



FedRAMP Online Training Security Assessment Plan (SAP) 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. How to Write to a Control
 7. Continuous Monitoring Overview
- 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.

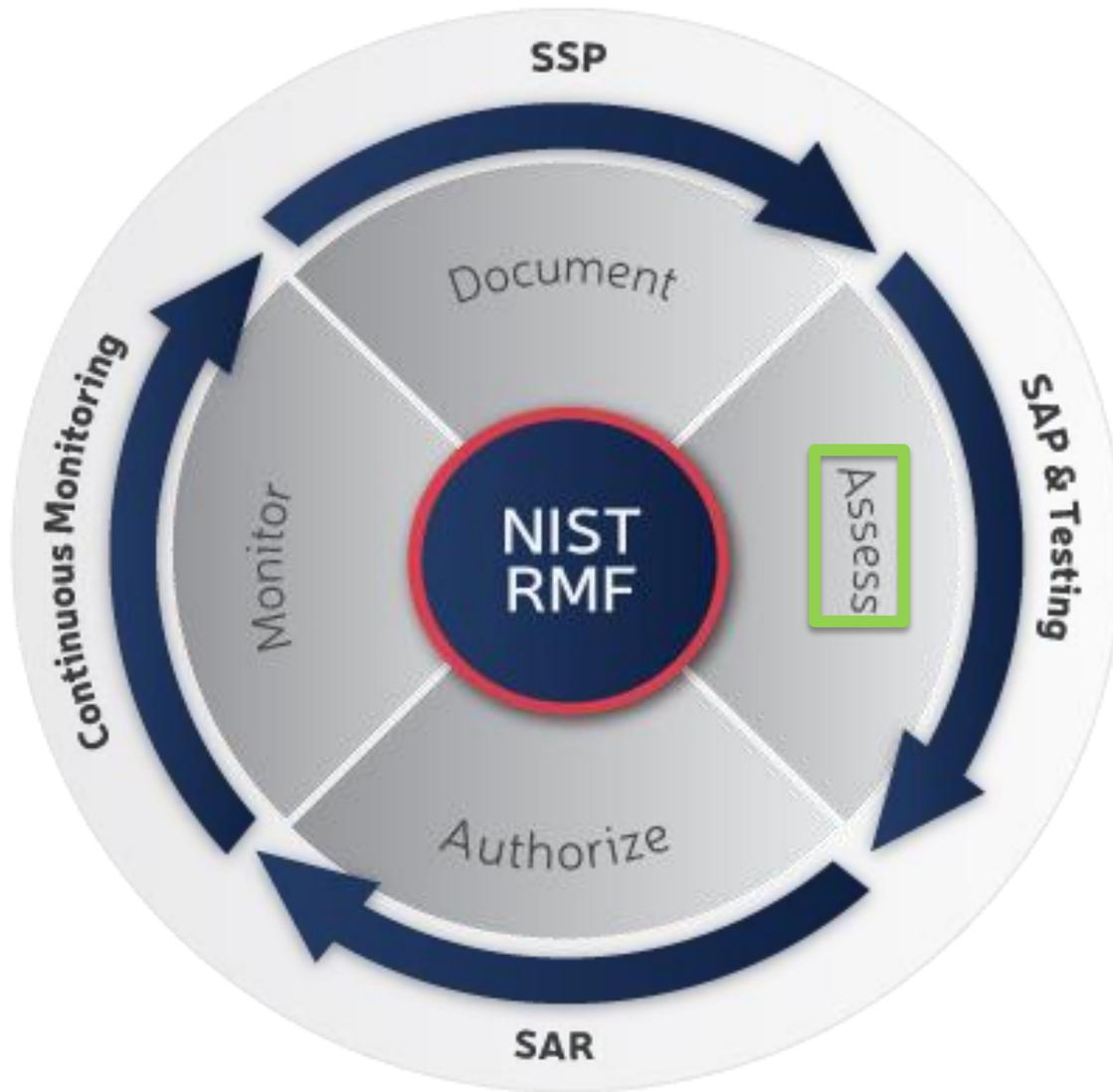


Training Objectives

- At the conclusion of this training session you should understand:
 - The relationship between the 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



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





Role of a 3PAO



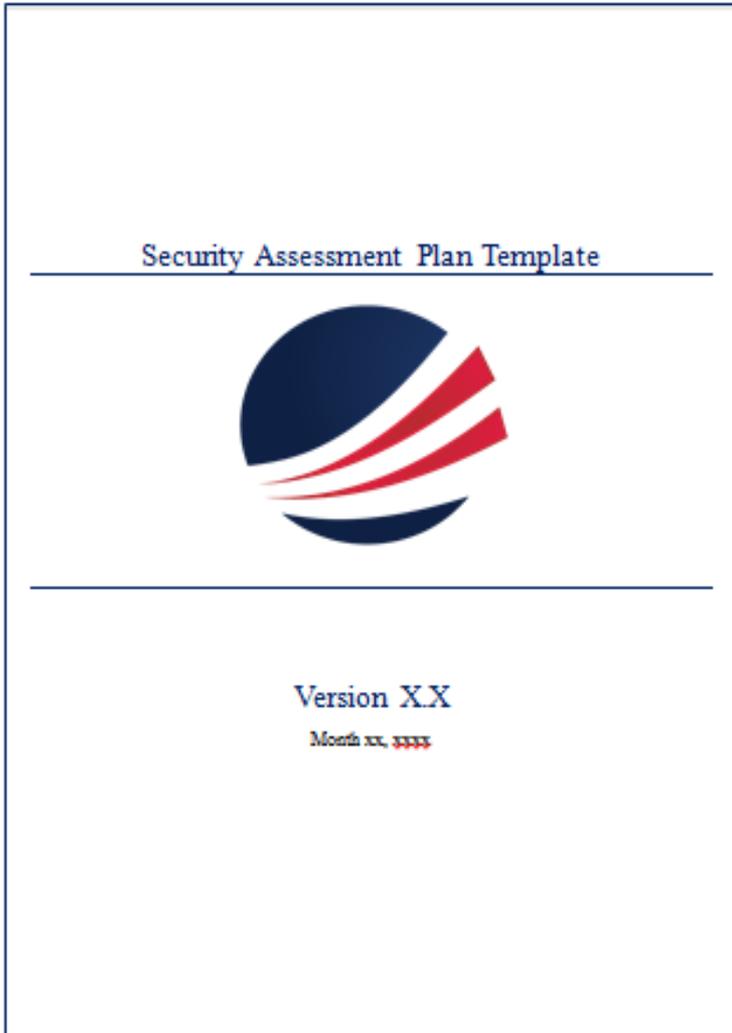


Role of a 3PAO

- 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



SAP Template



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



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



Scope and Assumptions

Scope Identification

- Physical locations of all the different components
- IP addresses, and network ranges, of the system
- Web based applications and the logins
- Databases
- Functions and roles

Assumptions

- Dependencies on resources
- Appropriate login account information / credentials
- Access to hardware, software, systems, and networks
- 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



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.



Examine

- Reviewing, inspecting, observing, studying, or analyzing one or more assessment objective
- Gain an understanding, clarification, or evidence

Interview

- Holding discussions
- Gain an understanding, clarification, or evidence

Test

- Exercising objects under specified conditions
- To compare actual with expected behavior



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



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



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



Initial and Detailed Reviews

- Completeness
- Showstoppers
- Common Problems
- Critical Controls



Key Documentation Checks

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?

Table 2-3: Does this table include IP addresses for the complete inventory?

Table 2-4: Does this table include all web applications (URLs) for the complete inventory?

Table 2-5: Does this table include all database applications for the complete inventory?

Table 2-6: Are functions for each of the roles defined in enough detail to determine the testing that will be done?

Section 3: Have any assumptions been changed, deleted, or added.

Table 5-1: Does the “role” description provide information about what the tester will actually be doing, for example, penetration testing, vulnerability scanning?

Table 5-2: Does the “role” description provide information about what the CSP POC will be doing for these tests?

Table 5-3: Does the list of tools include a detailed description of what the tools will be used to test within the system?

Table 5-4: Does this table include manual tests that may be required for items that cannot be tested using automated tools?

Table 5-5: Does the schedule match the ISSO project schedule?



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