



FedRAMP Online Training Security Assessment Report (SAR) Overview

12/9/2015

Presented by: FedRAMP PMO



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. Third Party Assessment Organization (3PAO) New Requirements
 7. Significant Change Training for CSPs
- 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.



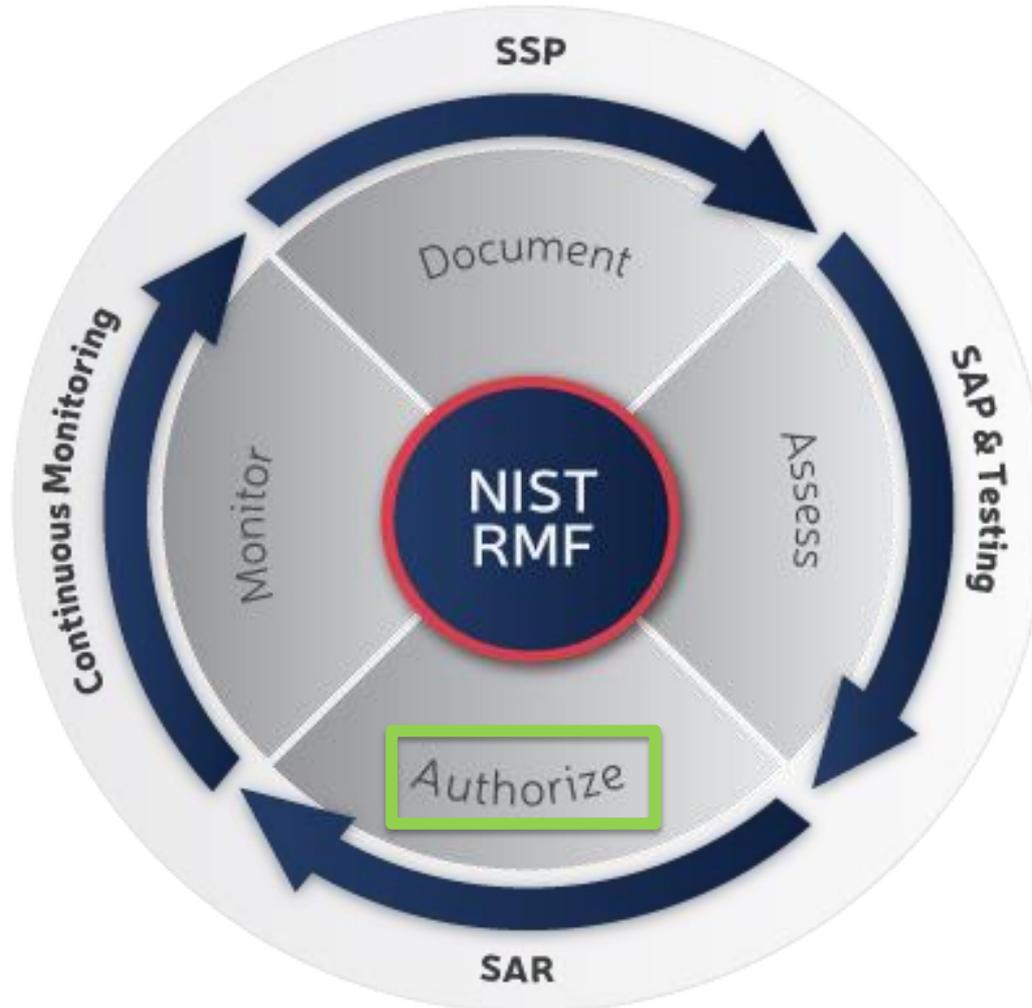
Training Objectives

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 Actions 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



FedRAMP Security Assessment Framework(SAF) and NIST RMF (Risk Management Framework)





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



Assessment Methodology

Reflective of the
agreed-upon SAP

Customized to correct
identified weaknesses
and validate those
corrections



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



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



Security Assessment Results

Affected IP Address/Hostname(s)/Database

- All affected IP addresses/hostnames/databases must be included

Applicable Threats

- Describes the unique threats that have the ability to exploit the security vulnerability

Likelihood, Impact and Risk Exposure

- Before and after mitigating control/factors have been identified and considered

Risk Statement

- Describes the risk to the business



Mitigating Controls/Factors

- Indicate whether the affected machines are internally or externally facing

Recommendation

- Describes how the vulnerability must be resolved

Justification or Proposed Remediation

- Provide a rationale for recommendation of risk adjustment or operational requirement



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



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



POA&M Objectives

- Primary mechanism for tracking all system security weaknesses and issues
- Facilitates a disciplined and structured approach to mitigating risks in accordance with the CSP's priorities

CSP Action

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

Mitigation Plan

- High < 30 Days
- Moderate < 90 Days
- Low – CSP Determined



The POA&Ms are based on:

- 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:

- The tasks the CSP plans to accomplish with a recommendation for completion either before or after information system implementation
- Any milestones the CSP has set in place for meeting the tasks
- The scheduled completion dates the CSP has set for the milestones



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

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

3PAO Action

CSP Action





Initial and Detailed Reviews

- Completeness
- Showstoppers
- Common Problems
- Critical Controls



Key Documentation Checks

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

Section 3: Are there any modifications to this section?

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.

Table 5-3: Ensure that the mitigating factors and compensating are sufficient to mitigate the risks.

Table 6-1: Does the table contain any information?

Section 7: Review all changes in first paragraph for correctness and consistency with the Executive Summary.

Table 7-1: Does this table include all items listed in Table 4-1, except operationally required and low impact items?

Appendix B: Test Cases – Verify that the information in the Observation and Evidence column for each test case contains sufficient information.



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