STUDENT GUIDE
Risk Management Framework –
Step 5: Authorizing Systems

RMF Module 5

Slide 1 - Risk Management Framework

Welcome to Risk Management Framework –Lesson 5 - RMF Step 5 Authorizing Systems.

Once the security controls are assessed, the POA&M and security authorization package must be finalized and submitted to the Authorizing Official for approval.

Slide 2 - Objectives

By the end of this lesson an Information System Owner or Common Control Provider should be able to:

- Prepare a Plan of Action and Milestones (POA&M)
- Assemble and submit the security authorization package to the Authorizing Official

An Authorizing Official or their Designated Representative should:

- Be able to understand overall risk based on artifacts submitted
- Have resources to make a decision whether overall risk is acceptable

Slide 3 - Sources

The authoritative sources listed here are to be used for Security Control Authorization 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 (CAC/PKI required)

Slide 4 – Who Are The Players?

There are four tasks that comprise Step 5 of the RMF. The Information System Owner and Common Control Provider have Primary Responsibility for the first two tasks.

These individuals have supporting roles for the first task: Information Owner/Steward, Information System Security Manager or ISSM, and Information System Security Officer or ISSO. These have supporting roles for the second task: ISSM, ISSO and Security Control Assessor or SCA.

The Authorizing Official has Primary Responsibility for the last two tasks.

These individuals have supporting roles for the last two tasks: Authorizing Official's Designated Representative, Risk Executive Function and Senior Information Security Officer.

Slide 5 - Task 5-1 Prepare the POA&M

Now let's take a closer look at Task 1. The Plan of Action and Milestones, also known as the POA&M, is prepared for the Authorizing Official by the information system owner or the Common Control Provider. It is one of the key documents in the security authorization package and describes the specific tasks that are planned to:

- Correct any weaknesses or deficiencies in the security controls noted during the assessment, and
- Address the residual vulnerabilities in the information system

Organizations develop specific plans of action and milestones based on the results of the security control assessment and in accordance with applicable laws, Executive Orders, directives, policies, standards, guidance, or regulations.

Please note that plan of action and milestones entries are *not* required when weaknesses or deficiencies are remediated either during the assessment or prior to the submission of the authorization package to the Authorizing Official.

Slide 6 - Task 6 - Task 5-1 POA&M Purpose

The plan of action and milestones is used by the Authorizing Official to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment. All security weaknesses and deficiencies identified during the security control assessment are documented in the Security Assessment Report to maintain an effective audit trail.

Slide 7 - Task 5-1 POA&M Elements

The POA&M identifies:

- Tasks to be accomplished with a recommendation for completion either before or after information system implementation
- Resources required to accomplish the tasks
- Milestones in meeting the tasks, and
- Scheduled completion dates for the milestones

Slide 8 - Task 5-1 POA&M Template

POA&M information can be added to the POA&M tab of the security authorization package. The spreadsheet template can be downloaded from the RMF Knowledge Service web site link shown on the screen.

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

Slide 9 - Task 5-1 POA&M and the System Life Cycle

POA&Ms are maintained throughout the system life cycle and must be active throughout a system's life cycle as vulnerabilities remain or are remediated. Once posted to the POA&M, vulnerabilities will be updated, but not removed, after correction or mitigation actions are completed. Inherited vulnerabilities must be addressed on POA&Ms. The Authorizing Official (AO) or their Designated Representative monitors and tracks overall execution of POA&Ms under their responsibility.

The Information System Owner (ISO) or Program or System Manager implements the corrective actions identified in the POA&M. With the support and assistance of the Information System Security Manager, they must also provide visibility and status to the Authorizing Official and the Senior Information Security Officer (SISO).

The DoD Component SISOs must monitor and track the overall execution of system-level POA&Ms across the entire Component until identified security vulnerabilities have been remediated and the RMF documentation is appropriately adjusted.

Slide 10 - Task 5-2 Security Authorization Package

The ISSM assembles the security authorization package for the Information System Owner or ISO. The package consists of the updated Security Plan, the Security Assessment Report (SAR), and the POA&M. The security authorization package must also contain, or provide links to, the appropriate documentation for any security controls being satisfied through inheritance (for example, contract documents, MOAs, and SLAs). The security authorization package is submitted to the Authorizing Official (via the AO's Designated Representative if appropriate) for review and final acceptance.

Slide 11 - Task 5-2 Security Authorization Package

As mentioned previously the security authorization package contains the:

- Security Plan

- Security Assessment Report, and
- Plan of Action and Milestones

The information in these key documents is used by the Authorizing Official to make risk-based authorization decisions. For information systems inheriting common controls for specific security capabilities, the security authorization package for the common controls or a reference to such documentation is also included in the package. The contents of the security authorization package are protected appropriately in accordance with federal and organizational policies.

The RMF Knowledge Service web site has a spreadsheet template you can download and use from the link shown on the screen, which also contains an Authorization Decision Document.

Slide 12 - Task 5-2 Security Authorization Package

eMass also provides an automated security authorization package. Your Authorizing Official should let you know whether to use the RMF Knowledge Service package or eMass or some combination of the two. If you are currently using eMass you should continue to do so.

Slide 13 - Task 5-3 Risk Determination

In Task 5-3 the Authorizing Official or AO, in collaboration with the Senior Information Security Officer, assesses the current security state of the system provided by the Information System Owner or Common Control Provider (as reflected by the POA&Ms, risk assessment and recommendations provided in the Security Assessment Report) and weighs this against the operational need for the system.

The Authorizing Official has to determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

The Risk Executive Function also provides information to the Authorizing Official that is considered in the final determination of risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of the information system.

Risk assessments (either formal or informal) are employed at the discretion of the organization to provide needed information on threats, vulnerabilities, and potential impacts as well as the analyses for the risk mitigation recommendations. The RMF Knowledge Service web site provides additional guidance and tools for conducting risk assessments. You may also want to refer to the NIST Special Publication 800-30, “Guide for Conducting Risk Assessments.”

Slide 14 - Task 5-3 Risk Management Strategy

Risk-related information includes the criticality of organizational missions and/or business functions supported by the information system along with the risk management strategy for the organization. A risk management strategy typically describes:

- How risk is assessed within the organization (e.g., tools, techniques, procedures, and methodologies)
- How assessed risks are evaluated with regard to severity or criticality
- Known existing aggregated risks from organizational information systems and other sources
- Risk mitigation approaches
- Organizational risk tolerance, and
- How risk is monitored over time

When making the final risk determination, the Authorizing Official or their designated representative considers information obtained from the Risk Executive Function along with the information provided by the Information System Owner or Common Control Provider in the security authorization package which includes the security plan, Security Assessment Report, and POA&Ms. Conversely, information system-related security risk information derived from the execution of the RMF is available to the Risk Executive Function for use in formulating and updating the organization-wide risk management strategy.

Slide 15 - Task 5-3 Risk Response

After determining risk, organizations can respond to risk in a variety of ways, including:

- Avoiding or eliminating risk
- Mitigating risk
- Accepting risk
- Sharing risk
- Transferring risk, or
- A combination of the above

Decisions on the most appropriate course of action for risk response include some form of prioritization. Some risks may be of greater concern than others. More resources may need to be directed at addressing higher-priority risks than at other lower-priority risks. This doesn't necessarily mean that the lower-priority risks are ignored. Rather, it could mean that fewer resources are directed at the lower-priority risks, at least initially, or that the lower-priority risks are addressed at a later time.

A key part of the risk decision process is the recognition that, regardless of the risk decision, there may remain some residual risk. Organizations determine acceptable degrees of residual risk based on organizational risk tolerance.

For information systems, an Authorizing Official will generally try to eliminate the risk completely, mitigate the risk, or accept the risk with or without some mitigation and residual risk.

Slide 16 - Task 5-4 Authorization and Risk Acceptance

The explicit acceptance of risk is the responsibility of the Authorizing Official and cannot be delegated to other officials within the organization. The Authorizing Official considers many factors when deciding if the risk to organizational operations (including mission, function, image, or reputation), organizational assets, individuals, other organizations, and the Nation, is acceptable.

Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision. The Authorizing Official issues an authorization decision for the information system and the common controls inherited by the system after reviewing all of the relevant information and, where appropriate, consulting with other organizational officials including the Risk Executive Function.

Slide 17 - Task 5-4 Authorization Decision Document

DoD Security Authorization Decision information can be added to the Authorization Decision Document tab of the security authorization package template on the RMF Knowledge Service web site, available for download from the link shown on the screen. This information can also be stored in eMass. If you are currently using eMass you should continue to do so.

This conveys the final security authorization decision from the Authorizing Official to the Information System Owner, Common Control Provider and other organizational officials. The authorization decision document contains the following information:

- Authorization decision (to operate or not)
- Terms and conditions for the authorization, and
- Authorization termination date

The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the System Owner or Common Control Provider.

The authorization termination date established by the Authorizing Official indicates when the security authorization expires. Authorization termination dates are influenced by federal and/or organizational policies which may establish maximum authorization periods. Organizations may choose to eliminate the authorization termination date if the continuous monitoring program is sufficiently robust to

provide the Authorizing Official with the needed information to conduct ongoing risk determination and risk acceptance activities with regard to the security state of the system and related security controls. \

Slide 18 - Task 5-4 Authorization Decision

An authorization decision applies to a specifically identified information system or platform IT system. It balances mission need against risk to the mission, the information being processed, the broader information environment, and other missions reliant on the shared information environment. A DoD authorization decision is expressed as an ATO, an ATO with conditions, an IATT, or a DATO. An information system or platform IT system is considered unauthorized if an authorization decision has not yet been made.

Please note that an "ATO with conditions" is what was referred to under DIACAP as an IATO. The Authorizing Official no longer issues IATO's under the Risk Management Framework.

Slide 18a - Task 5-4 ATO – Authority to Operate

If overall risk is determined to be acceptable, and there are no non-compliant (NC) controls with a level of risk of "Very High" or "High," then the authorization decision should be issued in the form of an ATO. An ATO authorization decision must specify a termination date that is within 3 years of the authorization date unless the information system or platform IT system has a system-level continuous monitoring program compliant with DoD continuous monitoring policy as issued.

Slide 18b - Task 5-4 ATO with conditions

If NC controls with a level of risk of "Very High" or "High" exist that cannot be corrected or mitigated immediately, but overall system risk is determined to be acceptable due to mission criticality, then the authorization decision will be issued in the form of an "ATO with conditions" and only with permission of the responsible DoD Component CIO.

The "ATO with conditions" should specify an AO review period that is within 6 months of the authorization date. The POA&M supporting this ATO documents identified vulnerabilities and specifies corrective actions to be completed before the review.

If the system still requires authorization with a level of risk of "Very High" or "High" after 1 year, the DoD Component CIO must again grant permission for continued operation of the system. This authority cannot be delegated below the DoD Component CIO. The DoD Component CIO must concur in writing or through DoD public key infrastructure (PKI)-certified digital signature and that the security risk of continued system operation is acceptable due to mission criticality. The DoD Component CIO provides a copy of the concurrence and authorization decision document with supporting rationale to the DoD ISRMC Secretariat and the DoD SISO. This authorization decision closely manages risk while allowing system operation.

Slide 18c - Task 5-4 IATT - Interim Authorization to Test

IATTs should be granted only when an operational environment or live data is required to complete specific test objectives and should expire at the completion of testing, normally for a period of less than 90 days. Operation of a system under an IATT in an operational environment is for testing purposes only, which means the system will not be used for operational purposes during the IATT period.

For full and independent operational testing, an ATO rather than an IATT may be required if operational testing and evaluation is being conducted in the operational environment or on deployed capabilities. In this case, the ATO should be reviewed following operational testing and evaluation for modification as necessary in consideration of the operational test results.

Slide 18d - Task 5-4 DATO - Denial of Authorization to Operate

If risk is determined to be unacceptable, the authorization decision should be issued in the form of a DATO. If the system is already operational, the Authorizing Official will issue a DATO and stop operation of the system immediately. Network connections will be immediately terminated for any system issued a DATO.

Examples of when a DATO may be issued include when:

- Terms and conditions of the original authorization have been violated
- There is failure to maintain effective continuous monitoring
- Immediate steps cannot be taken to reduce risk to an acceptable level

A DATO may also be issued coincidental to implementing a decommissioning strategy for a system.

Slide 19 - Milestone Checkpoint #5

This milestone checkpoint taken from NIST Special Publication 800-37 can be used to assess whether you are prepared to go to Step 6 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 20 - Lesson Summary

STUDENT GUIDE
Risk Management Framework –
Step 5: Authorizing Systems

An Information System Owner or Common Control Provider should now be able to:

- Prepare a Plan of Action and Milestones (POA&M)
- Assemble and submit the security authorization package to the Authorizing Official

An Authorizing Official or their Designated Representative:

- Should now be able to understand overall risk based on artifacts submitted, and
- Now has resources to make a decision whether overall risk is acceptable

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