RMF Stage 4 – Assessing Controls (Part Two)

Reading

45m

Status | Incomplete

Introduction

In the last reading, you looked at the first two tasks of the Assess RMF stage: *Developing Security Assessment Plan* and *Assessing Control Compliance*. In this reading, you will look at the next two tasks of this stage: *Preparing Security Assessment Report* and *Conducting Remediation*.

Reading

Read pages 32 and 33 of the *Guide for Applying the Risk Management Framework to Federal Information Systems* prepared by NIST to understand the third and fourth tasks of the RMF Assess stage, *Prepare Security Assessment Report* and *Conduct Remediation*.

While reading, focus on the following key information:

- Who is primarily responsible for developing the security assessment report in an SOC
- What important information is covered in the security assessment report
- How the report provides visibility into specific weaknesses and deficiencies in the security controls employed
- How remediation actions are decided based on the findings and recommendations in the security assessment report

> Security Control Assessor (SCA) and Security Control Assessment Representative (SCAR) are two key roles at the Assessing Controls stage of the RMF. Read the information given below to understand the difference between the two roles.

SCA vs. SCAR

- An SCA is always an individual and is appointed by CIO. The tasks (as specified below) that are assigned to the SCA may not be delegated. Also, an SCA is the individual authorized to sign the final Security Assessment Report.
- A SCAR, on the other hand, could be an individual or organization and is appointed by an SCA. They assist SCAs:
  - Assesses control compliance
  - Assesses mitigations
  - Prepares draft Security Assessment Report

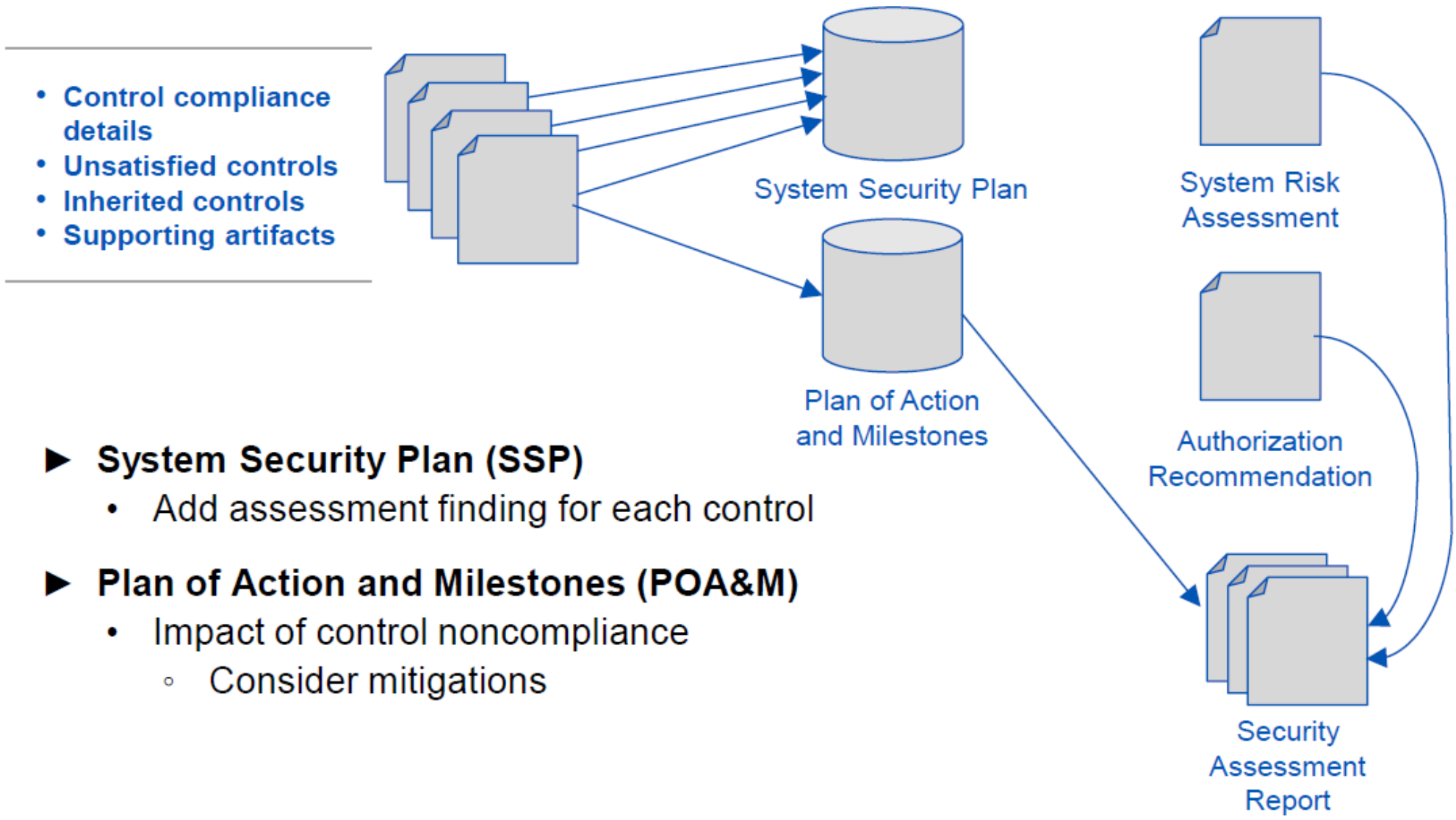

Fig 1: Process to document the Assessing Control Compliance Step

NIST SP 800-53 provides a framework for managing and securing information systems within federal agencies. In stage four of the RMF, controls are assessed to determine their effectiveness in mitigating risk. The following are the steps for documenting the Assessing Control Compliance step:

1. **Document the assessment results**: the assessment results should be documented in a format that allows for easy review and analysis. This documentation should include the control objectives, the assessment methodology, and the results of the assessment.
2. **Identify any control deficiencies**: if any control deficiencies are identified during the assessment, they should be documented in detail. This documentation should include the specific control that is deficient, the severity of the deficiency, and any recommended remediation actions.
3. **Review and approve the assessment results**: the assessment results should be reviewed and approved by the appropriate stakeholders, including the system owner, the authorizing official, and any other relevant parties.
4. **Update the SSP**: any changes to the security controls resulting from the assessment should be documented in the SSP. The updated SSP should reflect the new security posture of the system.
5. **Update the Plan of Action and Milestones (POA&M)**: if any control deficiencies are identified, a POA&M should be developed to address them. The POA&M should include specific remediation actions, timelines, and responsible parties.
6. **Document any residual risk**: the residual risk associated with the assessed controls should be documented. This documentation should include the level of residual risk, the rationale for accepting this risk, and any risk mitigation strategies that will be implemented.
7. **Prepare the final assessment report**: the final assessment report should document the assessment results, control deficiencies, and any remediation actions or risk mitigation strategies. The report should be reviewed and approved by the appropriate stakeholders before being submitted for authorization.

Conclusion

You learned in the Assessing Controls readings (parts one and two) that the purpose of the Assess step helps determine if the selected security and privacy controls are implemented correctly, operate as intended, produce the desired outcome, and meet organizational or system security and privacy requirements. In the upcoming unit, you will learn about the next stage of the RMF: *Authorize*.

✓ Mark Completed

Previous
RMF Stage 4 – Assessing Controls (Part One)

Next
GRC Quiz 2

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W05D1

Mon Jul 22

Lectures (1)

Work (8)

7 hrs

- Risk Management Methodology Document
- RMF Stage 4 – Assessing Controls (Part One)
- RMF Stage 4 – Assessing Controls (Part Two)
- GRC Quiz 2
- RMF Stage 5 - Authorizing Information Systems
- Conducting Residual Risk Assessment
- RMF Stage 6 - Monitoring Security Controls
- Writing Statement of Applicability (SOA)

W05D1 Schedule »