STUDENT GUIDE
Risk Management Framework –
Step 4: Assessing Security Controls

Slide 1 - Risk Management Framework

Welcome to Risk Management Framework –Lesson 4 - RMF Step 4: Assessing Security Controls.

Once the security controls are implemented they must be assessed, the results documented in the Security Assessment Report, and remediation efforts completed.

Slide 2 - Objectives

By the end of this lesson you should be able to:

- Develop and approve a security assessment plan
- Assess security controls based on the plan
- Document security assessment results
- Conduct remediation activities

Slide 3 - Sources

The authoritative sources listed here are to be used for Security Control Assessment Guidance:

- DoDI 8510.01 dated March 2014 is the high level document that sets forth the policy stating RMF is to be used by DoD
- NIST Special Publication 800-37 is the Guide for Applying RMF to Federal Information Systems
- The RMF Knowledge Service at https://rmfks.osd.mil/rmf is the go-to source when working with RMF

Slide 4 - Security Controls Assessment

- Assessment procedures are used to verify that a security control has been properly implemented
- One or more assessment procedures that describe requisite preparatory steps and conditions, actual assessment steps and expected results have been developed for each security control
- Each procedure includes supporting background material, sample results, or links to automated testing tools
- Assessment procedures are maintained by the RMF Technical Advisory Group and published on the Security Controls Explorer page and eMASS

If you already use eMASS to help with security control assessment you should continue to do so.

Slide 4a - RMF Knowledge Service Security Control Explorer

Here we have a subset of controls using the security control explorer in the RMF Knowledge Service site. By clicking one of the control acronyms we can see the assessment procedures.

Slide 4b - Assessment Procedures

After clicking a specific control, expand the Implementation Guidance and Assessment Procedures link to see the assessment procedures for that particular control.

Slide 5 – Who Are The Players?

There are four tasks that comprise step 4 of the RMF. The Security Control Assessor or SCA has Primary Responsibility for all tasks, while the Information System Owner and Common Control Provider also share a Primary Responsibility with the SCA for the fourth task.

These individuals have supporting roles at various times throughout the process: Authorizing Official or their Designated Representative, Chief Information Officer, Senior Information Security Officer, Information System Owner, Common Control Provider, Information Owner/Steward and Information System Security Officer or ISSO.

Slide 6 - Task 4-1 Develop and Approve a Security Assessment Plan - Key Activities

Now let's take a closer look at Task 1. The SCA develops the security assessment plan, and the Authorizing Official or their Designated Representative reviews and approves the plan. The purpose of the security assessment plan is to establish the appropriate expectations for the security control assessment and bound the level of effort for the assessment.

From an organizational perspective, preparing for a security control assessment includes the following key activities:

- Ensuring that appropriate policies covering security control assessments are in place and understood by all affected organizational elements
- Ensuring that all steps in the RMF prior to the security control assessment step have been successfully completed and received appropriate management oversight

- Ensuring that security controls identified as common controls (and the common portion of hybrid controls) have been assigned to appropriate organizational entities (such as common control providers) for development and implementation, and

- Establishing the objective and scope of the security control assessment, the purpose of the assessment and what is being assessed

Slide 7 - Task 4-1 Develop and Approve a Security Assessment Plan - Steps

An approved security assessment plan helps to ensure that an appropriate level of resources is applied toward determining security control effectiveness. When security controls are provided to an organization by an external provider (such as through contracts, licensing agreements, etc.), the organization obtains a security assessment plan from the provider.

The following steps are considered by assessors in developing plans to assess security controls in organizational information systems or security controls inherited by those systems:

- Determine which security controls and control enhancements are to be included in the assessment based upon the contents of the security plan and the scope of the assessment
- Select the appropriate assessment procedures to be used during the assessment based on the security controls and control enhancements that are to be included in the assessment
- If required, tailor the selected assessment procedures. For example, select appropriate assessment methods and objects, assign depth and coverage attribute values
- Optimize the assessment procedures to reduce duplication of effort. For example, sequencing, consolidating assessment procedures, and reusing DT&E and OT&E test results
- Provide cost-effective assessment solutions, and
- Finalize the assessment plan and obtain the necessary approvals to execute the plan

The SCA ensures the plan is consistent with the security objectives of the organization; employs state-of-the-practice tools, techniques, procedures, and automation to support the concept of information security monitoring and near real-time risk management; and is cost-effective with regard to the resources allocated for the assessment.

The Authorizing Official or their Designated Representative approves the security assessment plan, establishes appropriate expectations for the security control assessment, defines the level of effort for the assessment, and ensures the appropriate level of resources are applied in determining the effectiveness of the security controls.

Slide 8 - Task 4-2 Assess Security Controls

In Task 4-2 we assess the security controls in accordance with assessment procedures defined in the security assessment plan. Security control assessments determine the extent to which the controls are

implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for the information system. Assessments occur as early as ~~practicable~~ practical in the system development life cycle, preferably during the development phase of the information system. Related activities may include design and code reviews, application scanning, and regression testing.

Organizations consider both the *technical expertise* and level of *independence* required in selecting security control assessors. Organizations also ensure that security control assessors possess the required skills and technical expertise to successfully carry out assessments of system-specific, hybrid, and common controls.

Slide 9 - Task 4-2 Security Control Assessor

The information system owner relies on the technical expertise and judgment of assessors to:

- Assess the security controls employed within or inherited by the information system using assessment procedures specified in the security assessment plan, and
- Provide specific recommendations on how to correct weaknesses or deficiencies in the controls and reduce or eliminate identified vulnerabilities

The assessor findings are ~~an~~ unbiased, factual reporting of the weaknesses and deficiencies discovered during the security control assessment.

The organization ensures that assessors have access to:

- The information system and environment of operation where the security controls are , and
- The appropriate documentation, records, artifacts, test results, and other materials needed to assess the security controls

Slide 10 - Task 4-2 Assessment Results

SRG and STIG compliance results will be documented and used as part of the overall security control assessment. The RMF Knowledge Service is the authoritative source for security control assessment procedures. Actual results are recorded in the SAR and POA&M as part of the security authorization package, along with any artifacts produced during the assessment (for example, output from automated test tools or screen shots that depict aspects of system configuration).

In order to make the risk management process as timely and cost-effective as possible the reuse of previous assessment results, when reasonable and appropriate, is strongly recommended. Assessment results are reused to support reciprocity wherever possible.

For inherited security controls, assessment test results and supporting documentation are maintained by the providing system and are made available to SCAs of receiving systems when requested. For common controls inherited from the enterprise, instructions for documenting compliance are provided on the RMF Knowledge Service. SCAs will maximize the reuse of existing assessment and T&E documentation in their assessment of the system.

Slide 11 - Task 4-2 Compliance Status

When assessing security control compliance status:

- If no vulnerabilities are found through the process of executing the assessment procedures the security control is recorded as compliant
- If vulnerabilities are found the control is recorded as non-compliant or NC in the Security Assessment Report, with sufficient explanation
- If a security control is found to be not technically or procedurally relevant to the system, as determined by the Authorizing Official, an NA for Not Applicable is recorded in the Security Assessment Report, with sufficient justification

Not achieving expected results for all assessment procedures does not equate to unacceptable risk. However, all NC security controls must be assessed for risk and documented in a POA&M with an explanation as to how and when they will be fixed and/or mitigated. Also please note that any assessment procedures used that are not in accordance with the RMF Knowledge Service will be documented fully in the Security Assessment Report.

Slide 12 - Task 4-2 Record Results

Compliance status, justification for NC and NA, risk and comments can be added to the SAR tab of the Security Authorization Package. This spreadsheet template can be downloaded from the RMF Knowledge Service web site link shown on the screen. These results can also be stored in eMass. If you are currently using eMass you should continue to do so.

Slide 13 - Task 4-2 Determine Risk Level

The Security Control Assessor or SCA determines and documents in the SAR a risk level for every NC security control in the system baseline. NC controls are subjected to a risk assessment process that

considers multiple factors in producing the risk level. As described in the NIST Special Publication 800-30, "Guide for Conducting Risk Assessments," these factors include, but are not limited to:

- The SCA's determination that a credible or validated threat source and potential event exists that is capable of, and likely to, exploit vulnerabilities in the implementation of the control
- Vulnerability severity level and pre-disposing conditions. This includes the SCA's estimate of the adequacy of existing mitigations or compensating controls to address the vulnerability and mitigations provided by the hosting enclave, CNDSP, or other protective measures
- The cybersecurity attribute (that is confidentiality, integrity, or availability) and associated categorization impact level (high, moderate, and low) related to the control
- The SCA's estimate of impact of a successful threat event

The SCA must also determine and document in the SAR an assessment of overall system level of risk. The risk assessment must address all NC controls, and clearly communicate the SCA's conclusion on system cybersecurity risk, along with any recommendations for special instructions to accompany the authorization decision.

Slide 14 - Task 4-2 POA&M

All NC security controls must be documented in a POA&M with an explanation as to how and when they will be fixed and/or mitigated. POA&M information can be added to the POA&M tab of the Security Authorization Package. This spreadsheet template can be downloaded from the RMF Knowledge Service web site link shown on the screen.

POA&M information can also be stored in eMass. If you are currently using eMass you should continue to do so.

Slide 15 – Task 4-3 Security Assessment Report

A Security Assessment Report or SAR is always required before an authorization decision. The SAR documents the issues, findings, and recommendations from a security control assessment. It addresses security controls in a Non-Compliant or NC status, including existing and planned mitigations. A SAR is always required before an authorization decision. If a compelling mission or business need requires the rapid introduction of a new information system or Platform IT system, both the assessment activity and corresponding SAR are still required.

Organizations may choose to develop an executive summary from the detailed findings generated during a security control assessment. An executive summary provides the authorizing official with an abbreviated version of the assessment report focusing on the highlights of the assessment, synopsis of

key findings, and/or recommendations for addressing weaknesses and deficiencies in the security controls.

Slide 16 - Task 4-3 RMF Knowledge Service SAR

Here we see a snapshot the SAR template available from the RMF Knowledge Service website. This is part of the Security Authorization Package spreadsheet and can be obtained by following the link shown on the screen.

Slide 17 - Task 4-4 Remediation Preparation

In all cases, organizations review assessor findings and determine the severity or seriousness of the findings (that is, the potential adverse impact on organizational operations and assets, individuals, other organizations, or the Nation) and whether the findings are sufficiently significant to be worthy of further investigation and/or remediation.

The Security Assessment Report or SAR provides visibility into specific weaknesses and deficiencies in the security controls used within or inherited by the information system that remain unresolved. Such weaknesses and deficiencies are potential vulnerabilities if exploitable by a threat source. The SAR helps determine the initial remediation actions and the prioritization of such actions.

Slide 18 - Task 4-4 Remediation Actions

Remediation is intended to fix NC controls. POA&Ms are used to provide the method and timeline for remediation. Assigned personnel conduct remediation of NC controls based on findings and recommendations of the SAR, reassessing remediated control(s) as appropriate.

The security plan is updated based on the findings of the security control assessment and all remediation actions taken. The updated security plan reflects the actual state of the security controls after the initial assessment along with any modifications by the information system owner or common control provider in addressing recommendations for corrective actions.

Slide 19 - Task 4-4 Remediation Examples

Here we see some sample findings and associated remediation.

STUDENT GUIDE
Risk Management Framework –
Step 4: Assessing Security Controls

Slide 20 - Milestone Checkpoint #4

This Milestone Checkpoint taken from NIST Special Publication 800-37 can be used to assess whether you are prepared to go to step 5 of the RMF process.

Milestone Checkpoints contain a series of questions for the organization to help ensure important activities have been completed prior to proceeding to the next step.

Slide 21 - Lesson Summary

You should now be able to:

- Develop and approve a security assessment plan
- Assess security controls based on the plan
- Document security assessment results
- Conduct remediation activities

Please click Next to complete the assessment questions in order to receive credit for this course.