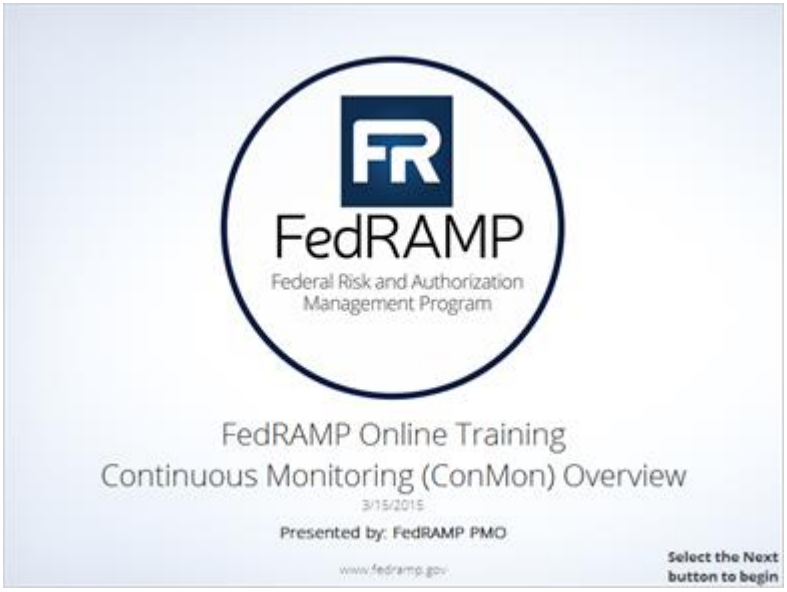
FedRAMP Training - Continuous Monitoring (ConMon) Overview

1. FedRAMP_Training_ConMon_v3_508

1.1 FedRAMP Continuous Monitoring Online Training Splash Screen



Notes:

Transcript

Title <N/A>

Image

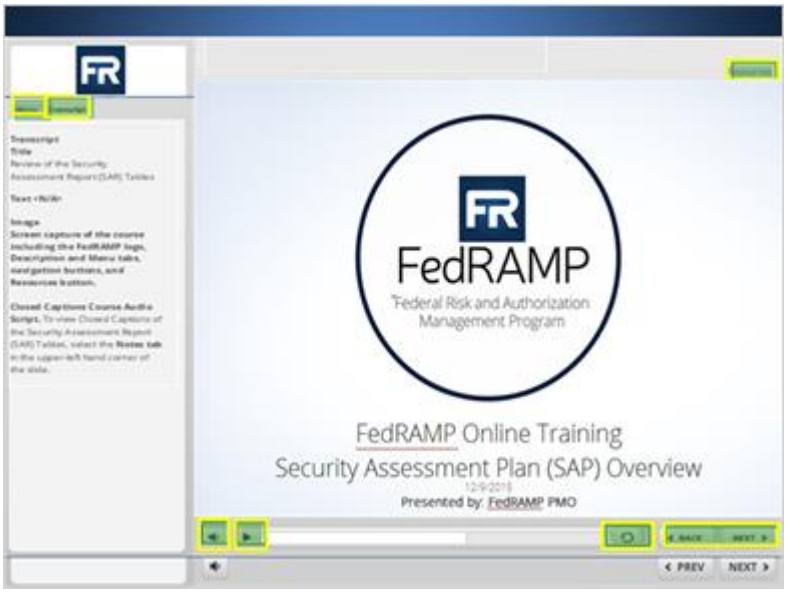
Image of FedRAMP logo.

Text

FedRAMP Online Training; Continuous Monitoring (ConMon). Presented by: FedRAMP PMO.

Select the Next button to begin.

1.2 Course Navigation



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.

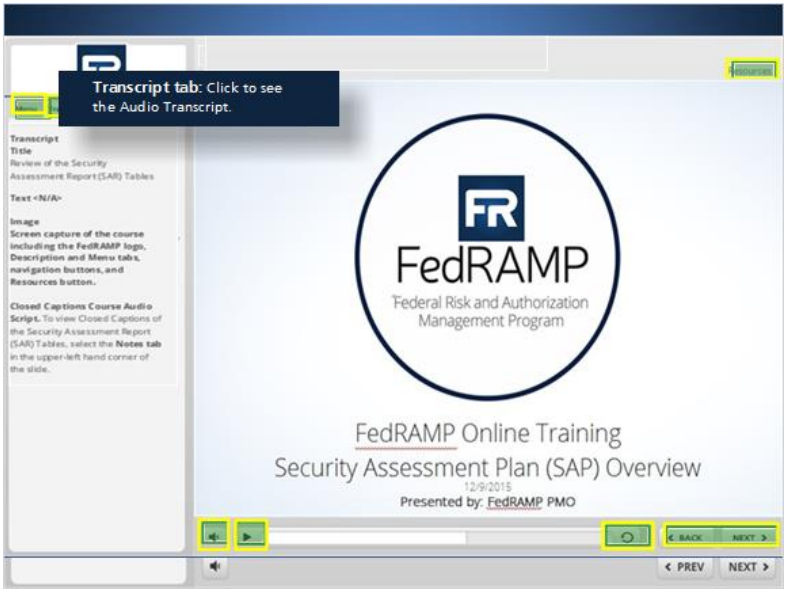
Audio

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.

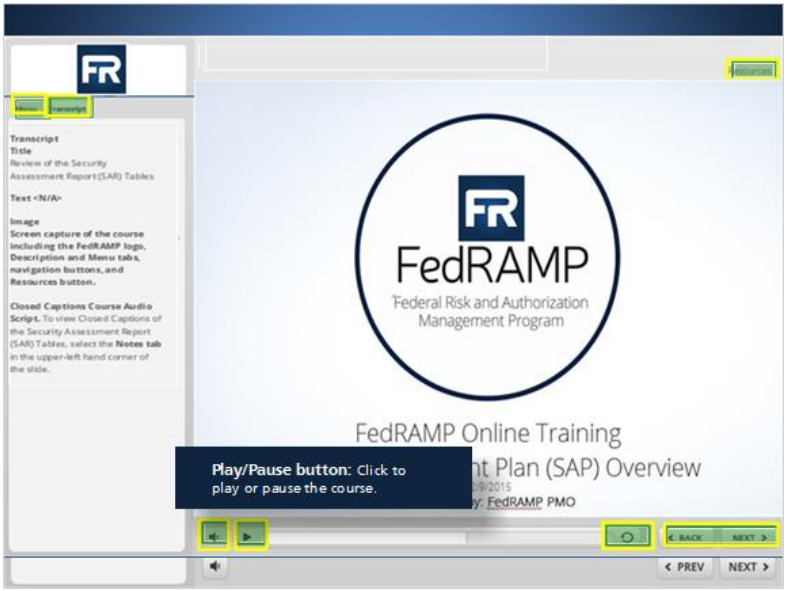
Menu (Slide Layer)

Transcript (Slide Layer)



Resources (Slide Layer)

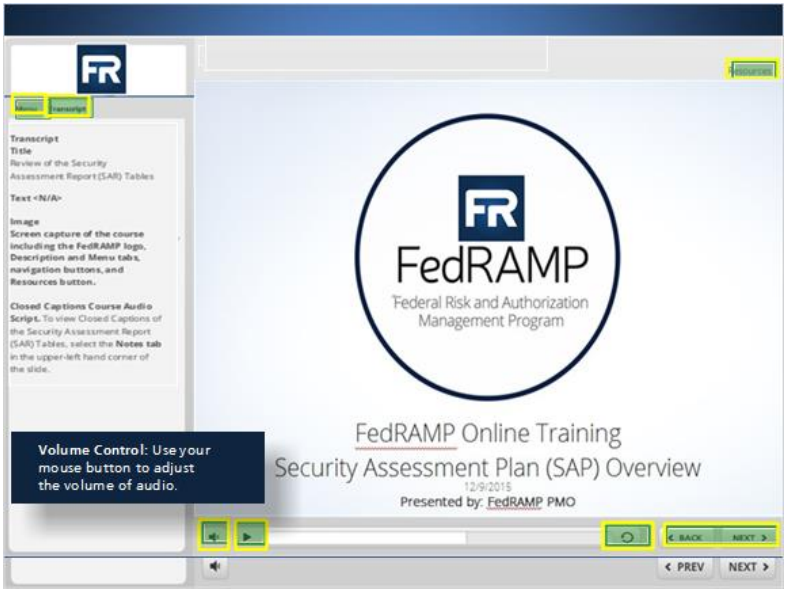
Play/Pause (Slide Layer)



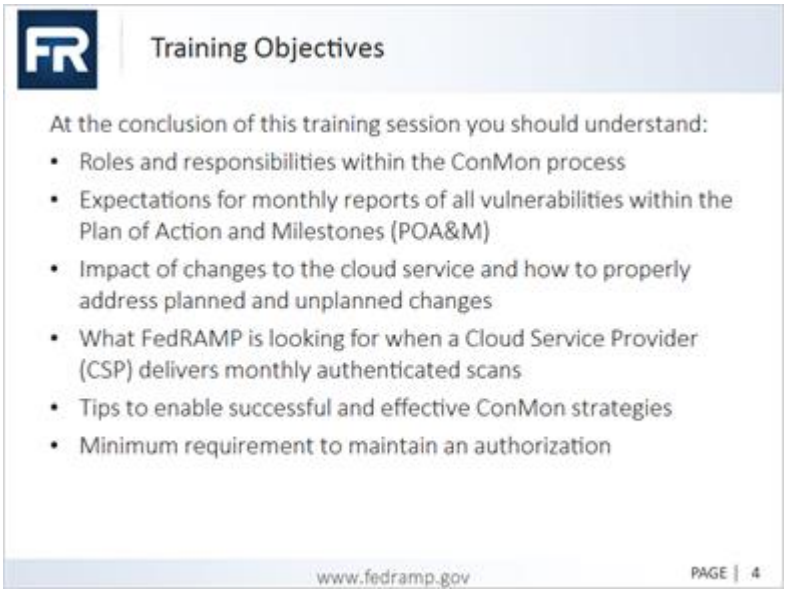
Replay (Slide Layer)

Back/Next (Slide Layer)

Volume Control (Slide Layer)



1.3 Training Objectives



Notes:

Transcript Title

Training Objectives

Image

<N/A>

Text

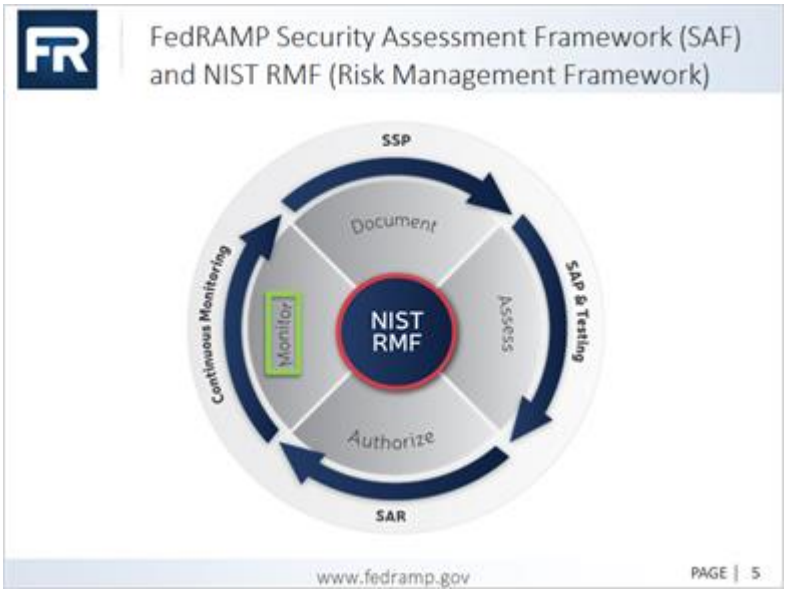
At the conclusion of this training session, you should understand:
- Roles and responsibilities within the ConMon process
- Expectations for monthly reports of all vulnerabilities within the Plan of Action and Milestones (POA&M)
- Impact of changes to the cloud service and how to properly address planned and unplanned changes
- What FedRAMP is looking for when a Cloud Service Provider (CSP) delivers monthly authenticated scans
- Tips to enable successful and effective ConMon strategies

●Minimum requirement to maintain an authorization

Audio

The purpose of our next training module Continuous Monitoring (ConMon) Overview is to provide guidance on continuous monitoring and ongoing authorization in support of maintaining a security authorization that meets the FedRAMP requirements. To maintain an authorization that meets the FedRAMP requirements, CSPs must monitor their security controls, assess them on a regular basis, and demonstrate that the security posture of their service offering is continuously acceptable.

1.4 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 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.
Within the FedRAMP Security Assessment Framework, once an authorization has been granted, the CSP's security posture is monitored according to the assessment and authorization process. Monitoring security controls is part of the overall risk management framework for information security and is a requirement for CSPs to maintain a security authorization that meets the FedRAMP requirements.
Traditionally, this process has been referred to as "Continuous Monitoring" as noted in *NIST SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations*. Other NIST documents such as NIST SP 800-37, Revision 1 refer to "ongoing assessment of security controls". It is important to note that both the terms "Continuous Monitoring" and "Ongoing Security Assessments" mean essentially the same thing and should be interpreted as such.

1.5 What is Continuous Monitoring?

Notes:

Transcript Title

What is Continuous Monitoring?

Image

Continuous Monitoring graphic that describes how ConMon maps to risk tolerance; adapts to ongoing needs; and actively involves management

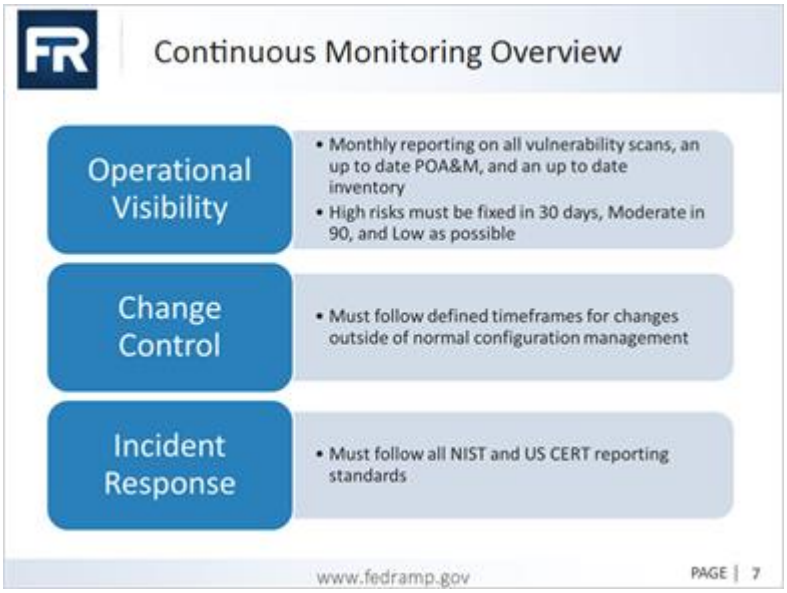
Text

<N/A>

Audio

Performing ongoing security assessments determines whether the set of deployed security controls in a cloud information system remains effective in light of new exploits and attacks, and planned and unplanned changes that occur in the system and its environment over time. To maintain an authorization that meets the FedRAMP requirements, CSPs must monitor their security controls, assess them on a regular basis, and demonstrate that the security posture of their service offering is continuously acceptable.
Ongoing assessment of security controls results in greater control over the security posture of the CSP system and enables timely risk-management decisions. Security-related information collected through continuous monitoring is used to make recurring updates to the security assessment package. Ongoing due diligence and review of security controls enables the security authorization package to remain current which allows agencies to make informed risk management decisions as they use cloud services.
As defined by the National Institute of Standards and Technology (NIST), the process for continuous monitoring includes the following initiatives:
Define a continuous monitoring strategy based on risk tolerance that maintains clear visibility into assets and awareness of vulnerabilities and utilizes up-to-date threat information.
Establish measures, metrics, and status monitoring and control assessments frequencies that make known original security status and detect changes to information system infrastructure and environments of operation, and status of security control effectiveness in a manner that supports continued operation within acceptable risk tolerances.
Implement a continuous monitoring program to collect the data required for the defined measures and report on findings; automate collection, analysis and reporting of data where possible.
Analyze the data gathered and **Report** findings accompanied by recommendations. It may become necessary to collect additional information to clarify or supplement existing monitoring data.
Respond to assessment findings by making decisions to either mitigate technical, management and operational vulnerabilities; or accept the risk; or transfer it to another authority.
Review and **Update** the monitoring program, revising the continuous monitoring strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities; further enhance data driven control of the security of an organization's information infrastructure; and increase organizational flexibility.

1.6 Continuous Monitoring Overview



Notes:

Transcript Title

Continuous Monitoring Overview

Image

Operational Visibility; Change Control; and Incident Response

Text

Operational Visibility

- Monthly reporting on all vulnerability scans, an up to date POA&M, and an up to date inventory
- High risks must be fixed in 30 days, Moderate in 90; and low as possible

Change Control

- Must follow defined timeframes for changes outside of normal configuration management

Incident Response

- Must follow all NIST and US Cert reporting standards

Audio

Three main areas:
Operational Visibility

- An important aspect of a CSP's continuous monitoring program is to provide evidence that demonstrates the efficacy of its program. CSPs and its independent assessors are required to provide evidentiary information to AOs at a minimum of a monthly, annually, every 3 years, and on an as-needed frequency after authorization is granted. The submission of

these deliverables allow AOs to evaluate the risk posture of the CSP's service offering.

- As part of the continuous monitoring process, CSPs are required to have a 3PAO perform an assessment on an annual basis for a subset of the overall controls implemented on the system. During the annual assessment selected controls are tested along with an additional number of controls selected by the AO. The AO has the option to vary the total number of controls tested to meet the desired level of effort for testing.
- CSPs must provide monthly, at a minimum, continuous monitoring deliverables which include vulnerability scans files, an up to date POA&M, and an up to date inventory to authorizing officials for review. These deliverables are really a subset of the evidence required at time of authorization. In this vein, the analysis of these scan results should be performed in the same manner they were for time of authorization. In particular, this means:
  - All scan findings must be documented (including low findings)
  - Each unique vulnerability is tracked as an individual POA&M item. High risks must be fixed in 30 days, Moderate in 90, Low as possible. Late POA&Ms and risk are of high importance to the JAB. This details an inability of vendors to meet the FedRAMP requirements and identifies key risks that agencies should be aware of. Also, a repeated history of late POA&Ms is a key indicator of an ineffective continuous monitoring program and usually also indicates misaligned business processes and operations within a CSP.
  - Deviation requests must be submitted for any requested changes to scan findings (e.g. risk adjustments, false positives, and operational requirements)

Change Control

- Systems are dynamic and FedRAMP anticipates that all systems are in a constant state of change. Configuration management and change control processes help maintain a secure baseline configuration of the CSP's architecture. Routine day-to-day changes are managed through the CSP's change management process described in their *Configuration Management Plan*.
- However, before a planned major significant change takes place, CSP's must perform a Security Impact Analysis to determine if the change will adversely affect the security of the system. The Security Impact Analysis is a standard part of a CSP's change control process as described in the CSP's *Configuration Management Plan*.
- CSPs must notify their AO with a minimum of 30 days before implementing any planned major significant changes. The AOs might require more time based on the severity of the change being implemented so CSPs must work close with the AOs to understand how much time is needed in advance of major changes. CSPs must complete a *Significant Change Security Impact Analysis Form* and provide to the AO for their analysis. All plans for major significant changes must include rationale for making the change, and a Security Assessment Plan (SAP) for testing the change prior to and following implementation in the production system.

  Incident Response

  FedRAMP requires that CSPs demonstrate that they are able to adequately respond to security incidents. As part of the FedRAMP requirements, CSPs are required to submit and maintain an incident response guide, which is approved by the AO. CSPs are also required to follow the incident response and reporting guidance contained in the F*edRAMP Incident Communications Procedure* and must follow all NIST and US CERT reporting standards.

1.7 ConMon Roles and Responsibilities

Notes:

Transcript Title

ConMon Roles and Responsibilities

Image

Authorizing Official (AO)--Agency or Joint Authorization Board (JAB)

Third Party Assessment Organization (3PAO)

Cloud Service Provider

FedRAMP PMO

Text

<N/A>

Audio

Authorizing Officials and their teams (“AOs”) serve as the focal point for coordination of continuous monitoring activities for CSPs. CSPs must coordinate with their AOs to send security control artifacts at various points in time. The AOs monitor both the Plan of Action & Milestones (POA&M) and any major significant changes and reporting artifacts (such as vulnerability scan reports) associated with the CSP service offering. AOs use this information so that risk-based decisions can be made about ongoing authorization. Agency customers must perform the following tasks in support of CSP continuous monitoring:

- Notify CSP if the agency becomes aware of an incident that a CSP has not yet reported
- Provide a primary and secondary POC for CSPs and US-CERT as described in agency and CSP *Incident Response Plans*
- Notify US-CERT when a CSP reports an incident
- Work with CSPs to resolve incidents; provide coordination with US-CERT if necessary

- Notify FedRAMP ISSO of CSP incident activity
- Monitor security controls that are agency responsibilities.

During incident response, both CSPs and leveraging agencies are responsible for coordinating incident handling activities together, and with US-CERT. The team based approach to incident handling ensures that all parties are informed and enables incidents to be closed as quickly as possible.

The FedRAMP Program Management Office (PMO) acts as the liaison for the Joint Authorization Board for ensuring that CSPs with a JAB P-ATO strictly adhere to their established Continuous Monitoring Plan. The JAB and FedRAMP PMO only perform Continuous Monitoring activities for those CSPs that have a JAB P-ATO.

The FedRAMP Policy Memo released by OMB defines the FedRAMP responsibilities to include:

- Assisting government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity
- Coordinating cybersecurity operations and incident response and providing appropriate assistance
- Developing continuous monitoring standards for ongoing cybersecurity of Federal information systems to include real-time monitoring and continuously verified operating configurations
- Developing guidance on agency implementation of the Trusted Internet Connection (TIC) program for cloud services.

The FedRAMP PMO works with DHS to incorporate DHS's guidance into the FedRAMP program guidance and documents.

Third Party Assessment Organizations (3PAO) are responsible for independently verifying and validating the control implementation and test results for CSPs in the continuous monitoring phase of the FedRAMP process. Specifically, 3PAOs are responsible for:

- Assessing a defined subset of the security controls annually.
- Submitting the assessment report to the ISSO one year after the CSP's authorization date and each year thereafter.
- Performing announced penetration testing.
- Perform annual scans of web applications, databases, and operating systems. Assessing changed controls on an ad hoc basis as requested by the AOs for any changes made to the system by the CSP.

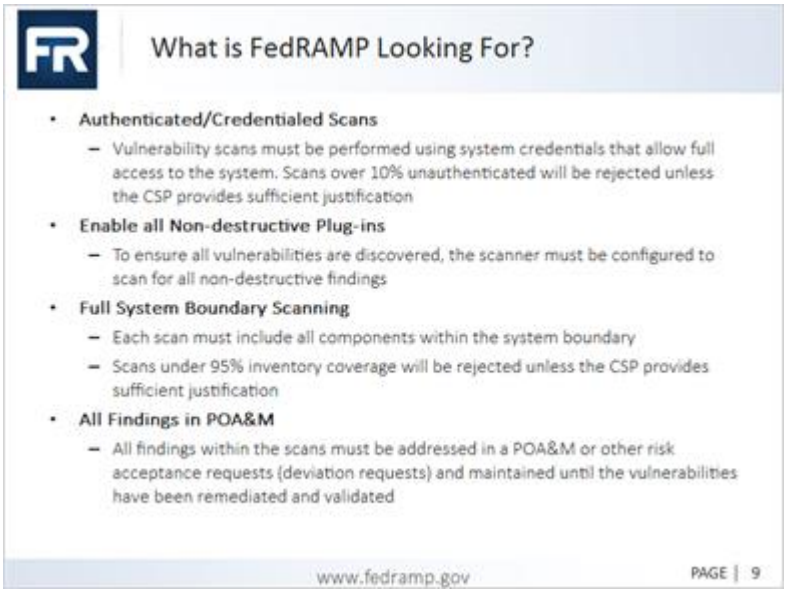
In order to be effective in this role, 3PAOs are responsible for ensuring that the chain of custody is maintained for any 3PAO authored documentation. 3PAOs must also be able to vouch for the veracity and integrity of data provided by the CSP for inclusion in 3PAO authored documentation. As an example: If scans are performed by the CSP, the 3PAO must either be on site and observe the CSP performing the scans or be able to monitor or verify the results of the scans through other means documented and approved by the AO.

Documentation provided to the CSP must be placed in a format that either the CSP cannot alter or that allows the 3PAO to verify the integrity of the document.

The CSP is responsible for: Submitting quality documentation in support of their FedRAMP application. This includes timely delivery of monthly POA&Ms. CSPs must provide monthly reports of all vulnerability scanning to authorizing officials for review and tracking these vulnerabilities within the POA&Ms.

- All scan findings must be documented (including low findings)
- Each unique vulnerability is tracked as an individual POA&M item
- Deviation requests must be submitted for any requested changes to scan findings (e.g. risk adjustments, false positives, and operational requirements)
- In addition, CSPs must work closely with an independent third party assessor to perform initial and annual assessments and,
- Maintain its authorization by complying with continuous monitoring requirements.

1.8 What is FedRAMP Looking For?



Notes:

Transcript Title

What is FedRAMP Looking For?

Image

<N/A>

Text

- **Authenticated/Credentialed Scans**
  - Vulnerability scans must be performed using system credentials that allow full access to the system. Scans over 10% unauthenticated will be rejected unless the CSP provides sufficient justification
- **Enable all Non-destructive Plug-ins**
  - To ensure all vulnerabilities are discovered, the scanner must be configured to scan for all non-destructive findings
- **Full System Boundary Scanning**
  - Each scan must include all components within the system boundary
  - Scans under 95% inventory coverage will be rejected unless the CSP provides sufficient justification
- **All Findings in POA&M**
  - All findings within the scans must be addressed in a POA&M or other risk acceptance requests (deviation requests) and maintained until the vulnerabilities have been remediated and validated

Audio

- **Authenticated/Credentialed Scans**
  - Vulnerability scans must be performed using system credentials that allow full access to the system. Scans over 10% unauthenticated will be rejected unless the CSP provides sufficient justification
- **Enable all Non-destructive Plug-ins**
  - To ensure all vulnerabilities are discovered, the scanner must be configured to scan for all non-

destructive findings

- **Full System Boundary Scanning**
  - Each scan must include all components within the system boundary
  - Scans under 95% inventory coverage will be rejected unless the CSP provides sufficient justification
- **All Findings in POA&M**
  - All findings within the scans must be addressed in a POA&M or other risk acceptance requests (deviation requests) and maintained until the vulnerabilities have been remediated and validated

1.9 Additional Tips

Notes:

Transcript Title

Additional Tips

Image

Image blocks that contain:

1. Reconcile monthly POA&M findings with the scan results to ensure accuracy

2. All findings must be recorded on the open tab of the POA&M

3. Select your monthly ConMon scan and Plan of Action & Milestones (POA&M) delivery date wisely

4. Ensure monthly scans are in sync with your patch cycle to avoid artificial inflation of reported vulnerabilities

5. Scans that reflect non-applicable issues will require proper management and remediation

6. Every vulnerability must be addressed

Text

1. Reconcile monthly POA&M findings with the scan results to ensure accuracy

2. All findings must be recorded on the open tab of the POA&M

3. Select your monthly ConMon scan and Plan of Action & Milestones (POA&M) delivery date wisely

4. Ensure monthly scans are in sync with your patch cycle to avoid artificial inflation of reported vulnerabilities

5. Scans that reflect non-applicable issues will require proper management and remediation

6. Every vulnerability must be addressed

Audio

When submitting the monthly Plan of Actions and Milestones (POA&M) spreadsheet, the findings on the spreadsheet must be reconciled each month with the scan results to ensure POA&M accuracy. This means that any items that have closed throughout the month should be marked as such, and appropriate artifacts are provided to validate closure. It is important to stick to the template, don't add any extra columns or changing the way the data is entered.

All findings must be recorded on the open tab of the POA&M. A false positive (FP) vulnerability remains in the open tab until the deviation request (DR) is approved by the JAB. An operationally required (OR) vulnerability remains on the open tab indefinitely and is only closed if the circumstances creating the OR are resolved such as migration to a new technology. A vendor dependency also remains on the open tab indefinitely and is only closed once the CSP resolves the issue by applying a vendor approved fix or upgrade.

Select your monthly ConMon scan and Plan of Action & Milestones (POA&M) delivery date wisely. Consider vendor patch release schedules and your typical duration between the release of a vendor patch and its application within your environment. Plan your scans as soon as possible after patches are typically applied each month. The monthly con mon delivery date is decided upon prior to starting con mon, and the expectation is that a complete package is supplied prior to each month's due date, and if that is not possible then an adequate explanation and plan of action is given to the ISSO. Ideally, it is not acceptable to be providing last minute DR's or re-scans in order to fix problems found in the deliverable.

If your monthly scans are out-of-sync with your patch cycle, the number of vulnerabilities reported can be artificially inflated.

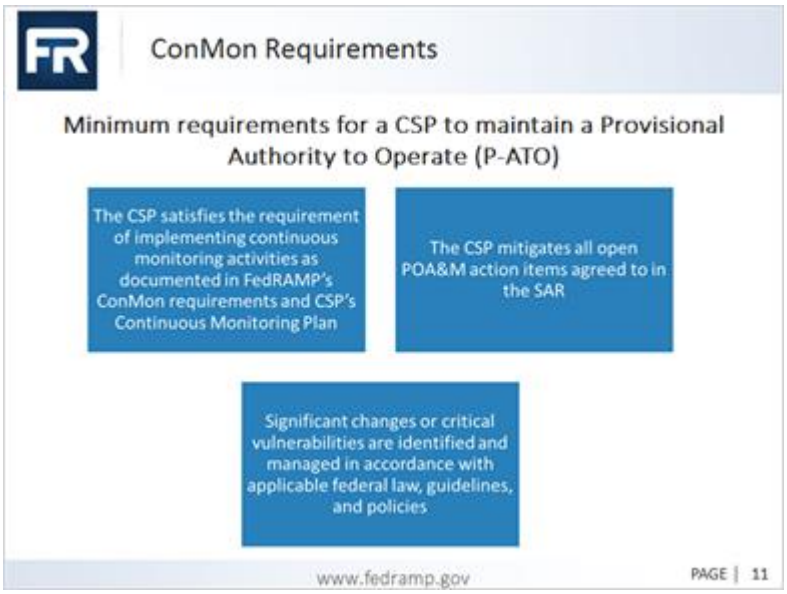
For example, if you have Microsoft-based hosts and a two week patch cycle, running scans just one week after "patch Tuesday" will report all of the newly released patches as new vulnerabilities on those hosts and inflate your vulnerability count. Scanning shortly after your patch cycle gives your admins time to remediate all of those new vulnerabilities. Therefore, only the exceptions - if any - are reported.

If a CSP submits Continuous Monitoring (ConMon) scans that reflect non-applicable issues, those findings will require proper management and remediation. For example, if you run Payment Card Industry (PCI) or Personally Identifiable Information (PII) compliance scans on a system that is not authorized to manage this type of information, the findings are irrelevant and will have to be properly managed and remediated. Scans must be delivered using the same tools as what was in the SAR, in a parseable format, and in the same format each month, unless ample notice is given by the CSP to the ISSO in order for FedRAMP to be able to create a new parser for Automated scanning.

Once submitted as part of your ConMon data, every vulnerability must be addressed through one of four possibilities:

- Remediate the finding within the required timeframe. Optionally, you can apply a mitigation and request a risk adjustment if you believe that the risk is higher/lower than the scanner rating.
- Seek approval as a false positive (FP), which can only happen if you can provide evidence that the finding is not accurate.
- Seek approval as an operational requirement (OR). Optionally, you can apply a mitigation and request a risk adjustment, which can also strengthen your justification. You cannot request an OR as a high, it must be at least mitigated down to a moderate.
- Justify the finding as a vendor dependency and check-in with the vendor every 30 days. In this case, the vulnerability will not be considered late.

1.10 ConMon Requirements



Notes:

Transcript Title

Minimum requirements for a CSP to maintain a Provisional Authority to Operate (P-ATO)

Image

Image blocks that contain:

1. The CSP satisfies the requirement of implementing continuous monitoring activities as documented in FedRAMP

2. The CSP mitigates all open POA&M action item agreed in the SAR

3. Significant changes or crucial vulnerabilities are identified with applicable federal law, guidelines, and policies.

Text

1. The CSP satisfies the requirement of implementing continuous monitoring activities as documented in FedRAMP

2. The CSP mitigates all open POA&M action item agreed in the SAR

3. Significant changes or crucial vulnerabilities are identified with applicable federal law, guidelines, and policies.

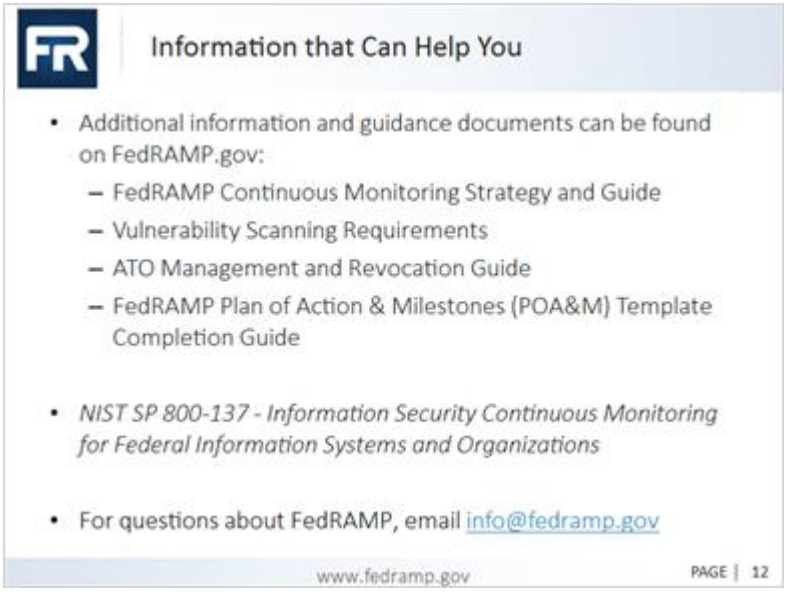
Audio

When a CSP receives a Provisional Authority to Operate (P-ATO) for its cloud system, it comes with the

following minimum requirements:
1. The CSP satisfies the requirement of implementing continuous monitoring activities as documented in FedRAMP's continuous monitoring (ConMon) requirements and CSP's Continuous Monitoring Plan;
2. CSP mitigates all open POA&M action items, agreed to in the Security Assessment Report (SAR); and
3. Significant changes or critical vulnerabilities are identified and managed in accordance with applicable Federal law, guidelines, and policies.

If a CSP fails to meet the FedRAMP ConMon requirements described in the FedRAMP Continuous Monitoring Strategy Guide, FedRAMP will initiate an escalation process. The severity and scope of the change in the cloud system's risk posture will define the escalation action taken by FedRAMP. Details of the escalation process can be found in the FedRAMP P-ATO Management and Revocation Guide which can be found on FedRAMP.gov or on the Resource button in this training module.

1.11 Information that Can Help You



Notes:

Transcript Title

Information that Can Help You

Image

<N/A>

Text

- Additional information and guidance documents can be found on FedRAMP.gov:
  - FedRAMP Continuous Monitoring Strategy and Guide
  - Vulnerability Scanning Requirements
  - ATO Management and Revocation Guide
  - FedRAMP Plan of Action & Milestones (POA&M) Template Completion Guide
- *NIST SP 800-137 - Information Security Continuous Monitoring for Federal Information Systems and Organizations*

- For questions about FedRAMP, email info@fedramp.gov

1.12 Untitled Slide

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