STUDENT GUIDE
Risk Management Framework –
Step 3: Implementing Security Controls

Slide 1 - Risk Management Framework

Welcome to *Risk Management Framework – Lesson 3, the RMF Process Step 3: Implementing Security Controls*

By approving the security plan, created in Step 2, the Authorizing Official agrees to the system categorization, the set of security controls proposed to meet the security requirements for the system, and the adequacy of the system-level continuous monitoring strategy. The approval of the security plan in Step 2 also establishes the level of effort required to successfully complete the remainder of the steps in the Risk Management Framework and provides the basis of the security specifications for the acquisition of the system, subsystems, or components.

The next step, Step 3, is to implement security controls.

Slide 2 - Objectives

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

- Implement the security controls specified in the security plan, and
- Document security control implementation in the security plan

Slide 3 - Sources

The authoritative sources listed here are to be used for Security Control Implementation 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 - Security Controls Implementation

- Implementation of security controls specified in the security plan will be in accordance with DoD implementation guidance for each security control found on the Security Controls Explorer page of the RMF Knowledge Service site
- Implementation guidance provided in Security Controls Explorer covers specific control documentation requirements, including required artifacts, templates, and best practices

- DoD-specific assignment values are embedded in the security control text found in both Security Controls Explorer and the eMASS (Enterprise Missions Assurance Support Service) database, along with security control implementation guidance and assessment procedures.
- eMASS is a database and workflow tool that has been used with DIACAP for many years. It is also available for use with the Risk Management Framework.

If you already use eMASS to help document security control implementation you should continue to do so.

Slide 4a - RMF Knowledge Service security control explorer

Here we see a subset of controls using the Security Control Explorer in the RMF Knowledge Service site. By clicking on one of the control acronyms we can see the implementation guidance.

Slide 4b - Implementation Guidance

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

Slide 5 – Who Are The Players?

There are two tasks that comprise Step 3 of the RMF. The Information System Owner and Common Control Provider have primary responsibility for both tasks which include implementing security controls and documenting that implementation in the security plan.

These individuals have supporting roles in the process: Information Owner or Steward; Information System Security Officer or ISSO; and Information System Security Engineer. (Note: Roles may vary)

Slide 6 - Task 3-1 Implement Security Controls

Now, let's take a closer look at Task 1. We want to keep the following in mind when implementing security controls:

- Products used within an IS or PIT system boundary will be configured in accordance with applicable STIGs (Security Technical Implementation Guide), or SRGs (Security Requirement s Guide) where the STIGs are not available (Note: other guidance may be provided by the Cognitive Security Agency (CSA) at their discretion.)

- Security controls are implemented consistent with DoD and DoD Component IA architectures and standards, employing system and software engineering methodologies, security engineering principles, and secure coding techniques. DoD-recommended security control implementation guidance is available at the RMF Knowledge Service.
- The Information System Owner or Program Manager must ensure early and ongoing involvement by information system security engineers qualified in accordance with DoD 8570.01-M
- Mission owner(s) must translate security controls into system specifications, and ensure the successful integration of those specifications into the system design

Slide 7 - Task 3-1 Implement Security Controls (continued)

We also want to:

- Make sure security engineering trades do not impact the ability of the system to meet the fundamental mission requirements - this includes ensuring that technical and performance requirements derived from the assigned security controls are included in requests for proposal and subsequent contract documents for design, development, production, and maintenance
- Be sure to address the proposed system security design in preliminary and critical design reviews
    - System security design should address security controls that may be satisfied through inheritance of common controls
- PMs for programs acquiring information or Platform IT systems in accordance with DoDI 5000.02 must integrate the security engineering of cybersecurity requirements and cybersecurity testing considerations into the program's overall systems engineering process, as well as document and update this approach in the program's systems engineering plan and program protection plan throughout the system development lifecycle

Slide 8 - Task 3-1 Best Practices

Best practices for implementing security controls within an information system include using system and software engineering methodologies, security engineering principles, and secure coding techniques.

Information system security engineers, with support from information system security officers, employ a sound security engineering process that captures and refines information security requirements and ensures the integration of those requirements into information technology products and systems through purposeful security design or configuration.

In addition, organizations should ensure that mandatory configuration settings are established and implemented on information technology products in accordance with federal and organizational policies, such as Federal Desktop Core Configuration.

Slide 9 - Task 3-2 Document Security Control Implementation

In Task 3-2 we document the security control implementation in the security plan, in accordance with DoD implementation guidance found on the RMF Knowledge Service site.

If a control isn't in accordance with the RMF Knowledge Service guidance, provide a description of the control implementation including planned inputs, expected behavior, and expected outputs.

Security controls that are available for inheritance (for example, common controls) by information and Platform IT systems will be identified and have associated compliance status provided by the hosting or connected systems (including environmental controls).

Slide 10 - Document Security Control Implementation Using Template

The RMF Knowledge Service site has specific control documentation requirements, including required artifacts, templates, and best practices.

Here we see the RMF Security Plan template with a column highlighted that can be used to document when a security control has been implemented. This column (Common Control Provider Column) can be used to document the Common Control Provider. The template is available from the RMF Knowledge Service web site as part of the RMF Security Authorization Package at the link shown on the screen. You must first login to the RMF site before you can access the link. (CAC/PKI required)

Slide 11 - Task 3-2 Best Practices

Documentation of security control implementation allows for traceability of decisions prior to and after deployment of the information system.

To increase overall efficiency and cost effectiveness of security control implementation:

- Reference existing documentation, either by vendors or other organizations that have employed the same or similar information systems
- Use automated support tools, and
- Maximize communications

Slide 12 - Milestone Checkpoint

STUDENT GUIDE
Risk Management Framework –
Step 3: Implementing Security Controls

This milestone checkpoint taken from NIST Special Publication 800-37 can be used to assess whether you are prepared to go to step 4 of the RMF process.

Slide 12a - Milestone Checkpoint

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 13 - Lesson Summary

You should now be able to:

- Implement the security controls specified in the security plan, and
- Document security control implementation in the security plan

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