STUDENT GUIDE
Risk Management Framework –
Step 2: Selecting Security Controls

Slide 1 - Risk Management Framework

Welcome to Risk Management Framework – Lesson 2: the RMF Process Step 2: Selecting Security Controls

Once 'Step 1: Categorization' has been successfully completed for an information system in accordance with the process described in RMF - Lesson 1, then Step 2 of the RMF requires the organization to determine the appropriate security controls to apply to the system in order to properly manage their mission, business, and system risks.

Slide 2 - RMF Overview

Shown here are the six steps in the RMF Process.

This lesson concentrates on the second of these steps: Step 2: Selection of Security Controls

Slide 3 - Objectives

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

- Locate security control policies and guidelines
- Identify security controls and common controls
- Select and document controls
- Describe the purpose of security overlays and tailoring
- Explain the importance of continuous monitoring
- Understand who approves the security plan
- Understand when to update the security plan

Slide 4 - Sources

The sources listed here can be used for RMF 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
- CNSSI 1253 establishes guidelines and a method for selecting security controls for information systems and the information they contain
- NIST SP 800-37 is the Guide for Applying RMF to Federal Information Systems

STUDENT GUIDE
Risk Management Framework –
Step 2: Selecting Security Controls

- NIST SP 800-53 provides a security controls catalog and guidance for security control selection
- The RMF Knowledge Service at https://rmfks.osd.mil/rmf is the go-to source when working with RMF (CAC/PKI required)

Next we'll take a look at Security Controls…

Slide 5 - What are Security Controls?

Security controls are safeguards and countermeasures prescribed for an information system:

- To protect the confidentiality, integrity, and availability of a system and its information
- To properly manage mission, business, and system risks, and
- To facilitate reciprocity

Slide 5a - Reciprocity

Cybersecurity reciprocity is an essential element in ensuring IT capabilities are developed and fielded rapidly and efficiently across the DoD Information Enterprise. Applied appropriately, reciprocity enhances cybersecurity through consistent application of controls across multiple enclaves while reducing redundant testing, assessment and documentation, and the associated costs in time and resources. More information about reciprocity can be found at the RMF Knowledge Service site.

Slide 6 - Who are the players?

There are four tasks that make up Step 2 of the RMF. The Chief Information Officer or Senior Information Security Officer, Information Security Architect, and Common Control Provider all have Primary Responsibility for the first task which is identifying common security controls and documenting them in a security plan or equivalent document.

These individuals have supporting roles for this first task: Risk Executive Function, Authorizing Official or their Designated Representative, Information System Owner, and Information System Security Engineer.

NIST SP 800-37 describes all four tasks for RMF Step 2. The last three are:

> Task 2-2: Select the security controls for the information system and document the controls in the Security Plan.
> Task 2-3: Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation.

STUDENT GUIDE
Risk Management Framework –
Step 2: Selecting Security Controls

Task 2-4: Review and approve the security plan.

Let's take a closer look at each of these tasks.

Slide 7 - Task 2-1: Identify common controls

Common controls are security controls that are inherited by one or more organizational information systems.

By identifying security controls that are provided by the organization as common solutions for information systems and Platform IT systems, and documenting the assessment and authorization of the controls in a security plan (or equivalent document), individual systems within those organizations can leverage these common controls through inheritance.

Please see the RMF Knowledge Service for identification of common controls for DoD and additional information on how they are documented.

Slide 7a - 18 Control Families

Security controls have a well-defined organization and structure. For ease of use in the security control selection and specification process, controls are organized into eighteen *families*. Each family contains security controls related to the general security topic of the family. A two-character identifier uniquely identifies security control families, for example PS stands for Personnel Security. Security controls may involve aspects of policy, oversight, supervision, manual processes, actions by individuals, or automated mechanisms implemented by information systems or devices.

Shown here is a list of the security control families and the associated family identifiers.

Slide 7b - *Typical Common Controls*

A security control is inheritable by an information system or application when that system or application receives protection from the security control and the control is developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application—entities either internal or external to the organization where the system or application resides.

Excellent candidates for common control status are:

- Contingency planning controls
- Incident response controls

- Security training and awareness controls
- Personnel security controls, and
- Physical and environmental protection controls

Information security program management controls may also be deemed common controls since the controls are employed at the organization level and typically serve multiple information systems.

Slide 8 - Task 2-2: Select and Document Controls

This task, 2-2, is to select security controls for the information system and document the controls in the security plan. RMF team members who have primary roles in the security control selection are the Information System Architect and Information System Owner. They will identify the security control baseline for the system as provided in CNSSI 1253 and document these in the security plan. The baselines identified in CNSSI 1253 address the overall threat environment for DoD information systems and Platform IT systems.

Those with have supporting roles include the Authorizing Official or their Designated Representative, the Information Owner or Steward, the Information System Security Officer and the Information System Security Engineer.

Slide 9 - RMF Knowledge Service Security Control Explorer

Based on the system's categorization, the RMF Knowledge Service (KS) generates the same baseline set of security controls within the security control explorer page as is found in CNSSI 1253. You're also able to export these controls to assist with documenting the security plan. First specify the Confidentiality, Integrity and Availability impact values, click the "Apply CIA Selection" button, then click at the end of the line "Export the complete list of Security Controls here".

Slide 10 - Apply Overlays

After selecting the applicable security control baseline, organizations initiate the tailoring process to modify them appropriately and align the controls more closely with the specific conditions within the organization. In this step the relevant security control overlays for a system are assigned, if applicable. Please note the typical information system is adequately protected by the existing baselines.

Overlays are developed, reviewed, and published by the CNSS and NIST. The CNSS web site provides downloadable copies of the approved and published overlays. Overlays may add or subtract security controls, or provide additional guidance regarding security controls, resulting in a set of security controls

applicable to that system that is a combination of the baseline and overlay. The combination of baselines and overlays addresses the unique security protection needs associated with specific types of information or operational requirements.

(Note: CNSS and NIST are not the only source of overlays.)

Slide 11 - Categories of Overlays

Overlays provide an opportunity to build consensus across communities of interest and develop security plans for organizational information systems that have broad-based support for very specific circumstances, situations, and/or conditions. An overlay may also be required to protect organizations, information, information systems, or individuals from different threats and vulnerabilities than typical information systems.

The overlays seen here can be obtained from cnss.gov. The Intelligence Overlay is designated FOUO, so please contact the CNSS office if you need to obtain a copy of this document.

Slide 11a – Multiple Overlays

Multiple overlays can be applied to a single security control baseline. The tailored baselines that result from the overlay development process may be more or less stringent than the original security control baselines.

If multiple overlays are employed, and there could be a conflict between the overlays, the Authorizing Official (or designee), in coordination with the Mission/Business Owner and/or Information Owner/Steward, can resolve the conflict.

In general, overlays are intended to reduce the need for ad hoc tailoring of baselines by organizations. Further tailoring to reflect organization-specific needs, assumptions, or constraints may require the concurrence or approval of the Authorizing Official or other organization-designated individuals.

Slide 12 - Tailoring

Decision-makers may find it necessary to further tailor a control set in response to increased risk from changes in threats or vulnerabilities, or variations in risk tolerance. Tailoring decisions must be aligned with operational considerations and the system environment and should be coordinated with mission owners. Security controls should be added or removed only as a function of specified, risk-based determinations.

STUDENT GUIDE
Risk Management Framework –
Step 2: Selecting Security Controls

Tailoring decisions, including the specific rationale for those decisions such as mapping to risk tolerance, are documented in the security plan. Every selected control must be accounted for. If a selected control is not implemented, then the rationale for not implementing the control must be documented in the security plan and the POA&M.

Slide 13 - Additional Controls

Organizations assign a hybrid status to security controls when one part of the control is common and another part of the control is system-specific. The determination as to whether a security control is common, hybrid, or system-specific is context-based.

External information system services are services implemented outside of the authorization boundaries established by the organization for its information system. These external services may be used or inherited by, but are not part of, the organization's information system.

Organizations are responsible and accountable for the risk incurred by use of services provided by external providers and must address this risk by implementing compensating controls when the risk is greater than the authorizing official or the organization is willing to accept.

Slide 14 - Security Control Selection Summary

To wrap up our discussion of Task 2-2, keep these steps in mind -

- Select the initial control set, or baseline, corresponding to the security categorization of the system based on RMF Step 1
- Apply appropriate overlay(s) based on information and mission requirements
- Make additional tailoring decisions aligned with operational considerations and the system environment and coordinated with mission owners
- Document the resulting set of security controls, along with the supporting rationale for selection decisions and any system use restrictions, in the security plan

Slide 15 - Task 2-3: Monitoring Strategy

Task 2-3 calls for the development of a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation.

STUDENT GUIDE
Risk Management Framework –
Step 2: Selecting Security Controls

A critical aspect of risk management is the ongoing monitoring of security controls employed within or inherited by the information system. An effective monitoring strategy is developed early in the system development life cycle, say during system design or COTS procurement decision, and can be included in the security plan. The implementation of a robust continuous monitoring program allows an organization to understand the security state of the information system over time and maintain the initial security authorization in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and business functions.

Slide 16 - Develop Monitoring Strategy

The continuous monitoring strategy for the information system identifies the security controls to be monitored, the frequency of monitoring, and the control assessment approach.

The strategy defines**:**

- Configuration Management process including
    - How changes to the information system will be monitored, and
    - Ensuring documentation is updated
- How security impact analysis will be conducted
- Security status reporting requirements

Security controls that are volatile (that is, most likely to change over time), critical to certain aspects of the organization's protection strategy, or identified in current POA&Ms may require more frequent assessment. The use of automation facilitates a greater frequency and volume of security control assessments.

Slide 17 - Effective Monitoring

An effective monitoring program includes: configuration management and control processes, security impact analyses on proposed or actual changes to the information system and its environment of operation, assessment of security controls employed within and inherited by the information system (including controls in dynamic subsystems), and security status reporting to appropriate organizational officials.

STUDENT GUIDE
Risk Management Framework –
Step 2: Selecting Security Controls

Slide 18 - Task 2-4: Review and Approve the Security Plan

In Task 2-4 an independent review of the security plan by the Authorizing Official or their Designated Representative with support from the Senior Information Security Officer, Chief Information Officer, and Risk Executive, helps determine if the plan is complete, consistent, and satisfies the stated security requirements for the information system.

The security plan review also helps to determine, to the greatest extent possible with available planning or operational documents, if the security plan correctly and effectively identifies the potential risk to organizational operations and assets, individuals, other organizations, and the nation, that would be incurred if the controls identified in the plan are implemented as intended.

The Authorizing Official or their Designated Representative approves the plan.

Slide 19 - Update Security Plan

The security plan should be updated whenever events dictate changes to the security controls employed within or inherited by the information system. Changes may be triggered by a variety of events, to include:

- Vulnerability scan or assessment
- New or recurring threat information
- Weaknesses or deficiencies discovered in security controls via alerts or breaches
- Redefined mission priorities or business objectives
- Changes in the information system, for example adding new hardware, software, firmware, adding new connections, or changing its environment of operation, such as moving to a new facility

Slide 20 - Update Security Plan Roles

The Information System Owner (ISO) has responsibility for:

- Ensuring development and maintenance of the security plan and that the system is deployed and operated in accordance with the agreed-upon security controls
- Updating the security plan, security assessment report, and POA&Ms based on the results of the continuous monitoring process

The ISSO and Information Owner/Steward have a supporting role in this process.

STUDENT GUIDE
Risk Management Framework –
Step 2: Selecting Security Controls

Slide 21 - Milestone Checkpoint

This checkpoint taken from NIST SP 800-37 can be used to assess whether you are prepared to go on to step 3 of the RMF process. There are six milestone checkpoints, one at the end of each step, which contain a series of questions for the organization to help ensure that important activities described in a particular step in the RMF have been completed prior to proceeding to the next step.

Slide 22 - Lesson Summary

You should now be able to:

- Locate security control policies and guidelines
- Identify security controls and common controls
- Select and document controls
- Describe the purpose of security overlays and tailoring
- Explain the importance of continuous monitoring
- Understand who approves the security plan
- Understand when to update the security plan

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