FedRAMP Security Assessment Report (SAR) Training

1. FedRAMP_Training_SAR_v4_508

1.1 FedRAMP SAR Overview Online Training Splash Screen

FedRAMP

Federal Risk and Authorization Management Program

FedRAMP Online Training

Security Assessment Report (SAR) Overview

12/9/2015

Presented by: FedRAMP PMO

www.fedramp.gov

Select the Next button to begin

Notes:

Transcript

Title <N/A>

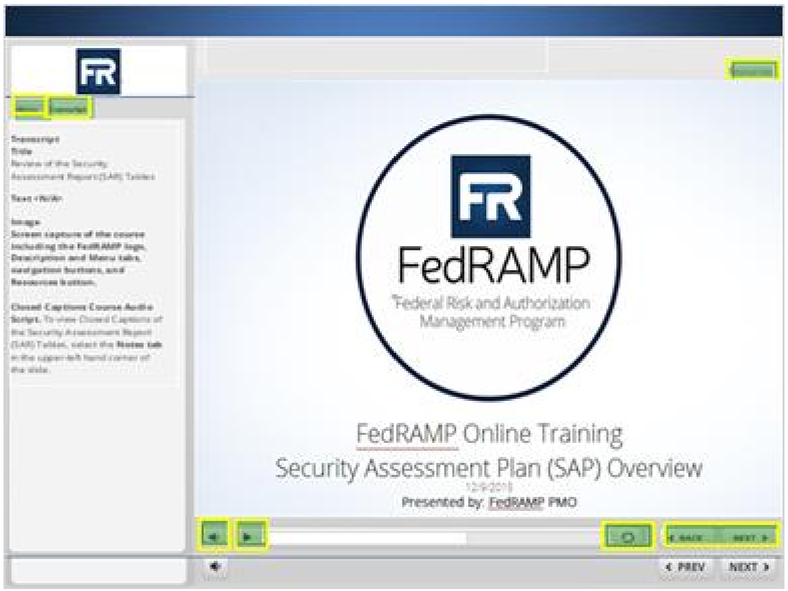
Image

Image of FedRAMP logo.

Text

FedRAMP Online Training; Security Assessment Report (SAR) 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
Presented by: FedRAMP PMO
◂ BACK
NEXT ▸
◂ PREV
NEXT ▸

Notes:

Transcript

Title

Course Features and Functions

Text

<N/A>

Image

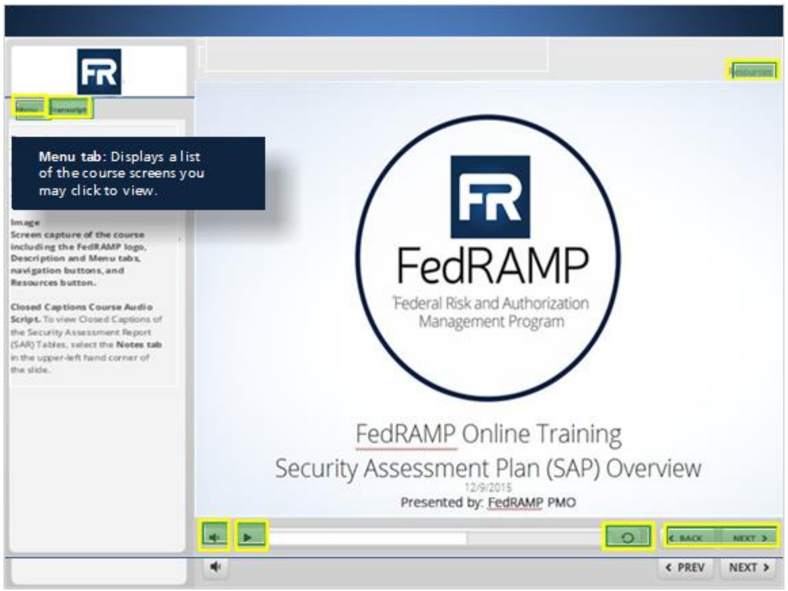
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

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)



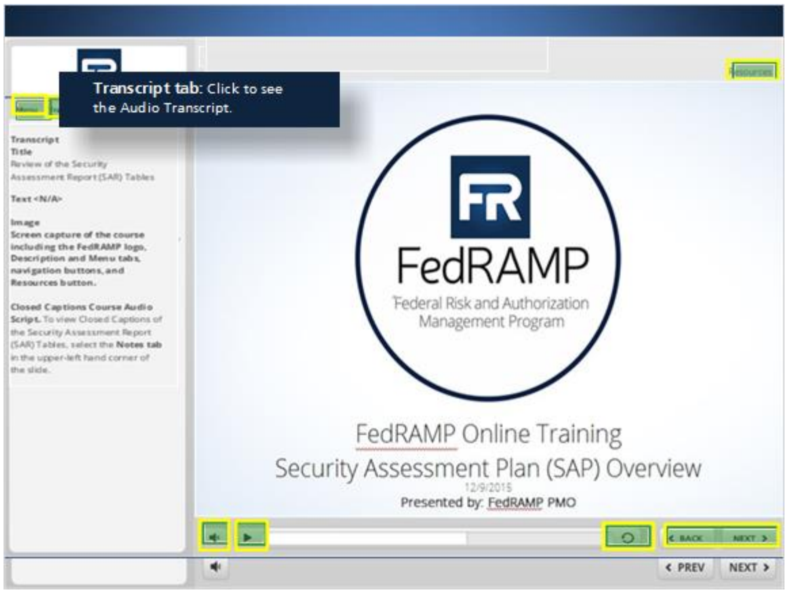
Menu tab: Displays a list of the course screens you may click to view.

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 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

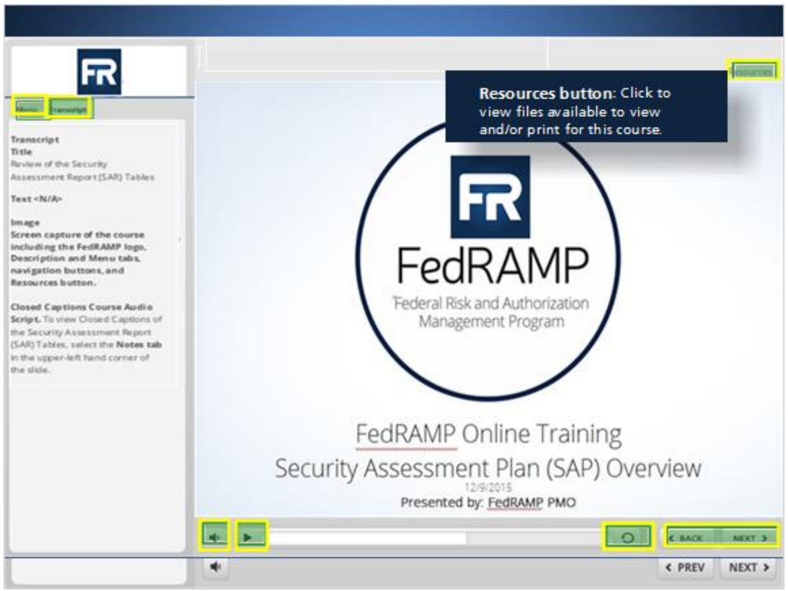
Text <N/A>

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

Resources (Slide Layer)



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

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

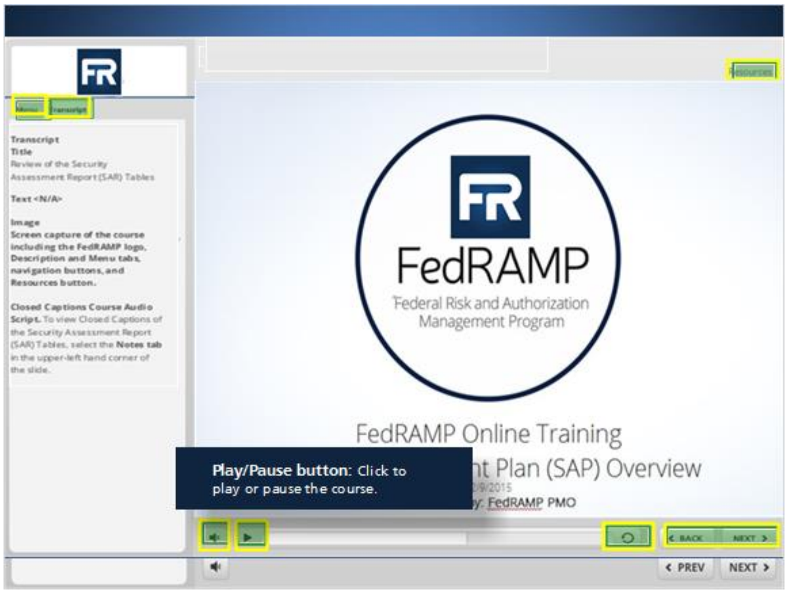
Text <N/A>

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

Play/Pause (Slide Layer)



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

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

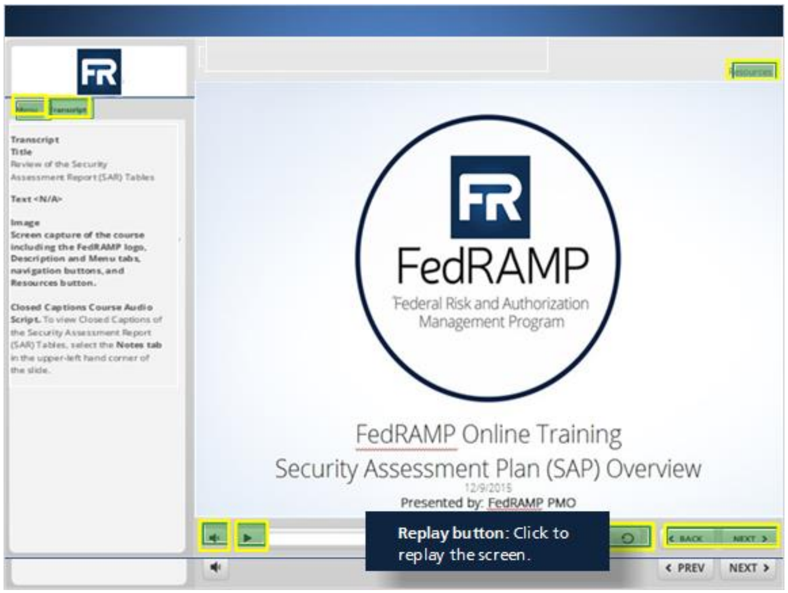
Text <N/A>

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
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.

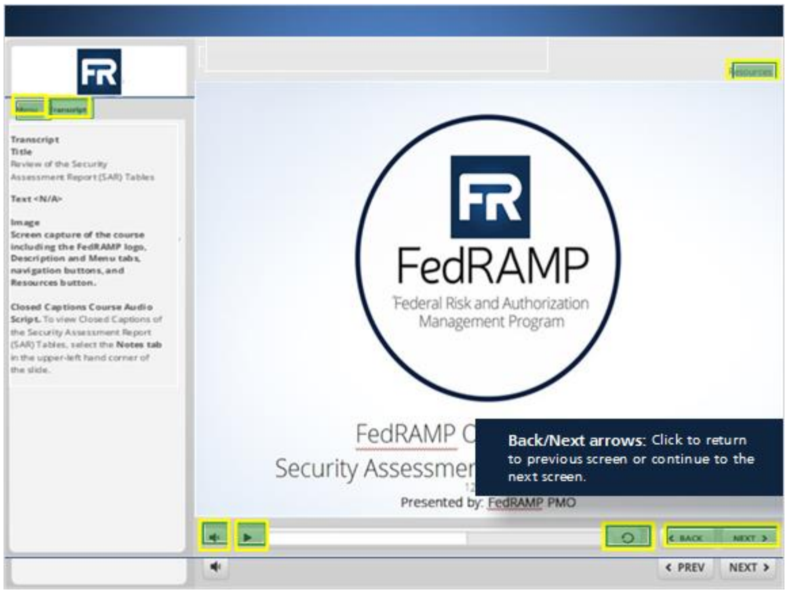
Closed Captions Course Audio Script. To view Closed Captions of the Security Assessment Report (SAR) Tables, select the **Notes tab** in the upper-left hand corner of the slide.

FedRAMP
Federal Risk and Authorization Management Program

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.

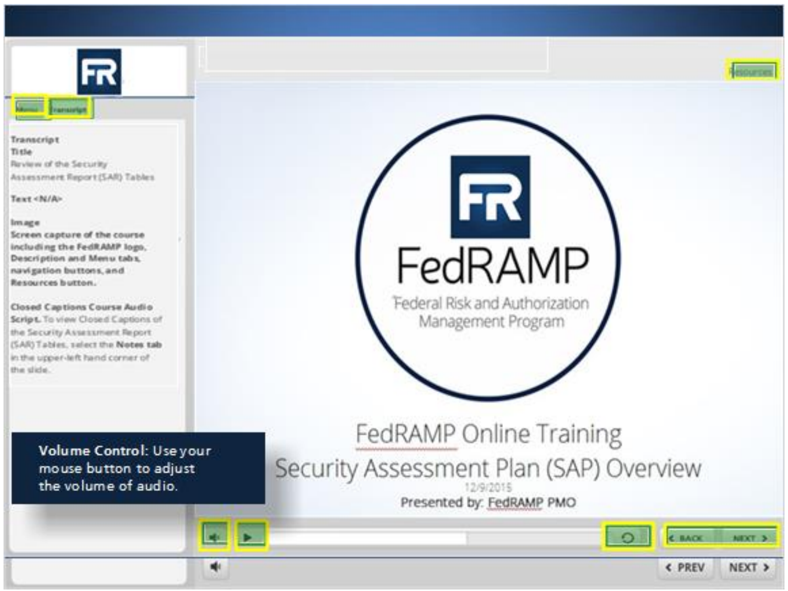
Closed Captions Course Audio Script. To view Closed Captions of the Security Assessment Report (SAR) Tables, select the **Notes tab** in the upper-left hand corner of the slide.

FedRAMP
Federal Risk and Authorization Management Program

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.

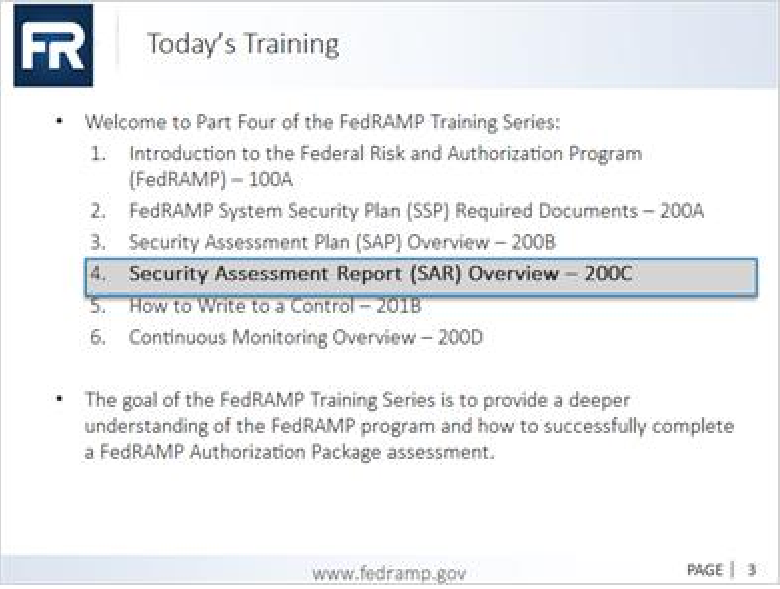
Closed Captions Course Audio Script. To view Closed Captions of the Security Assessment Report (SAR) Tables, select the **Notes tab** in the upper-left hand corner of the slide.

FedRAMP
Federal Risk and Authorization Management Program

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. Security Assessment Plan (SAP) Overview – 200B
  4. **Security Assessment Report (SAR) Overview – 200C**
  5. How to Write to a Control – 201B
  6. 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.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

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.

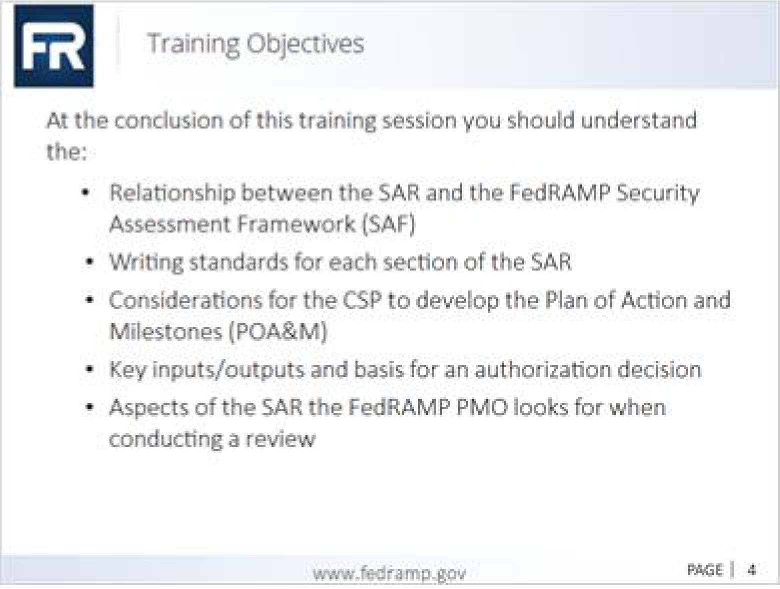
Audio

Welcome to the FedRAMP Online Training series. I am <NAME> your instructor for this training. In this course we will discuss and provide an overview of the Security Assessment Report or SAR.

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 required to satisfactorily complete a FedRAMP assessment.

This training module is tailored to a CSP going through the JAB path and a Third Party Assessment Organization or 3PAO conducting an assessment of the Cloud System. 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 SAR and the FedRAMP Security Assessment Framework (SAF)
- Writing standards for each section of the SAR
- Considerations for the CSP to develop the Plan of Action and Milestones (POA&M)
- Key inputs/outputs and basis for an authorization decision
- Aspects of the SAR the FedRAMP PMO looks for when conducting a review

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:

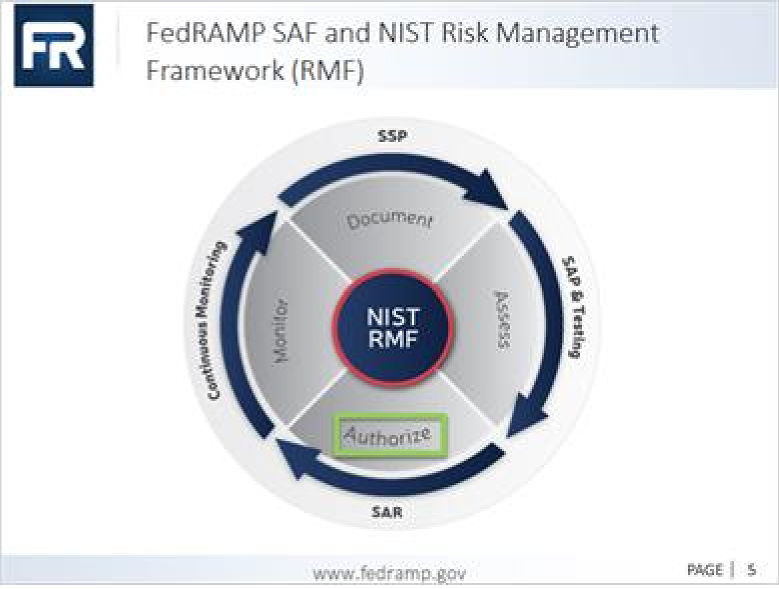
- Relationship between the SAR and the FedRAMP Security Assessment Framework (SAF)
- Writing standards for each section of the SAR
- Considerations for the CSP to develop the Plan of Action and Milestones (POA&M)
- Key inputs/outputs and basis for an authorization decision
- Aspects of the SAR the FedRAMP PMO looks for when conducting a review

Audio

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

- Relationship between the SAR and the FedRAMP Security Assessment Framework (SAF)
- Writing standards for each section of the SAR
- Considerations for the CSP to develop the Plan of Action and Milestones (POA&M)
- Key inputs/outputs and basis for an authorization decision
- Aspects of the SAR the FedRAMP PMO looks for when conducting a review

1.5 FedRAMP SAF and NIST RMF



FedRAMP SAF and NIST Risk Management Framework (RMF)

SSP

Document

SAP & Testing

Assess

SAR

Authorize

Continuous Monitoring

Monitor

NIST RMF

www.fedramp.gov

PAGE | 5

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

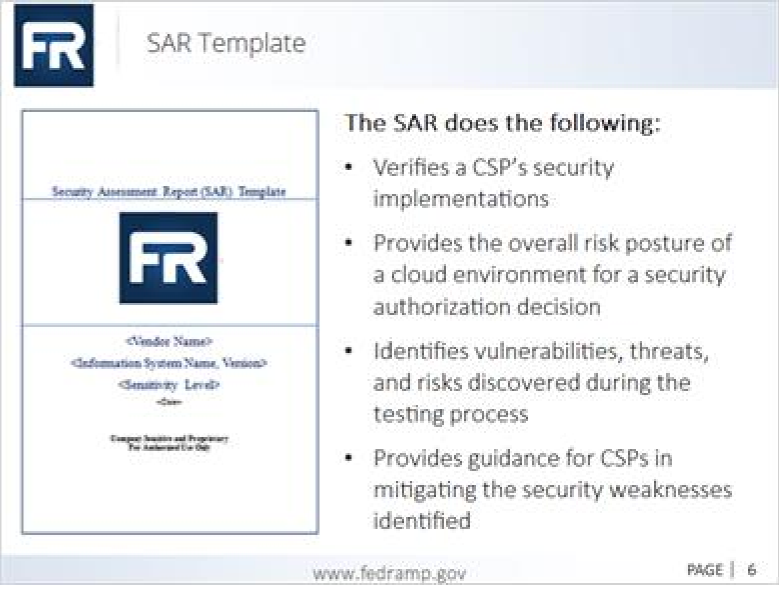
Federal agencies are required to assess and authorize information systems in accordance with FISMA. The FedRAMP SAF is compliant with FISMA and is based on the NIST RMF. In fact, FedRAMP uses the same documents and deliverables that NIST requires agencies to use. However, FedRAMP simplifies the NIST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

CSPs verify compliance by following the FedRAMP SAF. Through this process, the risks of a CSPs services are determined and it gives agency authorizing officials the ability to determine if the risk posture of a Cloud System meets the risk posture needed to host government data.

The Security Assessment Framework ensures that managing risk from the operation and use of federal systems is consistent with the organizations mission and business objectives and overall risk strategy and supports consistent, well informed, and ongoing security authorization decisions to achieve more secure information and systems.

Going forward in this training module we will focus on the Authorize Phase of the SAF which includes the SAR and Plan of Action and Milestones (POA&M) templates as the key documents that determine if the system's residual risk is acceptable.

1.6 SAR Template



SAR Template

Security Assessment Report (SAR) Template

<Vendor Name>
<Information System Name, Version>
<Sensitivity Level>
<Date>

Company Sensitive and Proprietary
For Authorized Use Only

The SAR does the following:

- Verifies a CSP's security implementations
- Provides the overall risk posture of a cloud environment for a security authorization decision
- Identifies vulnerabilities, threats, and risks discovered during the testing process
- Provides guidance for CSPs in mitigating the security weaknesses identified

www.fedramp.gov PAGE | 6

Notes:

Transcript Title

SAR Template

Image

Security Assessment Report Template cover

Text

The SAR does the following:
- Verifies a CSP's security implementations
- Provides the overall risk posture of a cloud environment for a security authorization decision
- Identifies vulnerabilities, threats, and risks discovered during the testing process
- Provides guidance for CSPs in mitigating the security weaknesses identified

Audio

The FedRAMP program requires Cloud Service Providers (CSPs) to use an independent third-party assessor. For the JAB path and the CSP path, FedRAMP requires the assessor to be FedRAMP Accredited Third-Party Assessor Organization (3PAO) to perform the security assessment and development of the SAR. For Agency Authorizations, an agency may use a FedRAMP 3PAO or an agency internal independent assessment organization. At the completion of the assessment testing, the Independent Assessors or 3PAO produces the Security Assessment Report (SAR) that documents the verification of the CSPs implementation of security and provides the overall risk posture of a CSP in support of security authorization decision. The SAR is records all current vulnerabilities and risks to CSP systems and contains the details of the testing methodology and results.

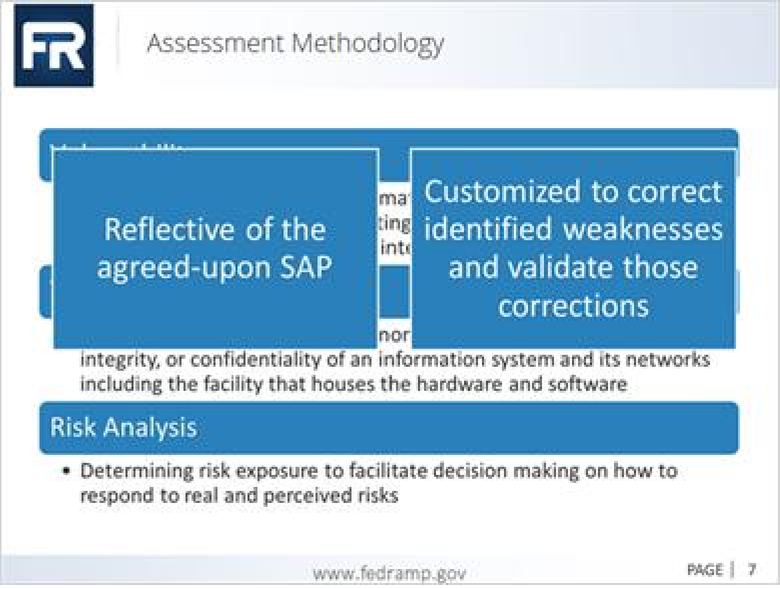
Additionally, the SAR provides guidance to CSPs in mitigating the security weaknesses found. The assessment must be conducted in compliance with NIST SP 800-53 revision 4. The plan for testing was documented in an SAP; however, quite frequently the testing and assessment deviate from the approved SAP. All deviations from the approved SAP are detailed in the List of Assessment Deviations. Example of deviations could be a change in inventory from the time of planning to testing, a change in schedule from planned to actual, etc.

The FedRAMP PMO provides a *Security Assessment Report* template, and all 3PAOs are required to use this template to report their findings. The SAR template is available on www.fedramp.gov.

For JAB Provisional ATO’s, the 3PAO is expected to provide a high-level briefing to the JAB TRs. This brief will highlight findings, mitigations, and operational requirements, as well as identify any problems or areas of concern. The FedRAMP ISSO coordinates with the *CSP and* 3PAO on the briefing.

The SAR is divided into eight sections and includes 9 appendices. The next few sections will detail each of these sections further and give specific instructions on how to write to them and what FedRAMP is looking for when reviewing these documents.

1.7 Assessment Methodology



Assessment Methodology

Reflective of the agreed-upon SAP

Customized to correct identified weaknesses and validate those corrections

integrity, or confidentiality of an information system and its networks including the facility that houses the hardware and software

Risk Analysis

- Determining risk exposure to facilitate decision making on how to respond to real and perceived risks

www.fedramp.gov

PAGE | 7

Notes:

Transcript Title

Vulnerability

Image

Reflective of the agreed-upon SAP; Customized to correct identified weakness and validate those correction

Text

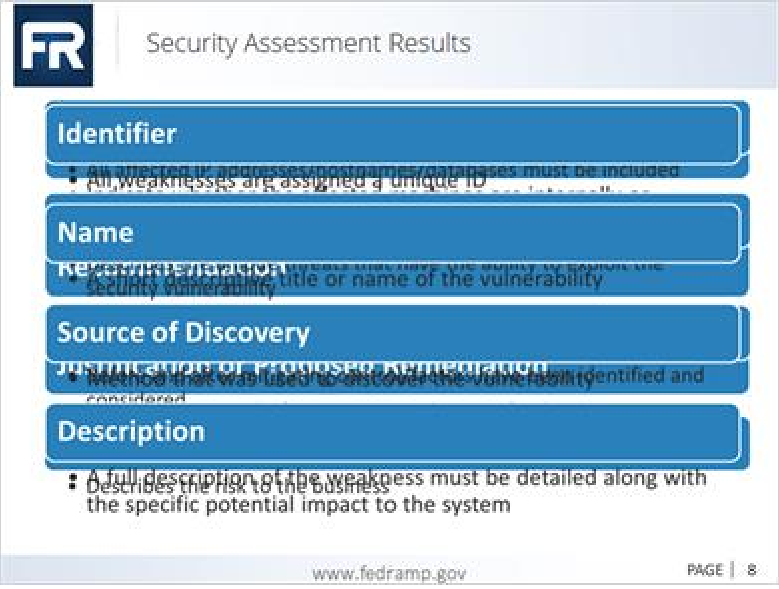
Vulnerability: an inherent weakness in an information system that can be exploited by a threat or threat agent, resulting in an undesirable impact on the protection of the confidentiality, integrity, or availability of the system.

Threat: an adversarial force or phenomenon that could impact the availability, integrity, or confidentiality of an information system and its networks including the facility that houses the hardware and software

Risk Analysis: determining risk exposure to facilitate decision making on how to respond to real and perceived risks.

Audio
Section 1 and 2 are straight forward and detail the scope of the testing conducted by the 3PAO and purpose of the system including security categorization determined in accordance with FIPS 199.
Beginning with Section 3, the 3PAO documents the assessment methodology used to conduct the security assessment. The methodology should be reflective of the agreed upon Security Assessment Plan (SAP) and customized to correct identified weaknesses and validate those corrections. A list of deviations from the original plan for the assessment presented in the SAP should be appropriately documented.
Additionally, the 3PAO must also identify all vulnerabilities, threats and provide a risk analysis.
A vulnerability is an inherent weakness in an information system that can be exploited by a threat or threat agent, resulting in an undesirable impact on the protection of the confidentiality, integrity, or availability of the system (application and associated data). A vulnerability may be due to a design flaw or error in configuration which makes the network, or a host on the network, susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in multiple areas of the system or facilities, such as in firewalls, application servers, Web servers, operating systems or fire suppression systems.
A threat is an adversarial force or phenomenon that could impact the availability, integrity, or confidentiality of an information system and its networks including the facility that houses the hardware and software. A threat agent is an element that provides the delivery mechanism for a threat. An entity that initiates the launch of a threat agent is referred to as a threat actor. A threat actor might purposefully launch a threat agent. However, a threat actor could also be a trusted employee that acts as an agent by making an unintentional human error. FedRAMP takes threat types into consideration to help determine the likelihood that a vulnerability could be exploited. The 3PAO is responsible for assigning threat types to vulnerabilities, then determine the likelihood that a vulnerability could be exploited by the corresponding threat.
Identifying vulnerabilities and threats are key in determining the risk exposure of a Cloud System. The goal of determining risk exposure is to facilitate decision making on how to respond to real and perceived threats.

1.8 Security Assessment Results



Security Assessment Results

Identifier
- All weaknesses are assigned a unique ID

Name
- A short descriptive title or name of the vulnerability

Source of Discovery
- Method that was used to discover the vulnerability

Description
- A full description of the weakness must be detailed along with the specific potential impact to the system

www.fedramp.gov

PAGE | 8

Notes:

Transcript Title

Security Assessment Results

Image

Identifier, Name, Source of Discovery, Description

Audio

The Security Assessment Results section describes all security weaknesses found during testing. The following elements for each security weakness are reported in the Risk Exposure Summary Worksheet.

Identifier: All weaknesses are assigned a unique ID in the form of V#-Security Control ID. For example, the first vulnerability listed would be reported as V1-AC-2(2) if the vulnerability is for control ID AC-2(2). If there are multiple vulnerabilities for the same security control ID, the first part of the vulnerability ID must be incremented, for example V1-AC-2(2), V2-AC-2(2).

Name: A short descriptive title or name of the vulnerability.

Source of Discovery: The source of discovery refers to the method that was used to discover the vulnerability (e.g., web application scanner, manual testing, security test procedure workbook, interview, document review). In practice, the reference to the source of discovery is generally a reference to the scan or re-scan include date, test procedure workbook, or pen test report and date.

Description: A full description of the weakness must be detailed along with the specific potential impact to the system.

Affected IP Address/Hostname(s)/Database: For each reported vulnerability, all affected IP addresses/hostnames/databases must be included. If multiple hosts/databases have the same vulnerability, list all affected hosts/databases.

Applicable Threats: The applicable threats describe the unique threats that have the ability to exploit the security vulnerability. Threat IDs are derived from list of threats in Table 3-3 of the SAR template.

Likelihood, Impact and Risk Exposure: These categories are noted both before and after mitigating control/factors have been identified and considered, and are rated on a scale of High, Moderate, or Low

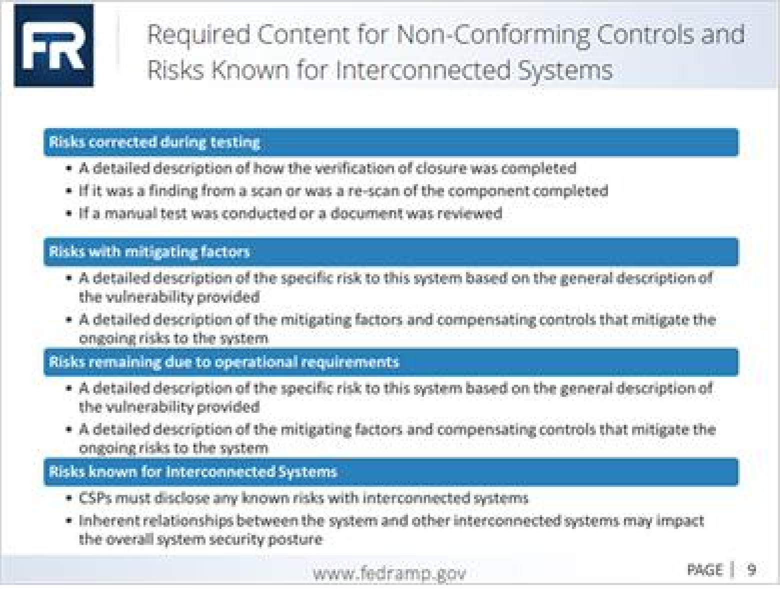
Risk Statement: Provide a risk statement that describes the risk to the business. Also indicate whether the affected machine(s) is/are internally or externally facing.

Mitigating Controls/Factors: Describe any applicable mitigating controls/factors that could downgrade the likelihood or risk exposure. Also indicate whether the affected machines are internally or externally facing. Include a full description of any mitigating factors and/or compensating controls if the risk is an operational requirement

Recommendation: The recommendation describes how the vulnerability must be resolved. Indicate if there are multiple ways that the vulnerability could be resolved or recommendation for acceptance of operational requirement.

Justification or Proposed Remediation: Provide a rationale for recommendation of risk adjustment or operational requirement.

1.9 Required Content for Non-Conforming Controls and Risks Known for Interconnected Systems



Required Content for Non-Conforming Controls and Risks Known for Interconnected Systems

Risks corrected during testing

- A detailed description of how the verification of closure was completed
- If it was a finding from a scan or was a re-scan of the component completed
- If a manual test was conducted or a document was reviewed

Risks with mitigating factors

- A detailed description of the specific risk to this system based on the general description of the vulnerability provided
- A detailed description of the mitigating factors and compensating controls that mitigate the ongoing risks to the system

Risks remaining due to operational requirements

- A detailed description of the specific risk to this system based on the general description of the vulnerability provided
- A detailed description of the mitigating factors and compensating controls that mitigate the ongoing risks to the system

Risks known for Interconnected Systems

- CSPs must disclose any known risks with interconnected systems
- Inherent relationships between the system and other interconnected systems may impact the overall system security posture

www.fedramp.gov

PAGE | 9

Notes:

Transcript Title

Required Content for Non-Conforming Controls and Risks Known for Interconnected Systems

Image

Risks corrected during testing; Risks with mitigating factors; Risks known for Interconnected Systems

Audio

Section 5 and 6 deal with identifying specific risks that have either been corrected, mitigated, accepted, or are considered part of an interconnected system.

In some cases, the initial risk exposure to the system are adjusted due to either corrections that occurred during testing or to other mitigating factors.

The 3PAO is responsible for documenting the following:

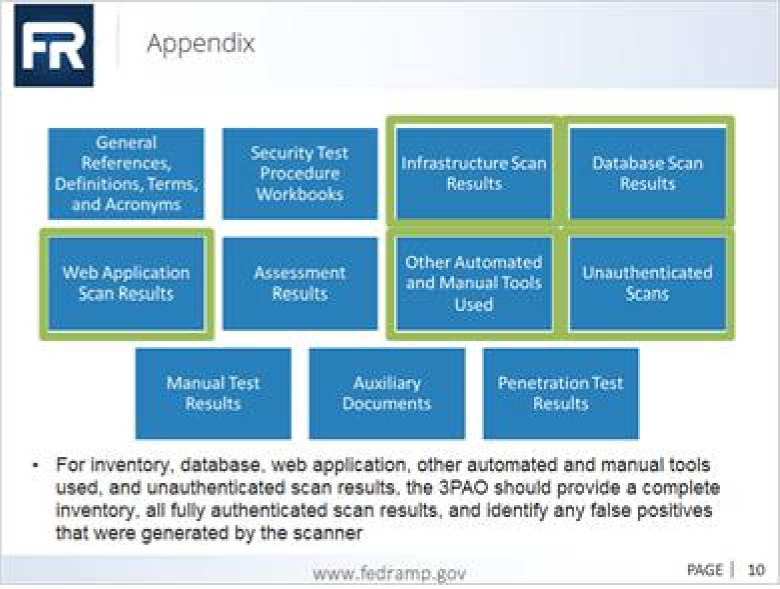
Risks corrected during testing - Risks discovered during the testing that have been corrected prior to completion of testing. These should be verified and the verification statements need to contain the following information. A Detailed description of how the verification of closure was completed. If it was a finding from a scan or a re-scan of the component completed; some scan finding validations are completed via manual methods as well. If a manual test was conducted or a document reviewed; if it was a finding from a manual test - a manual test will be used to verify such as a document examination.

R*isks with mitigating factors* - Risks that have had their severity levels changed due to mitigating factors. The factors used to justify changing the initial risk exposure rating should also be noted and the description of mitigating factors for each item should contain a detailed description of the specific risk to this system based on the general description of the vulnerability provided and, a detailed description of the mitigating factors and compensating controls that support the adjustment of risk.

R*isks remaining due to operational requirements* - Risks that reside in the system that cannot be corrected due to operational constraints. An explanation of the operational constraints and risks are also included in the appropriate Security Assessment Test Cases and System Security Plan (SSP). This applies to all findings in the SAR - all items in the risk summary table are documented in the test cases workbook and based on unique ID. Because these risks will not be corrected, they are not tracked in the Plan of Actions and Milestones (POA&M). The description of Operational Requirements Rationale and Mitigating Factors should contain a detailed description of the specific risk to this system based on the general description of the vulnerability provided and, a detailed description of the mitigating factors and compensating controls that mitigate the ongoing risks to the system.

R*isks known for Interconnected Systems* - 3PAOs must include any known risks with interconnected systems that they discovered. CSPs shall disclose any known risks with interconnected systems. In order to determine this information, it may be necessary to consult other Security Assessment Reports, Interconnection Agreements, Service Level Agreements, Memorandums of Understanding, US-CERT advisories and reference Table 11-1 in the SSP that lists interconnected systems as the authoritative source. Inherent relationships between the system and other interconnected systems may impact the overall system security posture. However, in some cases the system may not have any external interconnections in which case the 3PAO should note the rationale as to why this section is not applicable.

1.10 Appendix



Appendix

General References, Definitions, Terms, and Acronyms

Security Test Procedure Workbooks

Infrastructure Scan Results

Database Scan Results

Web Application Scan Results

Assessment Results

Other Automated and Manual Tools Used

Unauthenticated Scans

Manual Test Results

Auxiliary Documents

Penetration Test Results

- For inventory, database, web application, other automated and manual tools used, and unauthenticated scan results, the 3PAO should provide a complete inventory, all fully authenticated scan results, and identify any false positives that were generated by the scanner

www.fedramp.gov

PAGE | 10

Notes:

Transcript Title

Appendix

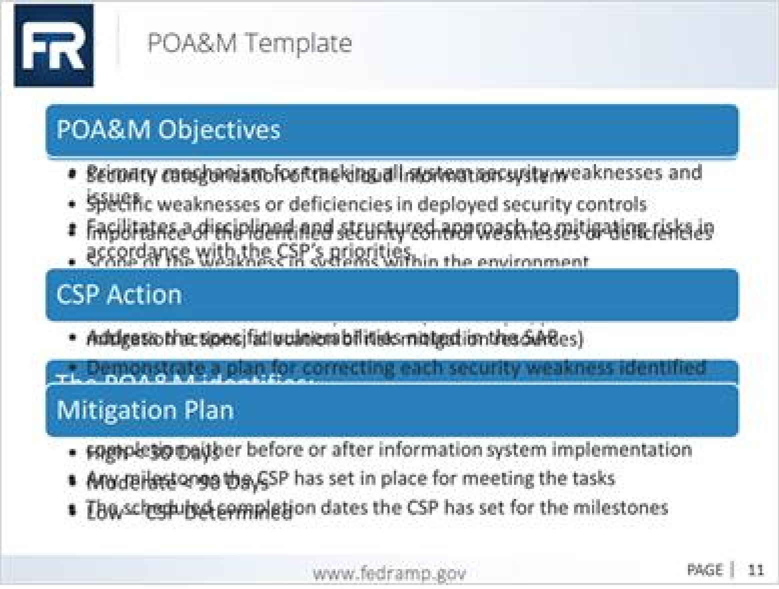
Audio

The appendices give you the opportunity to provide any supporting information that further tells the story of how the 3PAO tested 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 SAR the 3PAO is expected to add further information that is unique to the Cloud system being tested. In addition, a list of all documents reviewed is required.
- Security Test Procedure Workbooks - Provide the Security Test procedure workbooks. Ensure that results of all tests are recorded in the workbooks.

- Infrastructure Scan Results - All items in inventory must be scanned, unless sampling is permitted per the approved SAP. The scans should be referenced by “title” and detailed filename, including extension and not embedded in the document. They can be .zip files by type of scan, e.g., OS, web, etc however, they must be provided in a “parseable” format, such as .xml or .csv. Sample files should be provided to the PMO or agency prior to submission to verify readability.
- Database Scan Results - Provide all database scans results generated by the scanner in a readable format. Bundle all scan results into one zip file. Do not insert files that require a scan license to read the file.
- Web Application Scan Results - Indicate the web applications that were scanned and indicate the function that the web-facing application plays for the system.
- Assessment Results - Summary of System Security Risks from FedRAMP Testing and Final Summary of System Security Risks
- Other Automated and Manual Tools Used
- Unauthenticated Scans - Provide the results from any unauthenticated scans. However, in order to use this table, the IA must obtain approval from the AO when submitting the SAP. If this table is not used, write “Not Applicable”.
- Manual Test Results
- Auxiliary Documents
- And Penetration Test Results - These are provided in the pen test report and results are included in the risk summary table.
- For Inventory, Database, Web Application, Other Automated and Manual Tools, and Unauthenticated scan results the 3PAO should provide a complete inventory, all fully authenticated scan results, and identify any false positives that were generated by the scanner.
- As part of security testing, automated scans are required. On large implementations, a subset of all representative hosts and device types must be scanned using full authentication. The advantage of running scans as fully authenticated privileged users is that the scanner can access the registry, file attributes, installed packages, and patch levels. Account credentials for the authenticated scans must use login IDs and user roles that offer the greatest possible privileges for the scanned system (e.g., root, administrator).
- The use of non-authenticated scans can assist in vulnerability severity determinations and to prioritize remediation efforts since non-authenticated scan vulnerabilities are seen from the point of an attacker/intruder. Non-authenticated scans can augment fully authenticated scans if the information from these scans helps to determine the risk exposure. FedRAMP does not require non-authenticated scans.
- 3PAOs do not need to run source code scans. However, if a CSP develops and uses original source code in their service offering, the CSP is required to perform source code scanning on the installed release and provide the source code analysis report to the 3PAO to satisfy control SA-11(1). The 3PAO submits all scan results to the FedRAMP PMO ISSO at the same time the SAR is provided, and the 3PAO must be prepared to brief the results to the FedRAMP PMO and JAB representatives.

1.11 POA&M Template



POA&M Template

POA&M Objectives

- Primary mechanism for tracking all system security weaknesses and issues
- Security categorization of the individual information system
- Specific weaknesses or deficiencies in deployed security controls
- Facilitates a disciplined and structured approach to mitigating risks in accordance with the CSP's priorities
- Importance of the identified security control weaknesses or deficiencies
- Scope of the weakness in systems within the environment

CSP Action

- Address the specific vulnerabilities noted in the SAR
- Demonstrate a plan for correcting each security weakness identified

The POA&M identifies:

Mitigation Plan

- completion either before or after information system implementation
- High < 30 Days
- Any milestones the CSP has set in place for meeting the tasks
- Moderate < 90 Days
- The scheduled completion dates the CSP has set for the milestones
- Low – CSP Determined

www.fedramp.gov

PAGE | 11

Notes:

Transcript Title

POA&M Template

Image

POA&M Objectives; CSP Action; Mitigation Plan

Audio

The Federal Information Security Management Act (FISMA) requires that a Plan of Action and Milestones (POA&M) be developed and utilized as the primary mechanism for tracking all system security weaknesses and issues. The POA&M is a mitigation plan designed to address specific residual security weaknesses and includes information on costing, resources, and target dates.

The purpose of the POA&M is to facilitate a disciplined and structured approach to mitigating risks in accordance with the CSP's priorities. The POA&Ms include the findings and recommendations of the Security Assessment Report (SAR) and the continual security assessments. FedRAMP uses the POA&M to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment and throughout the continuous monitoring process.

After receiving the SAR from the 3PAO, the CSP develops a POA&M that addresses the specific vulnerabilities noted in the SAR. The CSP needs to demonstrate that it has a plan in place for correcting each security weakness identified. The POA&M serves as a tracking system for the CSP and represents the CSP's "to do" list.

FedRAMP provides a POA&M template for CSPs which is available on the FedRAMP website. All High, Moderate, and Low findings from the SAR must be mapped into the POA&M. High impact vulnerabilities must be mitigated within 30 days, and Moderate impact vulnerabilities must be mitigated within 90 days. The CSP determines a date for closure of low items. However, low items must have a completion date and be remediated. A large number of open low items may be considered a risk to the security posture of the system.

The POA&Ms are based on the:

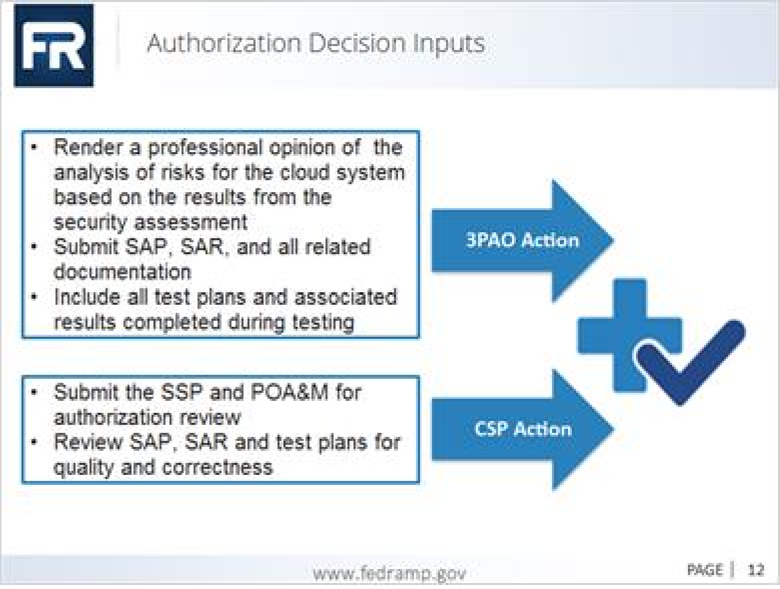
- Security categorization of the cloud information system
- Specific weaknesses or deficiencies in deployed security controls
- Importance of the identified security control weaknesses or deficiencies
- Scope of the weakness in systems within the environment
- Proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (for example, prioritization of risk mitigation actions, allocation of risk mitigation resources)

The POA&M identifies:

i. the tasks the CSP plans to accomplish with a recommendation for completion either before or after information system implementation;
ii. any milestones the CSP has set in place for meeting the tasks; and
iii.the scheduled completion dates the CSP has set for the milestones.

Documenting the results of security control testing creates a record of the security posture for the system at a given moment in time. The record can be reviewed for risk-based decision making and to create plans of action to mitigate risks..

1.12 Authorization Decision Inputs



Authorization Decision Inputs

- Render a professional opinion of the analysis of risks for the cloud system based on the results from the security assessment
- Submit SAP, SAR, and all related documentation
- Include all test plans and associated results completed during testing

3PAO Action

- Submit the SSP and POA&M for authorization review
- Review SAP, SAR and test plans for quality and correctness

CSP Action

www.fedramp.gov

PAGE | 12

Notes:

Transcript Title

Authorization Decision Inputs

Image

Arrow showing 3PAO Action; CSP Action

Audio
Within the SAR the 3PAO must render a professional opinion of their analysis of risks for the cloud system based on the results from the security assessment. Any recommendations must be supported by findings, evidence, and artifacts. This recommendation will be fully reviewed by the Authorizing Official. For JAB P-ATO packages, the 3PAO makes a recommendation for issuance of the P-ATO - agency AO might request a recommendation or indication of overall risk, such as High, Moderate, or Low.

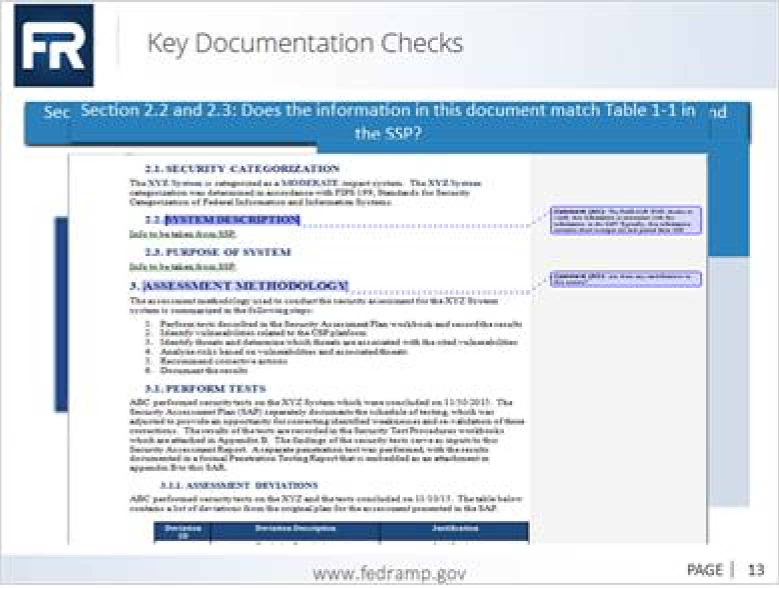
Following the development of the SAR and POA&M Template, the SAP and SAR and all related documents and attachments related to the assessment of the system [e.g., pen test plan, report] must be submitted by the 3PAO directly to FedRAMP or the Agency AO.

The CSP is responsible for submitting the SSP and all related documentation and the POA&M. Authorizing officials will review the entire security package and make a risk-based decision on whether or not to authorize the system.

CSPs that receive either type of authorization will be added to the list of authorized CSPs on www.fedramp.gov . The listing will provide basic information about the service offering related to the authorized system. The authorization letter and security package will be stored in a secure, access-controlled, repository for review by agencies that wish to leverage the CSP's authorization in order to issue their own ATO.

Once an authorizing official has made a risk-based decision to authorize a CSP environment for use, they formalize this decision in an ATO letter. Authorizing officials provide this letter to the CSP system owner and a copy to the FedRAMP PMO on these letters so that the FedRAMP PMO can verify agency use, keep agencies informed of any changes to a CSP's authorization, and submit their package to FedRAMP for inclusion in the FedRAMP secure repository. CSPs that have an agency authorization will have authorization letters granted by a specific government agency and CSPs that go through the JAB will have a P-ATO letter signed by the JAB.

1.13 Key Documentation Checks (Take 2)



Key Documentation Checks

Section 2.2 and 2.3: Does the information in this document match Table 1-1 in the SSP?

2.1. SECURITY CATEGORIZATION

The XYZ System is categorized as a MODERATE impact system. The XYZ System categorization was determined in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

2.2. SYSTEM DESCRIPTION

Info to be taken from SSP.

2.3. PURPOSE OF SYSTEM

Info to be taken from SSP.

3. ASSESSMENT METHODOLOGY

The assessment methodology used to conduct the security assessment for the XYZ System system is summarized in the following steps:

1. Perform tests described in the Security Assessment Plan workbook and record the results
2. Identify vulnerabilities related to the CSP platform
3. Identify threats and determine which threats are associated with the cited vulnerabilities
4. Analyze risks based on vulnerabilities and associated threats
5. Recommend corrective actions
6. Document the results

3.1. PERFORM TESTS

ABC performed security tests on the XYZ System which were concluded on 11/30/2015. The Security Assessment Plan (SAP) separately documents the schedule of testing, which was adjusted to provide an opportunity for correcting identified weaknesses and re-validation of those corrections. The results of the tests are recorded in the Security Test Procedures workbooks which are attached in Appendix B. The findings of the security tests serve as inputs to this Security Assessment Report. A separate penetration test was performed, with the results documented in a formal Penetration Testing Report that is embedded as an attachment in appendix B to this SAR.

3.1.1. ASSESSMENT DEVIATIONS

ABC performed security tests on the XYZ and the tests concluded on 11/30/15. The table below contains a list of deviations from the original plan for the assessment presented in the SAP.

Deviation ID	Deviation Description	Justification

[illegible]

[illegible]

www.fedramp.gov

PAGE | 13

Notes:

Transcript Title

Key Documentation Checks

Image

Section 2.2 and 2.3: Does the information in this document match Table 1-1 in the SSP?

Audio

All SARs are subject to FedRAMP review. When the SAR 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 SAR 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.

Beginning our review at Section 2.2 and 2.3 the FedRAMP PMO checks to verify this information is consistent with the information in the SSP? Typically, this information contains short excerpts cut and pasted from SSP.

Section 3: Are there any modifications to this section? Review any modifications to determine that they do not degrade or impact the completeness or integrity of the testing and that they do not deviate from the SAP. The PMO will check for completeness of this section and review all tables to ensure that the tables have not been manipulated and contain the right level of information regarding the assessment.

Section 4: There should be no changes to this text and the bulleted list of elements and the bulleted paragraphs must match.

Table 5-1: Ensure scans and artifacts verify remediation of the specific finding.

Table 5-2: Ensure that the mitigating factors and compensating are sufficient to support the adjustment. If

artifacts are referenced, ensure the artifact has been provided or is available for review on-site.
Table 5-3: Ensure that the mitigating factors and compensating controls are sufficient to mitigate the risks.
Table 6-1: Does the table contain any information? If there are not risks, ensure there is text in the paragraph above the table describing the test methodology used to make the determination. For example, ISAs were reviewed and interfaces were tested. This is especially important for PaaS and SaaS leveraging other systems.
Section 7: Review all changes in first paragraph for correctness and consistency with the Executive Summary. Review all changes in the last paragraph for a correct recommendation. If this is an initial assessment - the word “continuous improvement” is not applicable and should be removed. This must meet the intent of the attestation and recommendation.
Table 7-1: Does this table include all items listed in Table 4-1, except operationally required and low impact items? Are High items listed first in this table? They may be grouped, but all risks including their unique ID must be included in order of High to Moderate [Low risks are not required to be listed]. Typically, this information contains short excerpts cut and pasted from SSP.
And finally Appendix B: Test Cases - Verify that the information in the Observation and Evidence column for each test case contains the following:
The appropriate assessment method was used - actual examination was done for an examination, actual test for a test, and an actual interview was done.
There is enough detail to determine how the test was completed that also includes, references to artifacts that are provided or otherwise available for review onsite.

- Names, roles, dates and topics discussed for interviews is provided. Sufficient details of observations to determine that the test was completed.
  Sufficient artifacts and evidence is described to support results of the test. If there is text that indicates the test was not completed or the results do not match the test objective, then Column I must indicate “other than satisfied” and Columns J-N must be completed. For example, a result that indicates no account lockout on Widows systems cannot be identified as “satisfied.”
- The FedRAMP PMO will also review the other Appendix attachments as well for verification and adequacy.
- In addition, ensure that the applicable artifact and other documentation is reviewed. For example, the SSP may sufficient for some tests and additional specific artifacts are required for other tests.

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

1.Penetration Guidance

2.NIST 800 53

3.A2LA Website

4.SAP Template