FedRAMP Security Assessment Plan (SAP) Training

1. FedRAMP_Training_SAP_v6_508

1.1 FedRAMP Online Training: SAP Overview Splash Screen

FedRAMP Online Training

Security Assessment Plan (SAP) Overview

12/9/2015

Presented by: FedRAMP PMO

www.fedramp.gov

Select the Next button to begin

Notes:

Transcript

Title <N/A>

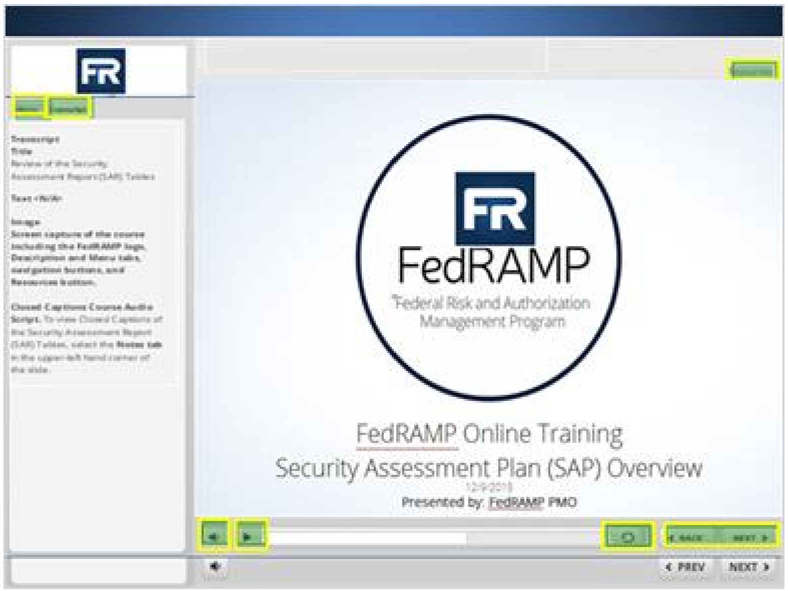
Image

Image of FedRAMP logo.

Text

FedRAMP Online Training; Security Assessment Plan (SAP) Overview. Presented by: FedRAMP PMO.

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
12/9/2018
Presented by: FedRAMP PMO

Notes:

Transcript

Title

Course Features and Functions

Text

<N/A>

Image

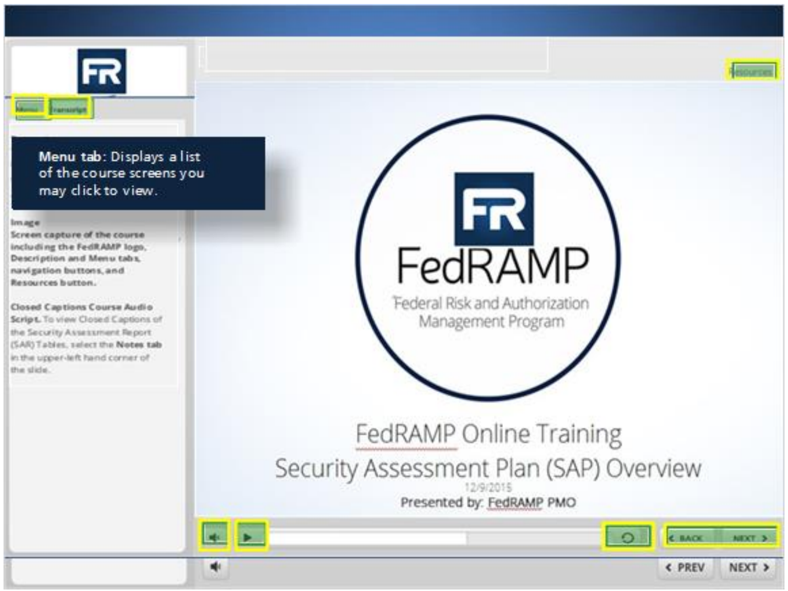
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

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.

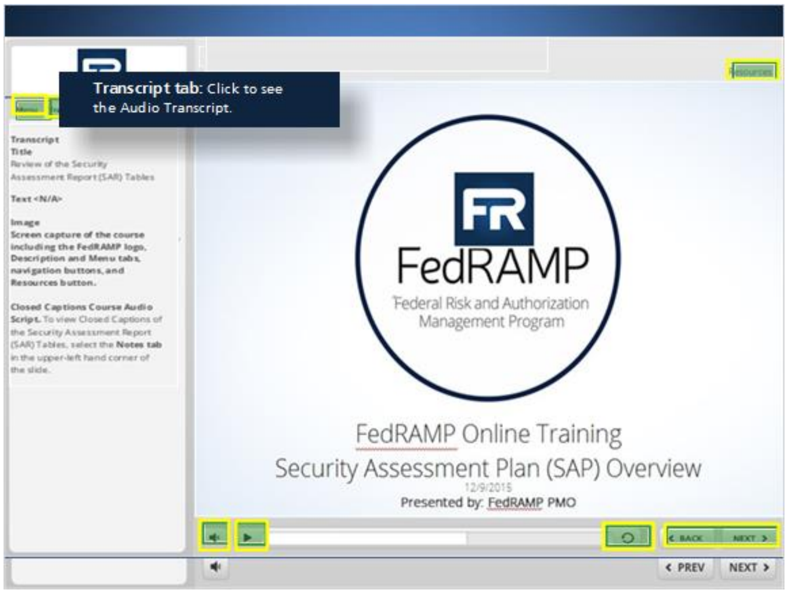
Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

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>

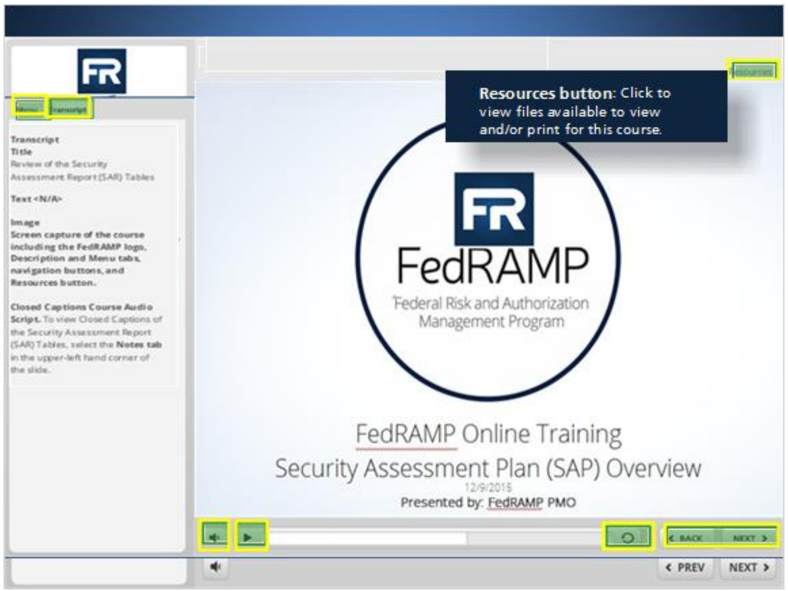
Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

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>

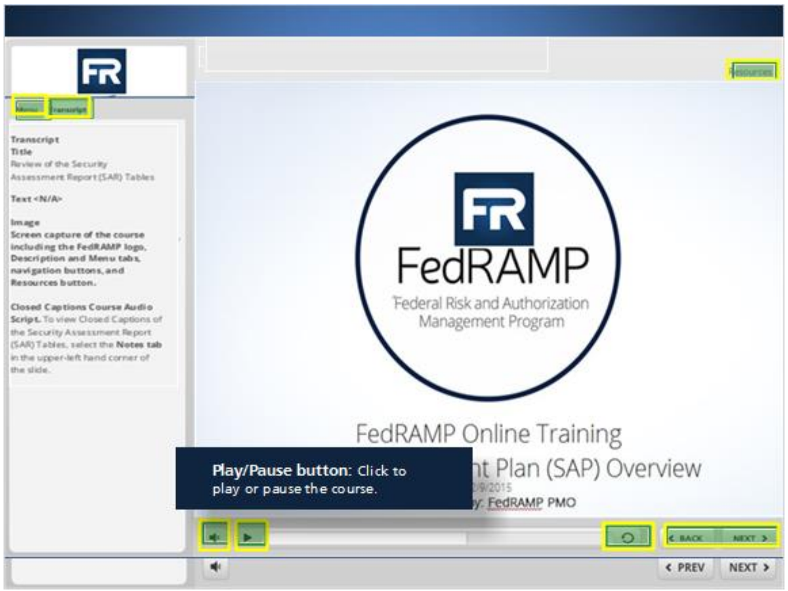
Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

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 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>

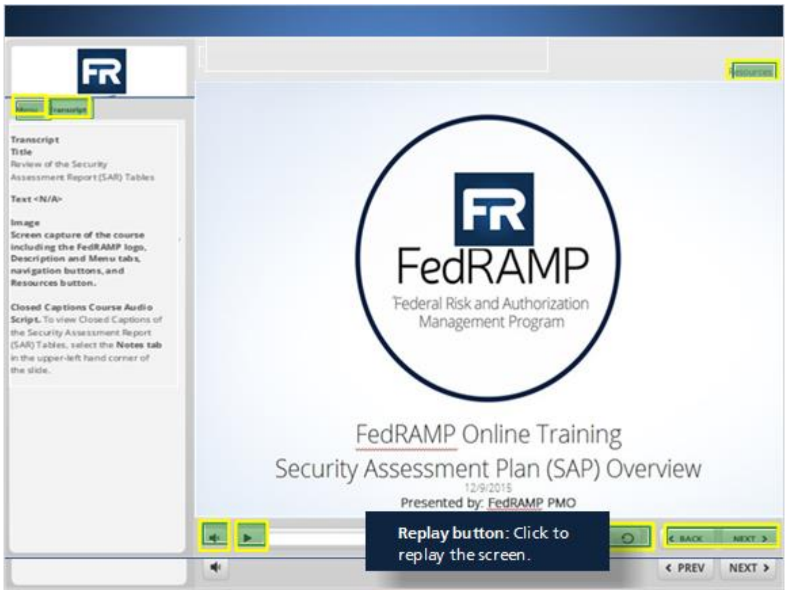
Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

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.

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

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

Replay (Slide Layer)



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

Text <N/A>

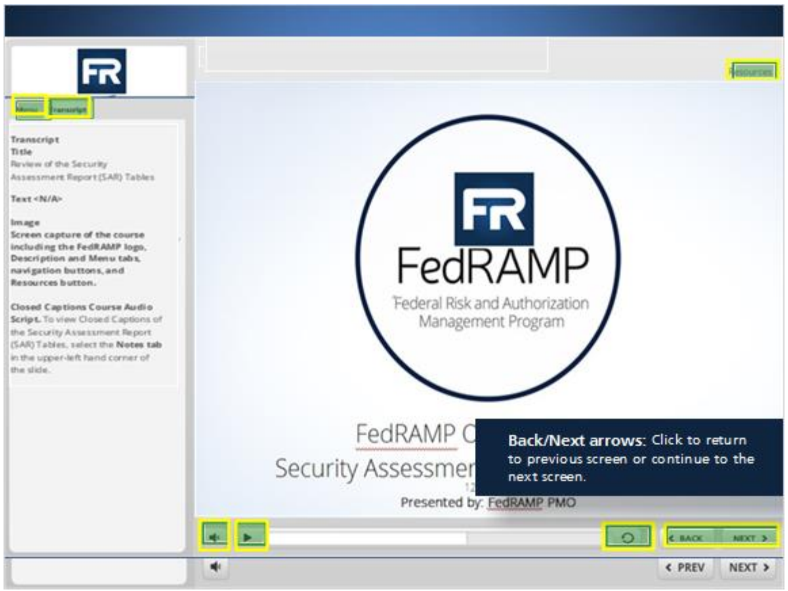
Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

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>

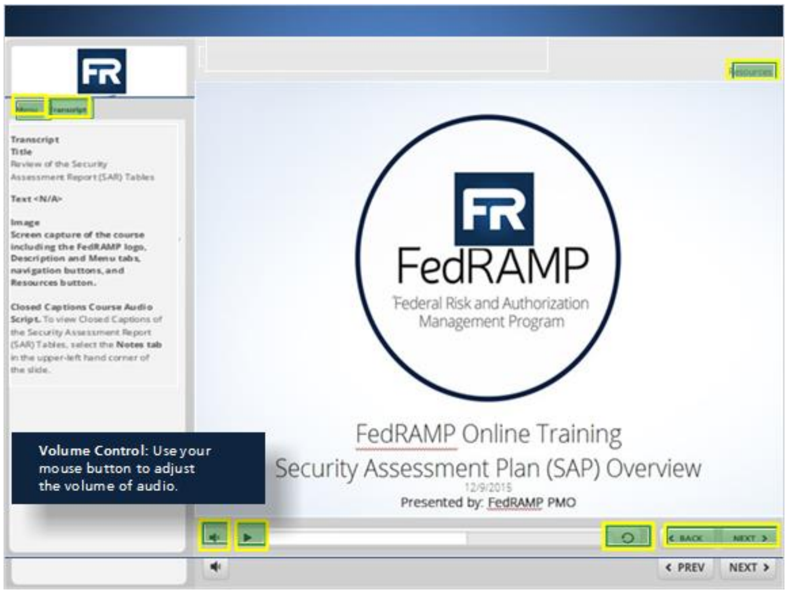
Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

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 C
Security Assessmen
12
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>

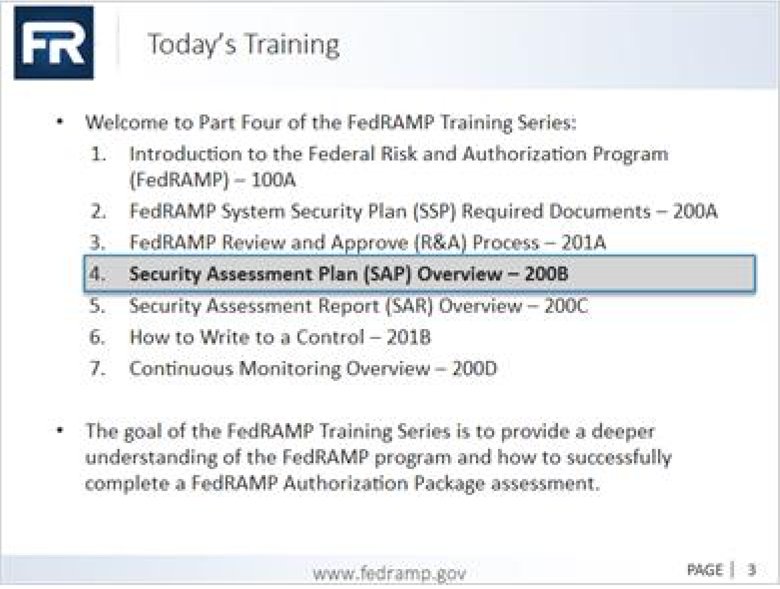
Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

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.

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

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

1.3 Today's Training



Today's Training

- Welcome to Part Four 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 (R&A) Process – 201A
  4. **Security Assessment Plan (SAP) Overview – 200B**
  5. Security Assessment Report (SAR) Overview – 200C
  6. How to Write to a Control – 201B
  7. Continuous Monitoring Overview – 200D
- The goal of the FedRAMP Training Series is to provide a deeper understanding of the FedRAMP program and how to successfully complete a FedRAMP Authorization Package assessment.

www.fedramp.gov

PAGE | 3

Notes:

Transcript Title

Today's Training

Image

<N/A>

Text
Welcome to Part Four of the FedRAMP Training Series:

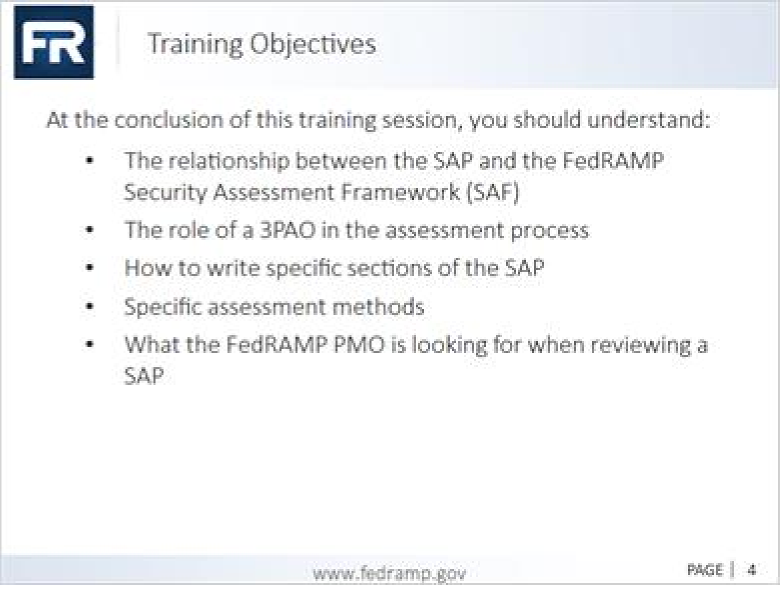
1. Introduction to the Federal Risk and Authorization Program (FedRAMP) - 100A
2. FedRAMP System Security Plan (SSP) Required Documents - 200A
3. FedRAMP Review and Approve (R&A) Process - 201A
4. **Security Assessment Plan (SAP) Overview - 200B**
5. Security Assessment Report (SAR) Overview - 200C
6. How to Write to a Control - 201B
7. Continuous Monitoring Overview - 200D

The goal of the FedRAMP Training Series is to provide a deeper understanding of the FedRAMP program and how to successfully complete a FedRAMP Authorization Package assessment.

Audio
Welcome to the FedRAMP online training series. I am <name> your instructor for this training.

In this course, we're going to talk about the Security Assessment Plan or SAP. The FedRAMP PMO developed this training series to help FedRAMP CSP applicants properly prepare for a FedRAMP assessment by providing a deeper understanding of the program and the level of effort (LOE) required to satisfactorily complete a FedRAMP assessment. This training module is tailored to a CSP going through the JAB path and using a third-party assessment organization or 3PAO by providing insight into what to expect when going through the FedRAMP assessment process, we want to ensure CSPs have the knowledge and resources to successfully achieve FedRAMP authorization.

1.4 Training Objectives



Training Objectives

At the conclusion of this training session, you should understand:

- The relationship between the SAP and the FedRAMP Security Assessment Framework (SAF)
- The role of a 3PAO in the assessment process
- How to write specific sections of the SAP
- Specific assessment methods
- What the FedRAMP PMO is looking for when reviewing a SAP

www.fedramp.gov PAGE | 4

Notes:

Transcript Title

Training Objectives

Image

<N/A>

Text
At the conclusion of this training session the you should understand:

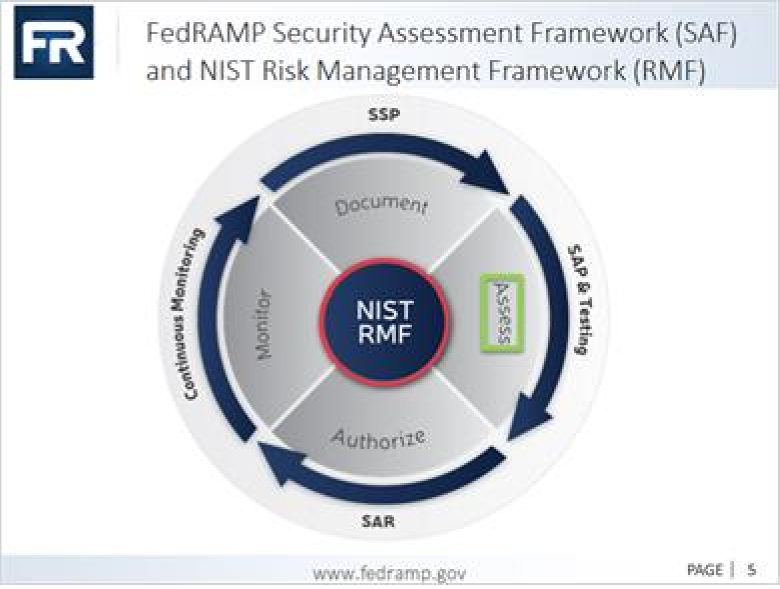
- The relationship between the SAP and the FedRAMP Security Assessment Framework (SAF)
- The role of a 3PAO in the assessment process
- How to write specific sections of the SAP
- Specific assessment methods
- What the FedRAMP PMO is looking for when reviewing a SAP

Audio
Welcome to Part Four of the FedRAMP Training Series:

At the conclusion of this training session, you should understand:

- the relationship between the SAP and the FedRAMP security assessment framework
- the role of the 3PAO in the assessment process
- how to write to each section of the SAP
- specific assessment methods
- and….what the FedRAMP PMO is looking for when reviewing a SAP.

1.5 FedRAMP SAF and NIST RMF



Notes:

Transcript Title

FedRAMP SAF and NIST Risk Management Framework (RMF)

Image

NIST RMF with designations on Document, Assess, Authorize, Monitor

Text

<N/A>

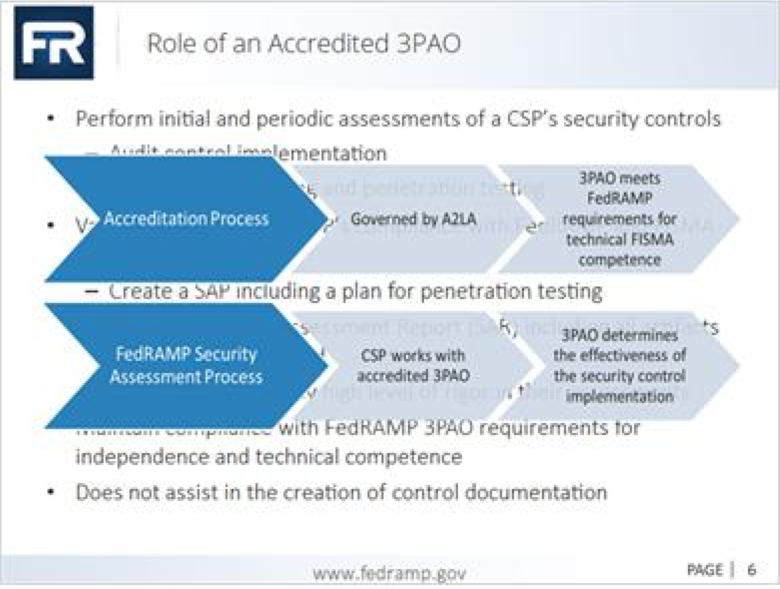
Audio

Federal agencies are required to assess and authorize information systems in accordance with FISMA. The FedRAMP---Security Assessment Framework---or SAF is compliant with FISMA and is based on the NIST RMF. In fact, FedRAMP uses the same documents and deliverables that NIST requires agencies to use. however, FedRAMP simplifies the NIST RMF by creating four process areas that encompass the 6 steps within 800-37 rev 1: Document, Assess, Authorize, and Monitor.

In this training module, we will focus on the Assess phase of the SAF, which includes SAP documentation and testing.

In the Assess phase - CSPs must use an independent assessor or 3PAO to test the information system to demonstrate that the controls are effective and implemented as documented in the SSP. This assessment starts with documenting the methodology and process for testing the control implementation in the Security Assessment Plan (SAP). The 3PAO will execute testing against the SAP using appropriate assessment procedures to determine the extent to which the controls are meeting the security requirements for the system. The results of this testing and recommendations for mitigating risk are documented in the Security Assessment Report or SAR.

1.6 Role of a 3PAO



Role of an Accredited 3PAO

- Perform initial and periodic assessments of a CSP's security controls
  - Audit control implementation
  - Create a SAP including a plan for penetration testing
- with FedRAMP 3PAO requirements for independence and technical competence
- Does not assist in the creation of control documentation

Accreditation Process → Governed by A2LA → 3PAO meets FedRAMP requirements for technical FISMA competence

FedRAMP Security Assessment Process → CSP works with accredited 3PAO → 3PAO determines the effectiveness of the security control implementation

www.fedramp.gov

PAGE | 6

Notes:

Transcript Title

Role of an Accredited 3PAO

Image

Map of Accreditation Process and FedRAMP Security Process

Text

Perform initial and periodic assessments of a CSP's security controls

- Audit control implementation
- Vulnerability scanning and penetration testing

Validate and attest to a CSP's compliance with FedRAMP and FISMA requirements

- Create a SAP including a plan for penetration testing
- Create a Security Assessment Report (SAR) including all artifacts and evidence collected
- Provide a consistently high level of rigor in their assessments

Maintain compliance with FedRAMP 3PAO requirements for independence and technical competence

Does not assist in the creation of control documentation

Audio

Accredited third party assessor organizations (3PAO) play a critical role in the FedRAMP Security Assessment Process. Accredited 3PAOs have demonstrated independence and technical competency required to testing the security implementations and collect representative evidence. The resulting Security Assessment Report (SAR) and supporting evidence make up a key requirement for leveraging agencies to use FedRAMP security assessment packages.

The accreditation process for 3PAOs is governed by the American Association for Laboratory Accreditation or A2LA and is based on the concept of conformity assessment--a methodology to demonstrate capability in meeting requirements relating to a product, process, system, person or body. For FedRAMP, the conformity assessment ensures that accredited 3PAOs consistently perform security assessments with the appropriate level of rigor and independence. accredited 3PAOs are required to meet FedRAMP requirements for technical FISMA competence through demonstrated expertise in assessing cloud-based solutions.

In the FedRAMP security assessment process, once the SSP has been approved, the 3PAO begins working with the CSP. The 3PAO performs and independently tests the CSP's system to determine the effectiveness of the security control implementation.

The role of the 3PAO within FedRAMP is to:

Perform initial and periodic assessments of the CSP's security controls

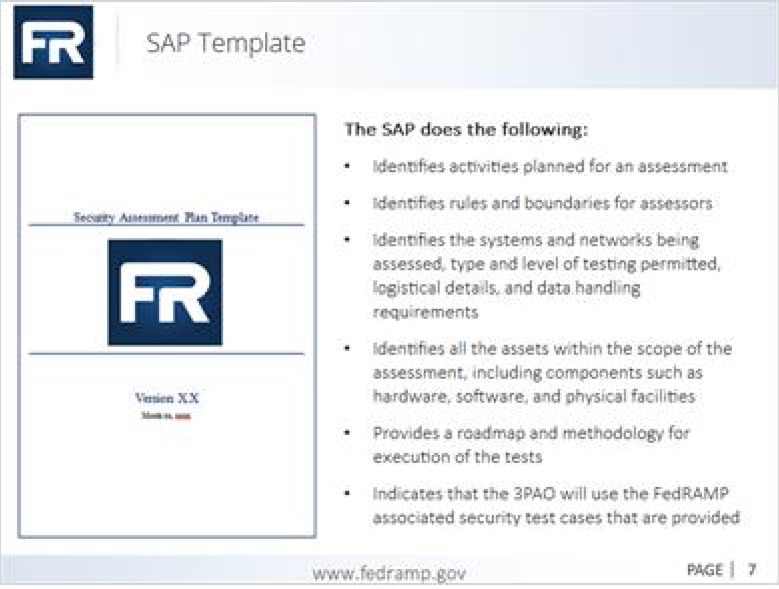
- Audit control implementation
- Vulnerability and penetration testing

Validate and attest to the CSPs compliance with FedRAMP and FISMA requirements

- Create a Security Assessment Plan including plan for penetration testing
- Create Security Assessment Report including all artifacts and evidence collected
- Provide a consistently high level of rigor in assessment

Maintain compliance with FedRAMP 3PAO requirements for independence and technical competence.

1.7 SAP Template



SAP Template

Security Assessment Plan Template

Version XX

The SAP does the following:

- Identifies activities planned for an assessment
- Identifies rules and boundaries for assessors
- Identifies the systems and networks being assessed, type and level of testing permitted, logistical details, and data handling requirements
- Identifies all the assets within the scope of the assessment, including components such as hardware, software, and physical facilities
- Provides a roadmap and methodology for execution of the tests
- Indicates that the 3PAO will use the FedRAMP associated security test cases that are provided

www.fedramp.gov

PAGE | 7

Notes:

Transcript Title

SAP Template

Image

Security Assessment Plan Template cover

Text

The SAP does the following:

- Identifies activities planned for an assessment
- Identifies rules and boundaries for assessors
- Identifies the systems and networks being assessed, type and level of testing permitted, logistical details, and data handling requirements
- Identifies all the assets within the scope of the assessment, including components such as hardware, software, and physical facilities
- Provides a roadmap and methodology for execution of the tests
- Indicates that the 3PAO will use the FedRAMP associated security test cases that are provided
-

Audio

Security assessments are complex activities because of organizational requirements, the amount and type of systems, technical techniques used, and the logistics. security assessments can be simplified and associated risks reduced through an established, repeatable planning process. the SAP helps by ensuring that testing activities are clearly documented.

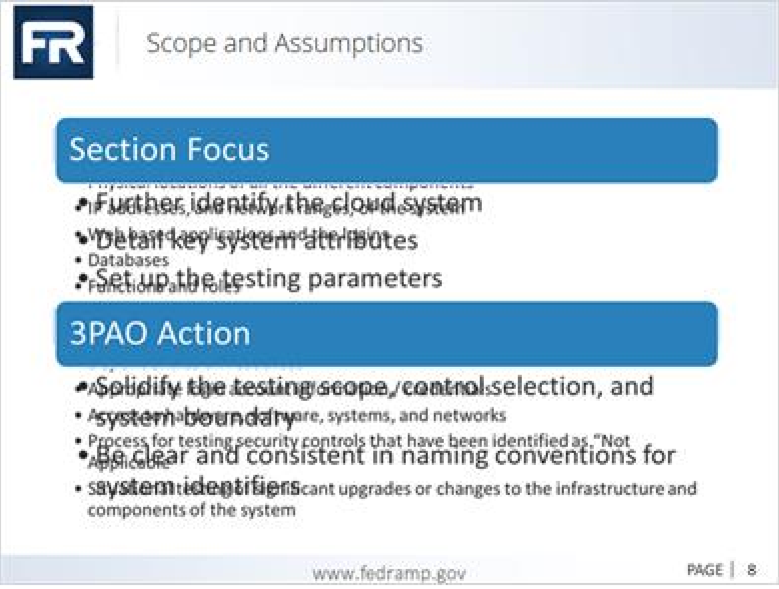
In the FedRAMP process, the 3PAO creates a testing plan using the FedRAMP Security Assessment Plan (SAP) template.

The SAP template assists with providing the right level of detail to properly prepare for testing--- and documents:

- Activities planned for an assessment and the rules and boundaries for assessors.
- Identifies the systems and networks being assessed, the type and level of testing permitted, logistical details, and data handling requirements.
- Identifies all the assets within the scope of the assessment, including components such as hardware, software, and physical facilities.
- Provides a roadmap and methodology for execution of the tests and indicates that the 3PAO will use the FedRAMP associated security test cases that are provided in the form of worksheets.

The FedRAMP ISSO reviews and approves the SAP to ensure that the assessment will cover the stated authorization boundary and controls. Once the SAP has been reviewed, the JAB approves the SAP and then the 3PAO performs an assessment of the CSP’s controls in accordance with the SAP. The SAP is divided into six primary sections and four Appendices and we will discuss each one in the upcoming segments to highlight key focus areas.

1.8 Scope and Assumptions



Scope and Assumptions

Section Focus

- Further identify the cloud system
- Detail key system attributes
- Set up the testing parameters

3PAO Action

- Solidify the testing scope/control selection, and system boundary
- Be clear and consistent in naming conventions for system identifiers

www.fedramp.gov

PAGE | 8

Notes:

Transcript Title

Scope and Assumptions

Image

Section Focus and 3PAO Action

Text

Section Focus

- Further identify the cloud system
- Detail key system attributes
- Set up the testing parameters
- 3PAO Action
- Solidify the testing scope/control selection, and system boundary
- Be clear and consistent in naming conventions for system identifiers

Audio

The sections that note the scope and assumptions of the assessment further identify the cloud system, detail key system attributes, and help set up the testing parameters. It is important here to solidify the testing scope, solidify the control selection, and clearly define the testing boundary, which should match the boundary defined in the SSP. When completing the scope section, the 3PAO should be clear and consistent in naming conventions for system identifiers and be sure to note any references to other documents or dependencies. The scope specifically asks the 3PAO to identify and list the following system attributes:

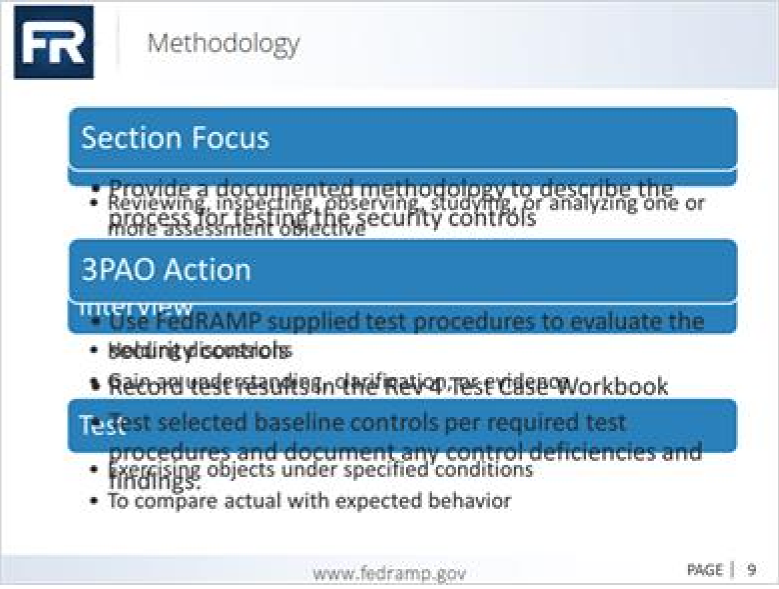
The physical locations of all the different components to be tested

- IP addresses and network ranges
- The various web-based applications that make up the system, and the logins and their associated roles
- Databases slated for testing; and
- Functions and roles that will be tested

For the assumptions section--the 3PAO must list assumptions for each unique engagement. Assumptions may vary from assessment to assessment but should take into consideration:

- Dependencies on resources, including documentation and individuals with knowledge of the systems and infrastructure
- Appropriate login account information / credentials
- Access to hardware, software, systems, and networks defined within the scope
- Process for testing security controls that have been identified as “not applicable”
- Situational testing of significant upgrades or changes to the infrastructure and components of the system

1.9 Methodology



Methodology

Section Focus

- Provide a documented methodology to describe the process for testing the security controls
- Reviewing, inspecting, observing, studying, or analyzing one or more assessment objective

3PAO Action

Interview

- Use FedRAMP supplied test procedures to evaluate the security controls
- Holding discussions
- Gain an understanding, clarification, or evidence
- Record test results in the Rev 4 Test Case Workbook

Test

- Test selected baseline controls per required test procedures and document any control deficiencies and findings.
- Exercising objects under specified conditions
- To compare actual with expected behavior

www.fedramp.gov

PAGE | 9

Notes:

Transcript Title

Methodology

Image

Section Focus, 3PAO Action, Test, Examine, Interview, Test

Text

Section Focus

Provide a documented methodology to describe the process for testing the security controls

3PAO Action

Use FedRAMP supplied test procedures to evaluate the security controls

Record test results in the Rev 4 Test Case Workbook

Test selected baseline controls per required test procedures and document any control deficiencies and findings

Audio

Within the SAP, FedRAMP provides a documented methodology to describe the process for testing the security controls. Independent assessors may add to this section; however, templates cannot be tampered with.

Recommended test procedures are provided by the FedRAMP PMO in the Rev 4 Test Case Workbook. This workbook contains the procedures and methodology for testing based on NIST SP 800-53a, revision 4. 3PAOs use this workbook to test baseline controls and enhancements per required test procedures and document any control deficiencies and findings. The 3PAO needs to address all the controls and requirements and document the results to a level of detail that the test can be replicated by another tester at another time.

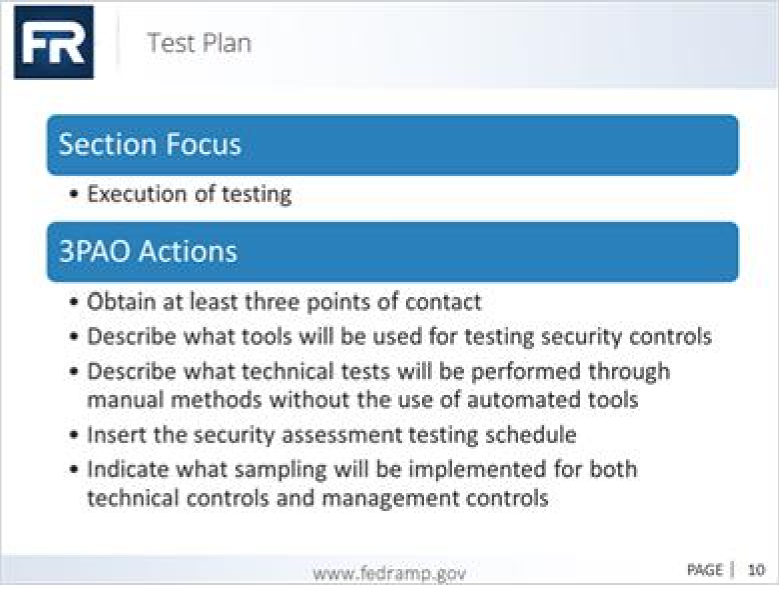
Assessment methods define the nature of the assessor actions and include EXAMINE, INTERVIEW, AND TEST.

Lets start with EXAMINE:

- **Examine**: This method is reviewing, inspecting, observing, studying, or analyzing one or more assessment objectives. for example safeguards and countermeasures, backup operations, monitoring activities, and contingency plans to name a few. the purpose of this method is to gain understanding, clarification, or evidence.
- **Interview**: This method involves holding discussions with individual stakeholders or groups to gain understanding, clarification, or evidence.
- **Test**: This method is exercising system components under specified conditions to compare actual results with expected behavior using automated and manual methods.

Assessment methods should have a set of associated attributes, either depth or coverage, which helps define rigor and scope of the assessment.

1.10 Test Plan



Test Plan

Section Focus

- Execution of testing

3PAO Actions

- Obtain at least three points of contact
- Describe what tools will be used for testing security controls
- Describe what technical tests will be performed through manual methods without the use of automated tools
- Insert the security assessment testing schedule
- Indicate what sampling will be implemented for both technical controls and management controls

www.fedramp.gov

PAGE | 10

Notes:

Transcript Title

Test Plan

Image

Section Focus, 3PAO Actions

Text

Section Focus

- Execution of testing

3PAO Actions

- Obtain at least three points of contact
- Describe what tools will be used for testing security controls
- Describe what technical tests will be performed through manual methods without the use of automated tools
- Insert the security assessment testing schedule
- Indicate what sampling will be implemented fir both technical controls and management controls.

Audio

The test plan section of the SAP focuses on execution of testing. how is the 3PAO going to test the cloud system? Who are they going to talk to? What tools are going to be used? Security control assessors play a unique role in testing system security controls because they are responsible for validating that controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

In this section, the 3PAO must obtain at least three points of contact from the CSP to use for testing communications. one of the contacts must be available 24 x 7 and must include an operations center (e.g. NOC, SOC). The key here is to be sure that each POC role and function in the assessment is clearly defined.

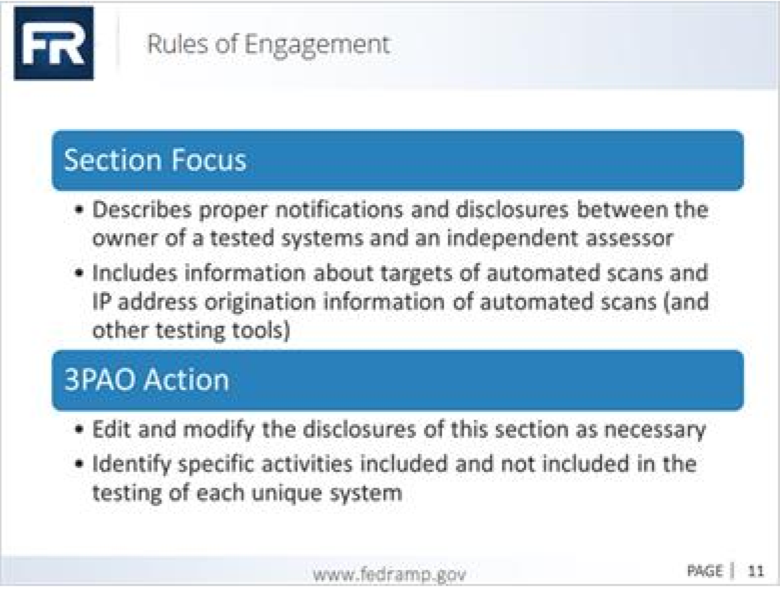
You'll also find a description of what tools will be used for testing security controls--including all product names, names of open source tools, and version numbers. If open source tools are used, name the organization (or individuals) that developed the tools and function and purpose of the tool (e.g., file integrity checking, web application scanning). For scanners, indicate what the scanner's capability is, e.g., database scanning, web application scanning, infrastructure scanning, code scanning/analysis).

Next are the technical tests that will be performed through manual methods--without the use of automated tools. The results of all manual tests must be recorded in the SAR. Examples are listed in the first four rows. Delete the examples, and put in the real tests. Add additional rows as necessary. Identifiers must be in the format MT-1, MT-2 which would indicate "Manual Test 1" and "Manual Test 2" etc. Automated tools and Manual test methods planned for Penetration Testing are included in these tables and in the Penetration Test plan.

After that, insert the Security Assessment testing schedule. The schedule should allow time to resolve findings with the CSP and correction of weaknesses and time permits and as agreed between the CSP and 3PAO.

The 3PAO also has to indicate what type of sampling will be implemented for both technical controls and management controls. Sampling of technical testing of system components may be defined in some cases [e.g., systems with thousands of components]. Sampling of management and operation controls is always defined [e.g., a minimum of 3 interviewees, 3 document reviews [e.g., signed Rules of Behavior], etc.] there are several of these types of tests where sampling is performed and the 3PAO must indicate how they intend to do that.

1.11 Rules of Engagement



Rules of Engagement

Section Focus

- Describes proper notifications and disclosures between the owner of a tested systems and an independent assessor
- Includes information about targets of automated scans and IP address origination information of automated scans (and other testing tools)

3PAO Action

- Edit and modify the disclosures of this section as necessary
- Identify specific activities included and not included in the testing of each unique system

www.fedramp.gov

PAGE | 11

Notes:

Transcript Title

Rules of Engagement

Image

Section Focus, 3PAO Actions

Text

Section Focus

- Describes proper notifications and disclosures between the owner of a tested systems and an independent assessor
- Includes information about targets of automated scans and IP address origination information of automated scans (and other testing tools)

3PAO Action

- Edit and modify the disclosures of this section as necessary
- Identify specific activities included and not included in the testing of each unique system.

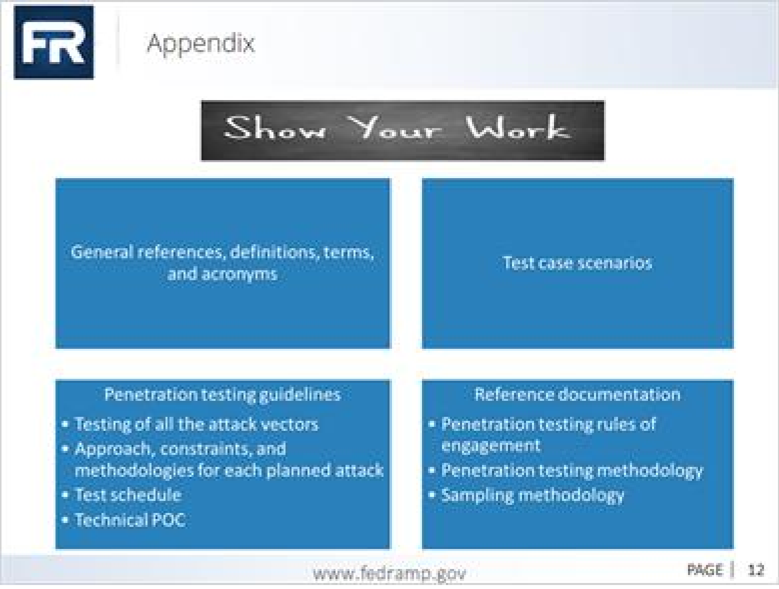
Audio

Rules of Engagement (ROE) -- is a document designed to describe proper notifications and disclosures between the owner of a tested system and an independent assessor. In particular, an ROE includes information about targets of automated scans and IP address origination information of automated scans (and other testing tools). Together, with the information provided in preceding sections of this document, this document will serve as a rules of engagement once signed.

You are free to edit and modify the disclosures of this section as necessary. If testing is to be conducted from an internal location, identify at least one network port with access to all subnets/segments to be tested. The purpose of identifying the IP addresses is to help the CSP understand that the rapid and high volume network traffic is not an attack and is part of the testing.

3PAOs must identify specific activities **included and not included in the testing of each unique system.**

1.12 Appendix



Appendix

Show Your Work

General references, definitions, terms, and acronyms

Test case scenarios

Penetration testing guidelines

- Testing of all the attack vectors
- Approach, constraints, and methodologies for each planned attack
- Test schedule
- Technical POC

Reference documentation

- Penetration testing rules of engagement
- Penetration testing methodology
- Sampling methodology

www.fedramp.gov

PAGE | 12

Notes:

Transcript Title

Appendix

Image

Show Your Work

Text

General references, definitions, terms, and acronyms

Test case scenarios

- Penetration testing guidelines
- Testing of all attack vectors
- Approach, constraints and methodologies for each planned attack
- Test schedule
- Technical POC
- Reference documentation
- Penetration testing rules of engagement
  - Penetration testing methodology
  - Sampling methodology

Audio

Show your work. The Appendices give you the opportunity to provide any supporting information that further tells the story of how the 3PAO plans to test the cloud system. supporting appendices provide detailed assessment related information including:

- General references, definitions, terms, and acronyms - even though this section is pre-populated with information already contained in the SAP. the 3PAO is expected to add further information that is unique to the cloud system being tested
- Test case scenarios - results of the security test case procedures shall be recorded directly in each respective Rev 4 Test Case Workbook.

Details regarding the penetration testing plan and methodology it is important to note that FedRAMP has issued guidance around penetration testing and that document can be found at FedRAMP.gov and by clicking on the Resources tab at the top part of this module. However, the penetration test plan must include:

- Actual testing of all the attack vectors
- A description of the approach, constraints, and methodologies for each planned attack
- A detailed test schedule that specifies the start and end date/times and content of each test period and the overall penetration test beginning and end dates
- Technical points of contact (POC) with a backup for each subsystem and/or application that may be included in the penetration test
- And, finally, Appendix D allows you to provide other reference documentation including penetration testing rules of engagement, penetration testing methodology, and the sampling methodology used in testing.

1.13 Key Documentation Checks (Take 2)

Key Documentation Checks

Section 1-3: Does the system overview information match the information in the SSP?

Security Assessment Plan Template

Version 1.0

November 30, 2015

www.fedramp.gov

PAGE | 14

Notes:

Transcript Title

Key Documentation Checks

Image

Security Assessment Plan, version 1.0, November 30, 2015

Text

Section 1-3: Does the system overview information match the information in the SSP?

Audio

All SAPs are subject to FedRAMP review. when the SAP has been reviewed by the CSP, has been satisfactorily documented by FedRAMP and CSP standards, and is ready for submission the 3PAO should post the document on OMB MAX and notify the FedRAMP ISSO of submission. Once FedRAMP receives the SAP, the document will pass through an initial and detailed review to check the document for quality and content.

The initial review will validate the document against FedRAMP standards for completeness and showstoppers. Checks are also made for common problems and critical controls.

The majority of the Initial review will check for Completeness. The FedRAMP PMO is specifically looking to check if all sections and tables of the SAP are populated with relevant information and if that information is complete.

For example, one of the checks the PMO looks for is to see if all required attachments are provided?

- *The Penetration Test Plan.* A check to ensure compliance with SSP controls CA-7(2) and RA-5(9) and FedRAMP Penetration Test Guidance document.
- *The Assessment Test Cases.* A Check to ensure correct test cases template is used and has not been changed.
- *Rules of Engagement (may be included in Penetration Test Plan).*
- *The Detailed Review* will go further and much of the verification checks will focus on verification of information to ensure consistency with the SSP but also to confirm that the testing plans are clear and appropriate for the system.

As we walk through the following sections of the SAP we will highlight key checks and tips for writing to each section and table.

- Section 1.3 Does the system overview information match the information in the SSP? Excerpts from the system information from the SSP needs to be included and must be consistent. CSP and system names need to match SSP and be consistent throughout.
- Table 2-1: Does the information in this document match Table 1-1 in the SSP?
- Table 2-2: Does information include all locations listed in the SSP? If all the locations are not listed, then the criteria/rationale for selection of the locations [sampling methodology] must be clearly described.
- Table 2-3: Does this table include IP addresses for the complete inventory? This inventory needs to match the inventory in the SSP. This may be a separate file vs. using the table in the SAP. [table headers should not be changed]

If all the inventory items are not listed, then the criteria/rationale for selection of the locations [sampling methodology] must be clearly described.

- Table 2-4: Does this table include all web applications (URLs) for the complete inventory? This inventory needs to match the inventory in the SSP. This may be a separate file vs. using the table in the SAP. [table headers should not be changed]

If all the inventory items are not listed, then the criteria/rationale for selection of the locations [sampling methodology] must be clearly described.

- Table 2-5: Does this table include all database applications for the complete inventory? This inventory needs to match the inventory in the SSP. This may be a separate file vs. using the table in the SAP. However, table headers should not be changed

If all the inventory items are not listed, then the criteria/rationale for selection of the locations [sampling methodology] must be clearly described.

- Table 2-6: Are functions for each of the roles defined in enough detail to determine the testing that will be done? This is part of ensuring the testing methodology is being tailored for this specific system and that separation of duties/roles and privilege escalation will be tested. The information can be in this section or the Penetration Test Plan.
- Section 3: Have any assumptions been changed, deleted, or added. Assumptions may need to be tailored to the system to the system being tested.
  Ensure that these changes do not degrade or negatively impact the purpose, completeness, and/or

integrity of the testing.

Methodology - is there a complete and detailed description of the testing methodology for this specific system? If there are alternative controls, review the methodology to determine if the implementation of those controls impacts the testing methodology. Is the methodology detailed in this section consistent with the assumptions in Section 3 and the testing detailed in the Rules of Engagement? Ensure consistency across the various sections in the document that describe the testing methodologies for this system. Does the methodology provide detail on “sampling” of non-technical controls, such as management controls?. There should be an indication in this section or Appendix B, Test Cases, on what is considered an “agreed upon” sample for examination of items like the executed ROBs (rules of behavior) or training records, etc

- Table 5-1: Does the “role” description provide information about what the tester will actually be doing, for example, penetration testing, vulnerability scanning? Check to see if they have quality control identified. If not, suggest they identify this role as well.
- Table 5-2: Does the “role” description provide information about what the CSP POC will be doing for these tests? The role as defined in the User Types may also be applicable.
- Table 5-3: Does the list of tools include a detailed description of what the tools will be used to test within the system? For example, Nessus will be used to scan OS and database applications for vulnerabilities. It is not sufficient to indicate that Nessus is a vulnerability scanner.
- Table 5-3: Does the list of tools include tools that will be utilized as part of penetration testing? It is OK to include these here and include that detailed information. The information here must be consistent with the penetration testing plan.
- Table 5-4: Does this table include manual tests that may be required for items that cannot be tested using automated tools? This might include manual tests of the firewall configuration rules, for example. The PMO will also verify with the CSP and 3PAO that the tools selected for routine continuous monitoring of the OS, Web, and Database vulnerability scanning that are listed in this table will be the tools used for continuous monitoring? This is required. The 3PAO may use additional tools to verify tests for example, but the CSP must be able to continue to manage initial and future findings using the same tools.
- Table 5-5: Does the schedule match the ISSO project schedule? Resolve any inconsistencies to ensure the project schedule is maintained.

The PMO will also review Section 6 and the Appendix attachments as well for verification and adequacy of Rule of Engagement, Test Cases, and Penetration Testing Plans.

1.14 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