.

1.15 Section 10: Information System Environment



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

www.fedramp.gov

PAGE 15

Notes:

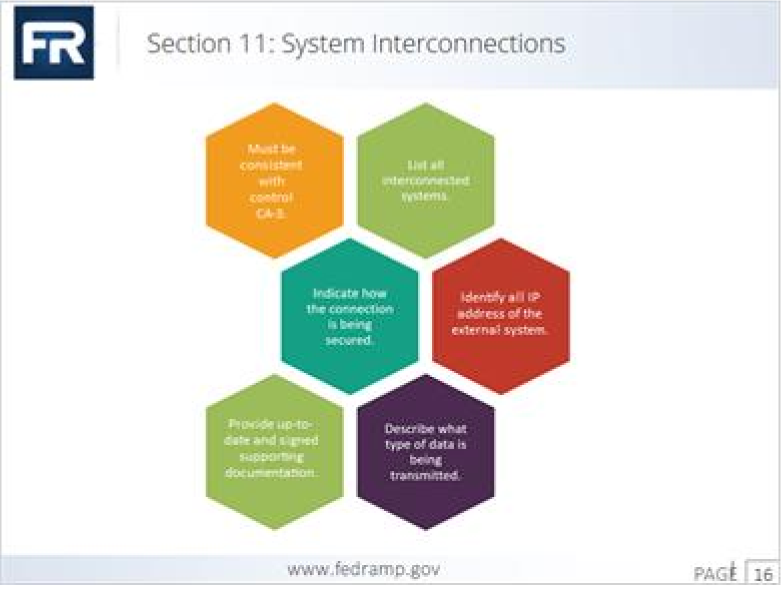
Transcript

Section 10: Information System Environment

Image
<N/A>
T**ext**
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
A**udio**
Section 10 asks for a detailed, technical description of the system environment (Production, test, staging or QA environments used in the system). Test and Staging environments should be mentioned to inform that you have them but, details about them (inventory, architecture) are not required unless included in the authorization boundary. Typically, they are not.
This section also asks for detailed inventories of hardware, software, network devices and components;

and ports, protocols, and services. It's key that these inventories are detailed and comprehensive. Missing components or simply not providing an inventory is a show stopper during the review of the System Security Plan. Once again, make sure the names used for components are consistent with the boundary description and the network diagrams. Section 10 also asks the CSP to provide a data flow diagram which maps the flow of data in and out of the boundaries. While this diagram focuses on illustrating the flow of data rather than the network topology, some network components of the system's network topology need to be included in order to illustrate the direction on how the network traffic flows through the system.

1.16 Section 11: System Interconnections



Section 11: System Interconnections

Must be consistent with control CA-3.

List all interconnected systems.

Indicate how the connection is being secured.

Identify all IP address of the external system.

Provide up-to-date and signed supporting documentation.

Describe what type of data is being transmitted.

www.fedramp.gov

PAGE 16

Notes:

Transcript

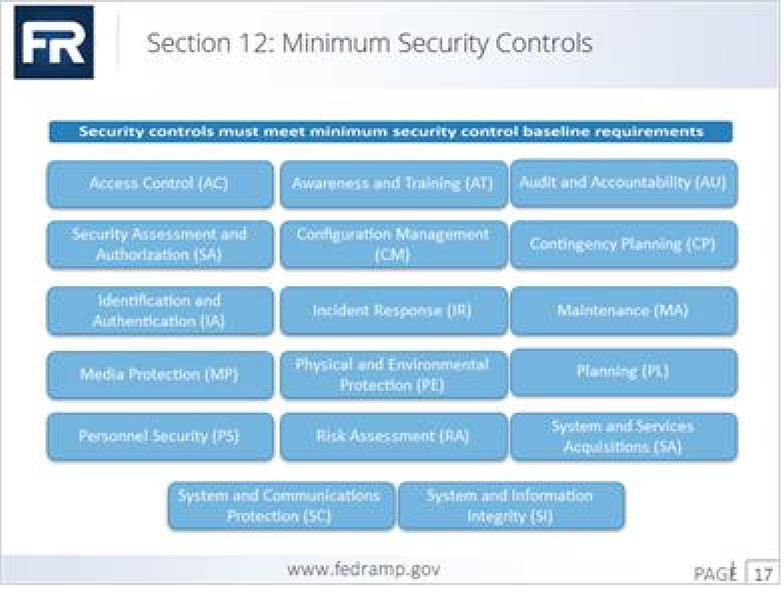
Section 11: System Interconnections

Image

- One large image of six interconnected smaller diagrams placed together as one
  T**ext**
  Must be consistent with control CA-3.
  List all interconnected systems.
  Indicate how the connection is being secured.
  Identify all IP address of the external system
  Provide up-to-date and signed supporting documentation
  Describe what type of data is being transmitted.
  A**udio**
  Section 11 continues with detailing the system boundary by providing a complete inventory of system interconnections. Interconnections describe connected systems that are outside the system boundary.
  List all interconnected systems.
  Provide the IP address and interface identifier for the CSP system that provides the connection.
  Name the external organization and the IP address of the external system.
  Indicate how the connection is being secured.
  For Data Direction, indicate which direction the packets are flowing.

For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number.
This table must be consistent with CA-3.
Make sure all Interconnection Security Agreements (ISA), Memorandum of Understanding (MOU), Service Level Agreements (SLA) clearly define roles and responsibilities, are up to date, and are signed by both parties.

1.17 Section 12: Minimum Security Controls



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)

www.fedramp.gov

PAGE 17

Notes:

Transcript

Section 12: Minimum Security Controls

Image

One large image of 17 interconnected smaller diagrams placed together as one
Text
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)

Audio

Security control baseline requirements as defined by NIST 800-53A Rev 4. Upon categorizing a system as Low, Moderate, or High sensitivity in accordance with FIPS 199, the appropriate security control baseline standards are applied. Some of the control baselines have enhanced controls which are indicated in parenthesis.

Guidance on how to describe the implemented standard can be found in NIST 800-53, Rev 4. Control enhancements are marked in parenthesis in the sensitivity columns.

The System Security Plan template includes the stated NIST control or enhancement requirement and a security control summary information table that CSPs must fill out to detail how the CSP meets the requirements of that control and for each enhancement. Each control has a Control Implementation Summary

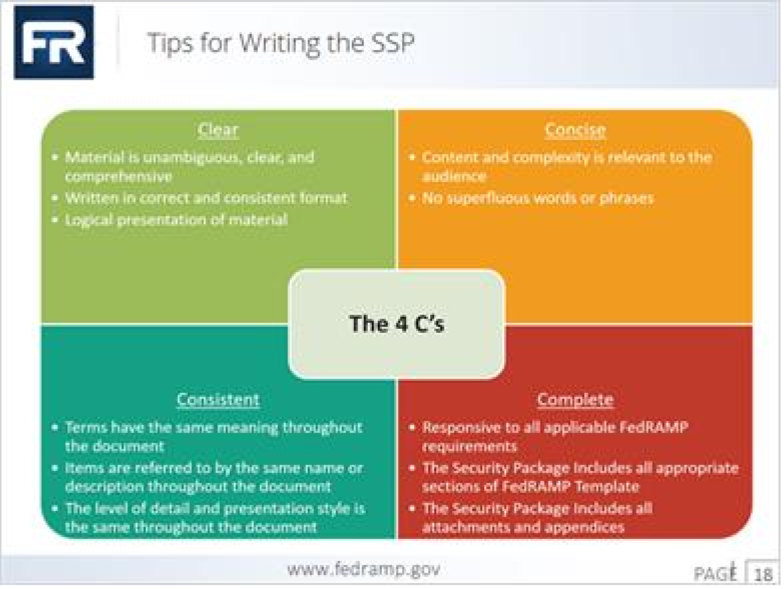
First, you'll have to name the Responsible Role for the control. - this is the staff responsible for maintaining and implementing the control - this is not a staff person's name, but rather a role that is identified to be responsible - e.g. System Engineer - and this role must align with stated roles and positions in the defined User Roles.

Next is parameter for the control - e.g. usually a frequency, such as number of days or length of time. Next is the implementation status for the control - this is where you detail whether the control is implemented, partially implemented, planned, if there is an alternate implementation or if the control is not implemented. Next, you detail the control origination - this is where you state who has the responsibility for implementing and managing the control. This responsibility may be assigned to the CSP, the customer, or be a shared responsibility. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage, and monitor the control.

The System Security Plan supplies a control origination table which provides the values for defining the control origination. The table includes the Control origination, the definition and an example. Service Provider Corporate refers to a control that originates from the CSP corporate network. Service Provider System Specific refers to a control specific to a particular system at the CSP and the control is not part of the standard corporate controls. Service Provider Hybrid refers to a control that makes use of both corporate controls and additional controls specific to a particular system at the CSP. Configured by Customer refers to a control where the customer needs to apply a configuration in order to meet the control requirement. Provided by Customer refers to a control where the customer needs to provide additional hardware or software in order to meet the control requirement. Shared refers to a control that is managed and implemented partially by the CSP and partially by the customer. Inherited from pre-existing Provisional Authorization refers to a control that is inherited from another CSP system that has already received a Provisional Authorization. None of the dash 1 controls (AC-1, AU-1, SC-1 etc.) can be inherited because these are policy controls and all CSPs need to have their own set of security policies.

Finally, you need to describe what the solution is, and how it is implemented. Here is where you must provide enough detail to adequately allow reviewers to understand exactly what it is you do to meet this security control providing enough information so an assessor will understand how the control meets the requirements. If you are using a Commercial Office the Shelf product to satisfy a control requirement, name the product and the version number and briefly state how it works. Simply stating that you meet the requirement or a one sentence description will not be enough information.

1.18 Tips for Writing the SSP



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

www.fedramp.gov

PAGE 18

Notes:

Transcript

Tips for Writing

Image

One large image of 4 interconnected smaller diagrams placed together as one:

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

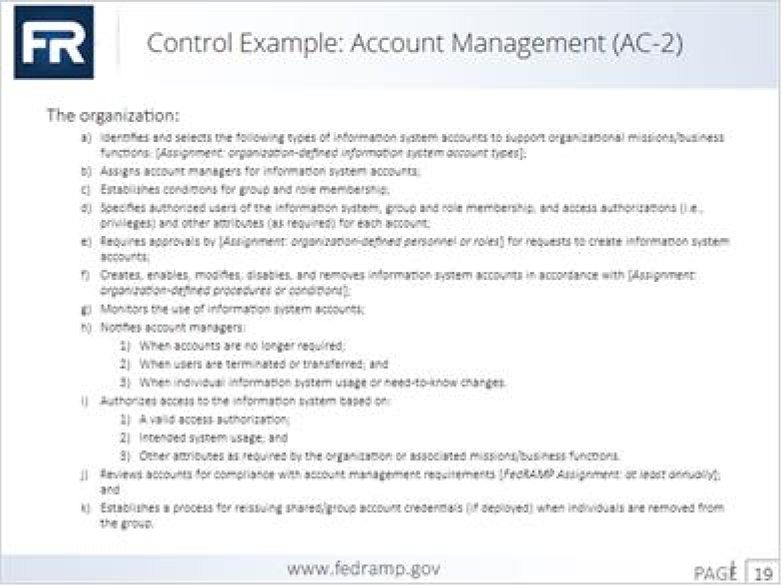
Complete: Responsive to all applicable FedRAMP requirements; The Security Package Includes all appropriate sections of FedRAMP Template;

The Security Package Includes all attachments and appendices
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
T**ext**
One large image of 4 interconnected smaller diagrams placed together as one:
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
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
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
Au**dio**
Tips for writing. As I mentioned before we are going to review the 4C's of writing a quality SSP.

This review is meant as general document acceptance criteria. It does not include technical review criteria used by ISSOs and JAB TRs to assess the technical quality of documents.
Clear, Concise, Consistent, and Complete. These will be the key points that the FedRAMP PMO will look for when you submit your Security Package. If these points are not met then the documents will not be accepted and the CSP will be asked to make updates.
Clear - straightforward, avoiding convoluted phrases or over-long phrases;
Concise - pack the most meaning into your words;
Consistent - Ensure terms have the same meaning throughout the document and items are referred to by the same name or description. The level of detail and presentation style should also remain the same throughout the document; and finally,
Complete - Be responsive to all applicable FedRAMP requirements and include all appropriate sections of the FedRAMP templates

1.19 Control Example: Account Management (AC-2)



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.

www.fedramp.gov

PAGE 19

Notes:

Transcript

Control Example: Account Management (AC-2)

Image

N/A

Text

- Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];
- Assigns account managers for information system accounts;
- Establishes conditions for group and role membership;

- 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;
- Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;
- Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];
- Monitors the use of information system accounts;
- Notifies account managers:
  - When accounts are no longer required;
  - When users are terminated or transferred; and
  - When individual information system usage or need-to-know changes.
- Authorizes access to the information system based on:
  - A valid access authorization;
  - Intended system usage; and
  - Other attributes as required by the organization or associated missions/business functions.
- Reviews accounts for compliance with account management requirements [*FedRAMP Assignment: at least annually*]; and

Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

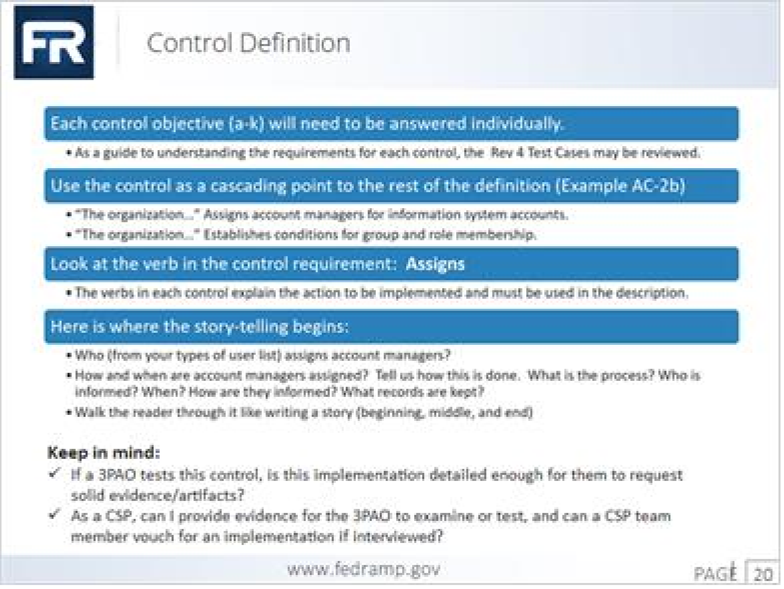
A**udio**

Let's look at an example of a control in the Access Control family. AC 2 addresses Account Management. It is the CSPs responsibility to describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage, and monitor the control. In some cases, the responsibility is shared by a CSP and by the customer.

With regards to Account Management specifically, Information system account types include, for example, individual, shared, group, system, temporary, and service. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability.

So, let's look further at how to specifically write to this control.

1.20 Control Definition



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?

www.fedramp.gov

PAGE 20

Notes:

Transcript

Control Definition

Image

N/A

Text

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?

Audio

Let's break the example of AC-2 down to a basic form.

First, each control objective (a-k) will need to be answered individually.

- As a guide to understanding the requirements for each control, the NIST SP 800-53 Rev 4 Test Cases may be reviewed.

Use the control as a cascading point to the rest of the definition

- “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.

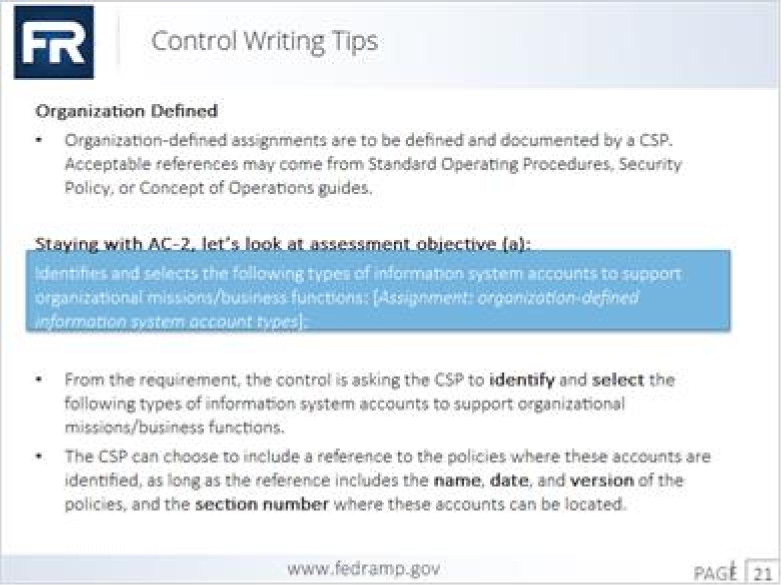
Here is where the story-telling begins:

- 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

A 3PAO must be able to test this control and examine the evidence provided by the CSP.

1.21 Control Writing Tips



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.

www.fedramp.gov

PAGE 21

Notes:

Transcript

Title

Control Writing Tips

Image

N/A.

Text

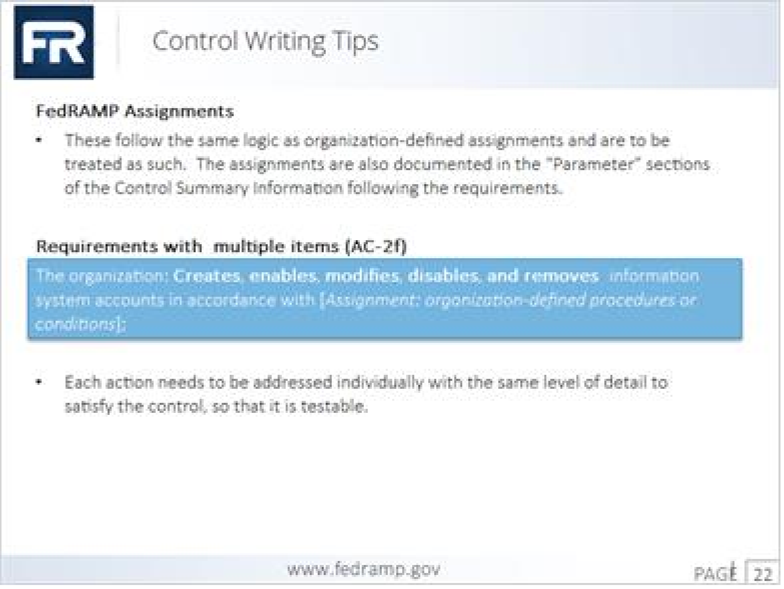
Let’s review what is meant by Organization defined assignments and use AC-2 objective (a) as an example. In this case the control is asking the CSP to Identifies and selects the following types of information system accounts to support organizational missions/business functions.

This definition and assignment may come from SOPs, Policy Documents, or ConOps guides.

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.

1.22 Control Writing Tips



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.

www.fedramp.gov

PAGE 22

Notes:

Transcript

Title

Control Writing Tips

Image

N/A.

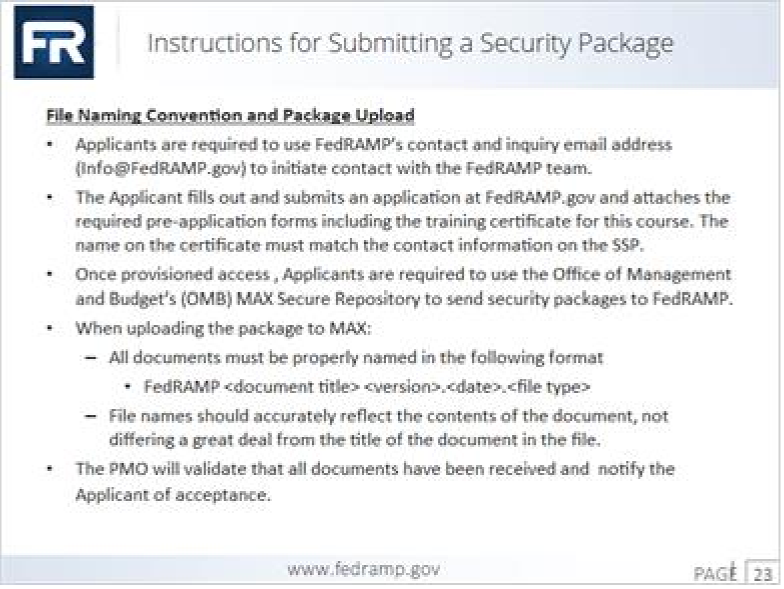
Text

FedRAMP Assignments follow the same logic as organization-defined assignments. The assignments are also documented in the “Parameter” sections of the Control Summary Information following the requirements.

When multiple requirements are presented as in the case with AC-2 objective (f) each action needs to be addressed individually with the same level of detail to satisfy the control, so that it is testable.

Make sure that you write to the how and why for how your organization Creates System Accounts, Enables System Accounts, Modifies System Accounts, Disables System Accounts and Removes System Accounts.

1.23 Instructions for Submitting a Security Package



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.

www.fedramp.gov

PAGE 23

Notes:

Transcript

Title

Instructions for Submitting a Security Package

Image

N/A.

Text

Ok… so now you are done with your documentation, it has been checked and rechecked against FedRAMP Quality Standards and you are ready to apply for a FedRAMP authorization. What do you do now? Well, first remember, that you must present the training certificate from this course to the FedRAMP PMO and the name on the certificate must match the point of contact on the SSP. Complete this training by passing the course exam and filling out the course survey. Both of these modules are located in the home screen of the course on the blackboard platform. Once both modules have been completed your training certificate will be made available for printing or download.

When you are ready to submit your documentation fill out and submit your application at FedRAMP.gov and attach the required pre-application forms including the training certificate for this course.

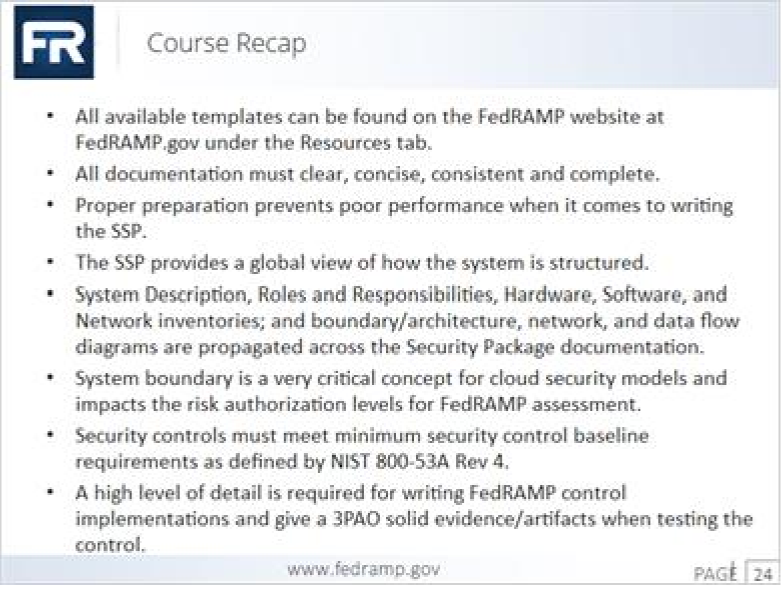
The FedRAMP PMO will confirm receipt of your application and provision the CSP access to the OMB MAX Security Repository. When uploading the package to MAX:

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.

Once the documents have been uploaded the FedRAMP PMO will validate that all documents have been received and accepted.

1.24 Course Recap



Course Recap

- All available templates can be found on the FedRAMP website at FedRAMP.gov under the Resources tab.
- All documentation must 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.

www.fedramp.gov

PAGE 24

Notes:

Transcript

Title

Course Recap

Image

N/A.

Text

We hope you have enjoyed this course and have found the content to be helpful as you prepare for a FedRAMP Assessment. 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… and the 5 P’s, proper preparation prevents poor performance

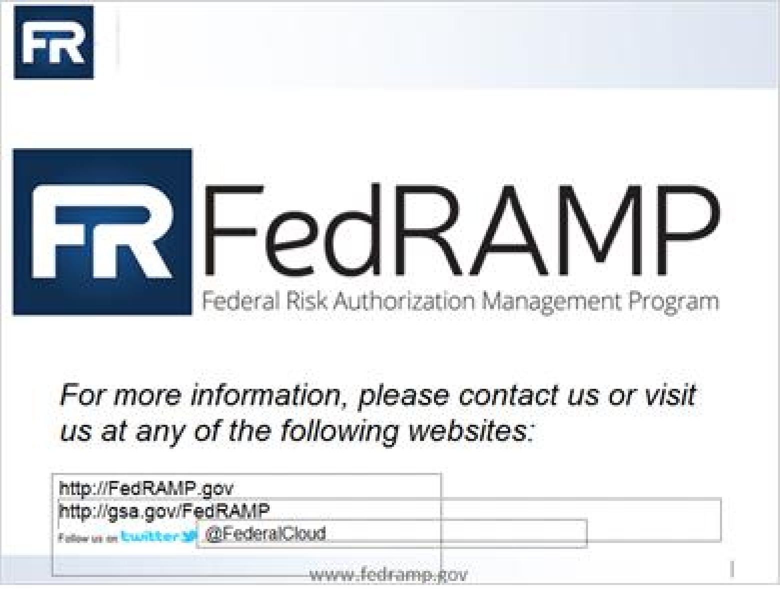
The SSP provides a global view of how the system is structured and is the focal point for all FedRAMP documentation but other documents that are provided along with the SSP have direct impact on the structure and content provided in the SSP.

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.

1.25 Untitled Slide



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

www.fedramp.gov

Notes:

Transcript

Title <N/A>

Image

Image of FedRAMP logo.

Text

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

http://FedRAMP.gov

http://gsa.gov/FedRAMP

@FederalCloud

References

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