STUDENT GUIDE
Risk Management Framework –
Step 1: Categorization of the Information System

RMF Module 1

Slide 1 – RMF Overview

RMF takes into account the organization as a whole, including strategic goals and objectives and relationships between mission/business processes, the supporting information systems, as well as organizational culture and infrastructure.

RMF provides implementation guidance through a six-step information system life cycle.

- Step 1: Categorization of the information system
- Step 2: Selection of security controls
- Step 3: Implementation of those security controls
- Step 4: Assessing the selected security controls
- Step 5: Authorizing the system
- Step 6: Instituting continuous monitoring of the security controls that have been put in place.

This lesson concentrates on the first of these steps: Categorization of the System.

Slide 2 - Introduction

Welcome to Risk Management Framework – Lesson 1 RMF Process Step 1: Categorization of the System

Integrating information security into organizational infrastructure requires an organization-wide perspective as well as a carefully coordinated set of activities to ensure that fundamental requirements for information security are addressed and risk to the organization from threats to information systems is managed efficiently and cost-effectively.

The Risk Management Framework or 'RMF' provides that structured, yet flexible approach for managing risk resulting from the incorporation of information systems into the mission and business processes of an organization.

Slide 3 - Objectives

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

- Identify security categorization resources
- Define security categorization
- Identify roles and responsibilities for Step 1
- Identify information types
- Explain how to assign impact values
- Describe security categorization factors
- Define system boundary and be prepared to complete the Security Plan
- Register the information system

STUDENT GUIDE
Risk Management Framework –
Step 1: Categorization of the Information System

Slide 4 - Sources

The authoritative sources listed here are to be used for Security Categorization Guidance.

CNSSI 1253 establishes guidelines and a method for security categorization for information systems and the information they contain.

NIST SP 800-60 Volume I, dated August 2008, is a best practice guideline to assist in identification of information types.

SP800-37 (need description)
DoDI8510.01 (need description)
RMF Knowledge Service at https://rmfks.osd.mil/rmf is the go to source when working with RMF. (CAC/PKI required)

Slide 5 - What is Security Categorization?

Security Categorization is determining and assigning appropriate values to information or an information system based on protection needs.

Security categorization establishes the foundation for the RMF process by determining the level of effort and rigor required to protect an organization's information. The results of the security categorization are subsequently used in defining the set of controls for the system.

Protection needs are determined by the impact to information or the information system resulting from a loss of Confidentiality, Integrity and Availability. Impact levels are defined as Low, Moderate, or High.

Properly identifying security requirements is essential because an incorrect security categorization can result in the organization either over protecting the information system, thus wasting valuable security resources, or under protecting the information system and placing important operations and assets at risk.

The security categorization method uses three impact values of low, moderate, or high reflecting the potential impact should a security breach occur, such as a loss of confidentiality, integrity, or availability. Organizations applying these definitions must do so within the context of their own organization as well as the overall national interest.

Slide 6 - Information Types

In preparing for the first step of the RMF Process, Categorization, the Mission/Business Owner/Information System Owner is responsible for identifying all information types.

An information type is considered any specific category of information defined by an organization or, in some instances, by a public law, executive order, directive, policy, or regulation.

STUDENT GUIDE
Risk Management Framework –
Step 1: Categorization of the Information System

For security categorization purposes, organizations should develop their own policies that identify information types.

Organizational policies should identify all of the information types that are input, stored, processed, and/or output from each system.

Slide 7 - Examples of Information Types

Information systems may contain more than one type of information:

- Privacy Information or PII
- Medical
- Proprietary
- Financial

The examples on the screen are derived from NIST SP 800-60 and are not all-inclusive.

Please note that System information such as, network routing tables, password files, cryptographic key management information, must be protected at a level commensurate with the most critical or sensitive user information being processed.

Slide 8 – Best Practices Guidelines

Please refer to NIST SP 800-60 Volume I from August 2008 for more information related to information type and mapping types of information in information systems to security categories.

(Refer to Volume 2 for examples of information types.)

Slide 9 - Who are the players?

(Roles and titles may vary between organizations.)

There are three tasks that comprise Step 1 of the RMF. The Information System Owner has Primary Responsibility for all three tasks, which include categorizing an IS and documenting the results in the Security Plan. The Information Owner/Steward also has a primary role for Task 1-1

Information to be documented in the Security Plan includes:

- Information Types
- Impact Values
- Rationale for Decisions

The following individuals have supporting roles in the process:

Risk Executive (Function); Authorizing Official or their Designated Representative; Chief Information Officer; Senior Information Security Officer; Information System Security Officer.

STUDENT GUIDE
Risk Management Framework –
Step 1: Categorization of the Information System

The Information Owner/Steward has a supporting role for Task 1-2.

The Authorizing Official, or AO, is the person known under DIACAP as the Designated Accrediting Authority, or DAA.

Slide 10 - Prepping for Step 1

Once the information types have been identified, collect all relevant documentation specific to the information system.

Some examples of relevant documentation include network diagrams, CONOPS, and mission requirements.

Also obtain organization-specific documentation such as: information types, categorization policies and procedures, and preliminary risk assessment results.

Slide 11 – Prepping 2 of 3

Next, to help you better gather the information you seek, develop relationships with:

- Information security program office
- Enterprise architects
- Individuals involved in capital planning and investment control
- Cross-organizational stakeholders
- Technical operations personnel

Slide 12 – Prepping 3 of 3

Finally, find out if there are any existing organizational risk assessments on such topics as vulnerability and threat information. Use them to help you get started.

Then, hold a 'Discovery' meeting with the Information Owner/Steward, Risk Executive Function, Authorizing Official or Designated Representative, CIO, Senior Information Security Officer, Information System Security Officer, etc. Let them know what you are doing and ask for their assistance.

Slide 13 - Task 1-1: Categorize

Now, let's take a closer look at Task 1.

To properly categorize the information system and document the results in the security plan, you should follow CNSSI 1253's two-step process. First, determine the impact values, and then identify overlays which identify additional factors, beyond impact, which influence the initial selection of security controls. Overlays are referenced in Appendix F of CNSSI 1253.

STUDENT GUIDE
Risk Management Framework –
Step 1: Categorization of the Information System

Slide 14 - Determine Potential Impact Values

Now let's see how to determine the potential impact values for the information types processed, stored or transmitted by the system.

There are three categories: Low (L), Moderate (M), or High (H)

Low = Limited adverse effect

Moderate = Serious adverse effect

High = Severe or catastrophic adverse effect

Values are assigned based on potential harm to the nation, organizations, mission, or to individuals should a damaging event affect any of the three security objectives of confidentiality, integrity and availability.

Slide 15 - Security Objectives

These are descriptions of the three security objectives:

Confidentiality is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity – guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification of information.

Availability – ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Slide 16 - Determine Potential Impacts Independently

It is important to understand that the determination of the potential impact for one security objective (e.g., confidentiality) is independent of the potential impact determination of the other two objectives (integrity and availability). Each potential impact is to be determined separately.

STUDENT GUIDE
Risk Management Framework –
Step 1: Categorization of the Information System

Slide 17 – Examples of Potential Impact Levels

Here is an example showing different impacts identified for each security objective.

You can see that for the PII information type the impact determined for Confidentiality is different from the impact for the other two security objectives, while all three are the same for the Contract Data information type.

Slide 18 - Potential Impact Levels

The determination of potential impact for a system relies on common definitions for each of the potential impact values. These are defined as follows:

The potential impact is **Low** if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, assets, individuals, other organizations, or the national security interests of the United States.

The potential impact is **Moderate** if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, assets, individuals, other organizations, or the national security interests of the United States.

The potential impact is **High** if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, assets, individuals, other organizations, or the national security interests of the United States.

Slide 19 - Other Confidentiality Security Factors

Potential impact is only one factor to consider with respect to confidentiality.

Potential (or provisional) impact levels are adjusted based on supplemental factors to determine Overall Impact Level:

- Aggregation of information or data
- Information system environment, like physical space
- Attributes of users such as Clearance, Formal Access, or Need to Know(NTK)
- Legislative and Executive Mandates that relate to specific information types

Please note that all classified National Security Systems must be categorized as Moderate or High with respect to the confidentiality security factor.

STUDENT GUIDE
Risk Management Framework –
Step 1: Categorization of the Information System

Slide 20 - Integrity Security Concerns

With respect to Integrity, unauthorized changes to information can be subtle and difficult to detect, or they can occur on a massive scale.

The most serious impact is when an action is taken, or a decision made, based on the unauthorized modifications to information.

If the loss of integrity goes undetected, the result can be catastrophic for many information types.

Slide 21 - Availability Security Categorization Factors

There are some other factors to consider with regard to availability.

The degree of impact depends on how long information remains unavailable and/or how long the loss of availability goes undetected.

Reconstruction of the information or IS could be time consuming/expensive.

Availability impact level recommendations should indicate if the information is time-critical.

Other systems dependent upon this system's information is also an important factor in determining impact level.

Answers to the following questions may help in the evaluation process as it relates to availability:

- How can a malicious adversary use the unauthorized disclosure of information to do harm to agency operations, assets, or individuals?
- How can a malicious adversary use the unauthorized disclosure of information to gain control of agency assets that might result in unauthorized modification or destruction of information, or denial of system services that would result in harm to agency operations, assets, or individuals?
- Would unauthorized disclosure of elements of the information type violate laws, executive orders, or agency regulations?

Slide 22 - Categorize the Information System

To sum up Task 1-1, categorization of systems begins by determining the security category for all information types resident on the target information system, taking into account each of the three security objectives independently. This means determination of the potential impact for one security objective (e.g., confidentiality) is independent of the potential impact determination of the other two objectives (integrity and availability).

The generalized format for expressing the security category (SC) of an information type is —

STUDENT GUIDE
Risk Management Framework –
Step 1: Categorization of the Information System

SC information type =
{(**confidentiality** impact *value*), (**integrity impact** *value*), (**availability impact** *value*)}
where the acceptable impact values are low, moderate, or high.

(This is not a mathematical equation but a concept).

Slide 23 – Examples of Potential Impact Levels

Here we see an example. For confidentiality (C) the highest impact information type is H or high. For integrity (I), the impacts are all the same so the highest is M or moderate. For availability (A), the highest impact is M or moderate.

Slide 24 - Task 1-2: Describe the Information System

Next we want to examine Task 1-2 where we describe the information system (including system boundary) and document the description in the Security Plan.

Primary Responsibility: Information System Owner.

The following individuals all have supporting roles: Authorizing Official or Designated Representative; Senior Information Security Officer; Information Owner/Steward; Information System Security Officer.

Slide 25 - System Boundary Definition

The term information system boundary is synonymous with authorization boundary.

Authorization boundaries are established in conjunction with the security categorization process and documented in the Security Plan.

Well-defined boundaries:

- Establish the scope of protection for information systems (i.e., what the organization agrees to protect under its direct management control or within the scope of its responsibilities)
- Include the people, processes, and information technologies that are part of the system

Slide 26 – System Resources and Components

Use the following questions when considering whether resources/components being identified should be included in the system boundary:

- Do they support the same mission/business objectives or functions?

- Do they essentially have the same operating characteristics and information security requirements
- Do they reside in the same general operating environment (or in the case of a distributed information system, reside in various locations having similar operating environments)
- Do they reside in the same geographic area (e.g., a site or campus environment)
- Are they part of the same contract?

If the answers are yes, then they could be included in the system boundary.

Slide 27 - System Boundary Specifications

Once you have determined the system boundary, specify the location(s) (e.g., facilities, buildings, rooms) where the information system processes, stores, or transmits data.

Identify the system as LAN, WAN, stand-alone, controlled interface (CI), cross domain solution (CDS), platform IT (PIT), or application.

Consider interconnectivity if you have two or more distinct authorization boundaries which are connected and the components or capabilities of the connection (e.g., firewalls, routers, encryption devices, etc.).

Identify the Authorizing Official.

Slide 27a - Interconnection Security Agreement (ISA)

Interconnected systems may require the use of an Interconnection Security Agreement (ISA) which defines the technical and security requirements for establishing, operating and maintaining the connection.

They are required whenever a system authorized by one Authorizing Official is connected to a system authorized by a different Authorizing Official.

Slide 27b1 - Controlled Interface (CI)

CIs include routers, firewalls, CDS (cross domain solution), etc.

- The type of CI required is determined by the classification levels of the domains it connects, this would include the criteria to release data.
- Routers and firewalls tend to be used when connecting security domains with the same classification level.

STUDENT GUIDE
Risk Management Framework –
Step 1: Categorization of the Information System

Slide 27b2 – Cross Domain Solutions (CDS)

CDS are a form of CI that provide the ability to automatically access and/or transfer information between security domains of different classification levels

CDS may be accredited separately or as a part of a system or network. If a CDS is required, contact your Organization Rep prior to contacting the Unified Cross Domain Services Management Office. (UCDSMO)

Slide 28 - Task 1-2: Document in Security Plan

The Security Plan is developed and maintained under the purview of the ISO.

In addition to authorization boundary, the document must include:

- System Description
- System Type
- System User Categories
- Authorization Termination Date
- RMF Team Roles, and
- Additional info as available, such as:
    - Hardware, Software
    - Interconnected Systems
    - Information Flows/Paths
    - Risk Determination

Slide 29 – Template

The RMF Security Plan template provides a fill-in form for Security Plans that meets the requirements for RMF.

The template is available from the RMF web site as part of the RMF Security Authorization Package at the link shown on the screen. *

https://rmfks.osd.mil/rmf/General/SecAuthPackage/Pages/SecurityPlan.aspx. (CAC required)

When completing the form be sure to provide a response for each required section.

*These templates are provided by the agency with oversight responsibilities; a DoD example is shown here.

STUDENT GUIDE
Risk Management Framework –
Step 1: Categorization of the Information System

Slide 30 - Task 1-3 Register

The last task in Step 1 is for the information owner to register the system. All DoD ISs are registered in the DoD IT Portfolio Repository (DITPR) or the SIPRNET IT Registry (SITR) in accordance with current DITPR and SITR guidance.

SAP IS should also be registered with the DoD Component SAP Central Office (SAPCO).

New DoD ISs should be entered into DITPR or SITR at the beginning of the system development life cycle.

Platform IT (PIT) systems are identified, designated as such, and centrally registered at the DoD Component levels but are not recorded in DITPR or SITR since they are not subject to FISMA reporting.

Slide 31 – Milestone Checkpoint 1

This checkpoint taken from NIST SP 800-37 can be used to assess whether you are prepared to go to Step 2 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 each ~~a~~ particular step in the RMF have been completed prior to proceeding to the next step.

Slide 32 - Lesson Summary

You should now be able to:

- Identify security categorization resources
- Define security categorization
- ID roles and responsibilities for RMF Step 1
- Identify information types
- Explain how to assign impact values
- Describe confidentiality security categorization factors
- Define the system boundary and be prepared to complete the Security Plan
- Register the information system

Complete the Assessment questions in order to get credit for this course.