Implementing the NIST Risk Management Framework (RMF) Study Notes.

NIST RMF

- **What will you learn in this course?**
    - You will understand the foundations of the NIST Risk Management Framework.
    - You will learn how to manage organizational risk in your IT systems.
    - You will learn how Categorize systems and select controls to minimize risk.
    - You will learn how Continuously monitor control implementation and risks to the system.
- **What are the requirements or prerequisites for taking your course?**
    - No special tools are required, just a willingness to learn about using the NIST Risk Management Framework.
- **Who is this course for?**
    - Cybersecurity Professionals.
    - Information Technology Practitioners.
    - Risk Management Practitioners.
    - Business Leaders and Executives.

Implementing the NIST Risk Management Framework (RMF) Study Notes.

Lecture 1

Welcome!

- **Risk Management Framework (RMF)**
  - Created by NIST to help provide a risk-based approach to control selection and help manage organizational risk.
  - A process for the preparation, categorization, selection, implementation, assessment, authorization and monitoring of a system and its security controls.
  - RMF can be applied to any system or technology.

- **eMASS**
  - Enterprise Mission Assurance Support Service

- **Framework**
  - A collection of best practices or guidelines that an organization should follow to manage its cybersecurity risk posture.

❖ **NIST RMF** is one of the most popular and widely used cybersecurity frameworks.

- Other Protocols:
  - NIST CSF
  - CIS
  - ISO/IEC 27001/27002

Lecture 3

Risk Management Framework

- The reasons RMF exists
- What RMF was designed for
- How it's implemented
  - **7-Step process:**
    - Prepare
    - Categorize
    - Select
    - Implement
    - Assess
    - Authorize
    - Monitor
  - **RMF**
    - Version 1
    - Version 2 (our focus of study)
  - **Authorization Boundaries**
    - Used to define which elements of a given system are going to be considered in scope for the different assessments.
- **RMF** is able to be scaled upward and downwards

Lecture 4

Summary of RMF

- Our **Goal** is to get to a point where an **authorizing official** can answer this question
    - Are we able to accept the residual risk of this system when we connect it to the network and use it to support our mission?
- There is no practical way to protect every digital asset 100% of the time
- The residual risk is going to be accepted based on the benefits
- **Residual Risk**
    - The risk that's left over in the system after implementing the controls.
- We want to come up with the right amount of **system security** at the right time, at the **right cost**, and with an acceptable amount of **residual risk.**
- **The 7 steps of the RMF process:**
    1. Prepare your organization and your system to manage security and privacy risk
    2. Categorize your system and the information that it processes, stores, and transmits.
    3. Select from the catalog of controls the ones that will help you reduce risk
    4. Implement the controls and document how they're deployed
    5. Assess to determine if the controls are in place
    6. Authorize the system to become a production system
    7. Monitor the implementation of the controls and ensure risks to your system stay reasonable.

Implementing the NIST Risk Management Framework (RMF) Study Notes.

Lecture 5

7-step process

1. **Prepare**
    - Security Risks
    - Privacy Risks

2. **Categorize**
    - Software
    - Hardware
    - Servers
    - Network

    - Categorize those systems based on analysis of how big the impact would be if those assets were deleted.
    - Focus on the information the system is processing, storing, and transmitting, and then categorize based on the impact of loss.

3. **Select**
    - Select controls to help protect those assets that we just categorized in step 2

    ❖ **NIST SP 800-53 revision 5 (Catalog of controls)**

    ✗ Is **NOT** a checklist of all the things you need to do to a system
    ✓ Is a list of things you can choose from and decide what you want

    ❖ The higher the categorization the more controls and protections you're likely going to be using.

4. **Implement**
    - Focuses on how we will take the controls we selected and how we will document how those controls will be employed within the systems

5. **Assess**

- How are those controls actually working after you implemented them?
- There is a lot of controls you can do that are considered administrative controls.
- Make sure those controls we selected and implemented are actually doing what we thought they were going to do.

6. Authorize

- In every organization, there's a senior official who gets to make the decision of when you can hook up something to the corporate network.
- Every organization is going to be different in terms of how much risk they're willing to accept.

7. Monitor

- Ensure that we are doing the proper work of being able to download, install, and validate those security patches.
- Monitoring of the systems and the controls is an ongoing process, and we're going to be assessing the controls' effectiveness through regular testing and analysis
- Risk assessments and impact analysis of the systems
- Reporting on the security and privacy posture of the system back up to the authorizing official

Lecture 6

SP800-37

- **Purpose statement**
- **Outcomes**
- **Tasks**

PREPARE TASKS—ORGANIZATION LEVEL [53]

Table 1 provides a summary of tasks and expected outcomes for the RMF *Prepare* step at the *organization* level. Applicable Cybersecurity Framework constructs are also provided.

TABLE 1: PREPARE TASKS AND OUTCOMES—ORGANIZATION LEVEL

Tasks	Outcomes
TASK P-1 RISK MANAGEMENT ROLES	• Individuals are identified and assigned key roles for executing the Risk Management Framework. [*Cybersecurity Framework*: **ID.AM-6; ID.GV-2**]
TASK P-2 RISK MANAGEMENT STRATEGY	• A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [*Cybersecurity Framework*: **ID.RM; ID.SC**]
TASK P-3 RISK ASSESSMENT—ORGANIZATION	• An organization-wide risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**]
TASK P-4 ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (OPTIONAL)	• Organizationally-tailored control baselines and/or Cybersecurity Framework Profiles are established and made available. [*Cybersecurity Framework*: **Profile**]
TASK P-5 COMMON CONTROL IDENTIFICATION	• Common controls that are available for inheritance by organizational systems are identified, documented, and published.
TASK P-6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)	• A prioritization of organizational systems with the same impact level is conducted. [*Cybersecurity Framework*: **ID.AM-5**]
TASK P-7 CONTINUOUS MONITORING STRATEGY—ORGANIZATION	• An organization-wide strategy for monitoring control effectiveness is developed and implemented. [*Cybersecurity Framework*: **DE.CM; ID.SC-4**]

Lecture 7

RMF VERSION 2

- The Risk management Framework has been updated several times
- RMF is at version 2, which was released in December 2018
- A major goal of version 2 is to make RMF easier to complete while giving better results at a reduced cost

New Prepare step	Missions and business functions	Communications among senior leaders	Privacy risk management processes
The system development life cycle	Incorporation of supply chain	NIST cybersecurity framework	Emphasis on the use of automation

Lecture 8

Information Security and Privacy

- Information Security and Privacy for a long time were treated as two separate thigs and were not integrated together.

- With the latest version of RMF we integrate Information Security and Privacy together

❖ **OMB Circular A-130**

- You're not just looking at the information systems, but also the privacy of the data that's being stored on those information systems.

- Have a close collaboration between your information security programs and your privacy programs.

- **Information Security Program**
  - Protects information and information systems from unauthorized access, use, disclosure, disruption modification, or destruction.

- **Privacy Programs**
  - Ensures compliance with the applicable privacy requirements and for managing the risk to individuals associated with the creation, collection, use, processing, dissemination, storage, maintenance, disclosure, or disposal of PII

- **Information Security**

- Confidentiality, integrity, and availability

- **Privacy**
  - Personally identifiable information

Privacy Control	Security Control
Administrative, technical, or physical safeguard that's going to be employed within an agency to ensure compliance with the applicable privacy requirements and to manage privacy risks	Safeguard or countermeasure prescribed for an information system or for an organization to protect the confidentiality, integrity, and availability of the system and its information

❖ In RMF a control can be a security control or a privacy control, or sometimes you'll have a single control that will work and give you protections in both areas

Lecture 9

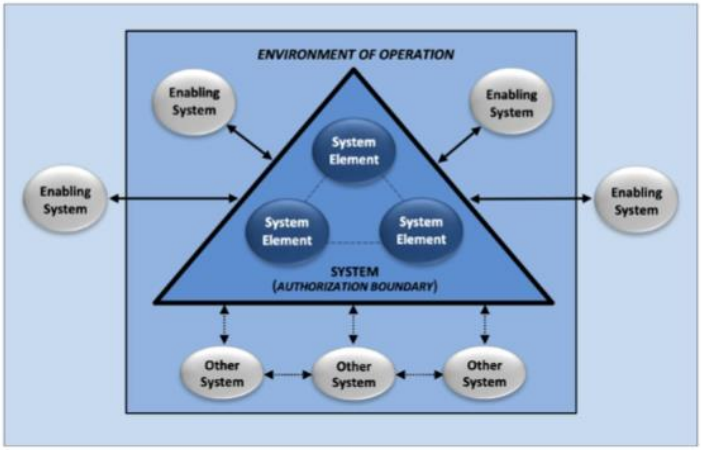
Authorization Boundary

- Authorization Boundaries are really important in RMF because they define what will be considered in scope for the RMF process

- **Authorization Boundary** is the set of system elements, compromising the system to be authorized for the operation or use by an authorizing official.

- This is what the organization is agreeing to protect under its direct management or within the scope of its responsibilities including:
  - People
  - Processes
  - Information Technologies

- Authorization boundaries should be set to the appropriate size.
  - If you have it too large, you're going to be spending a lot more time and money.
  - If you make it too small, you're also going to be running up the cost to your organization.
  - You have to figure out what should be included inside of your authorization boundary



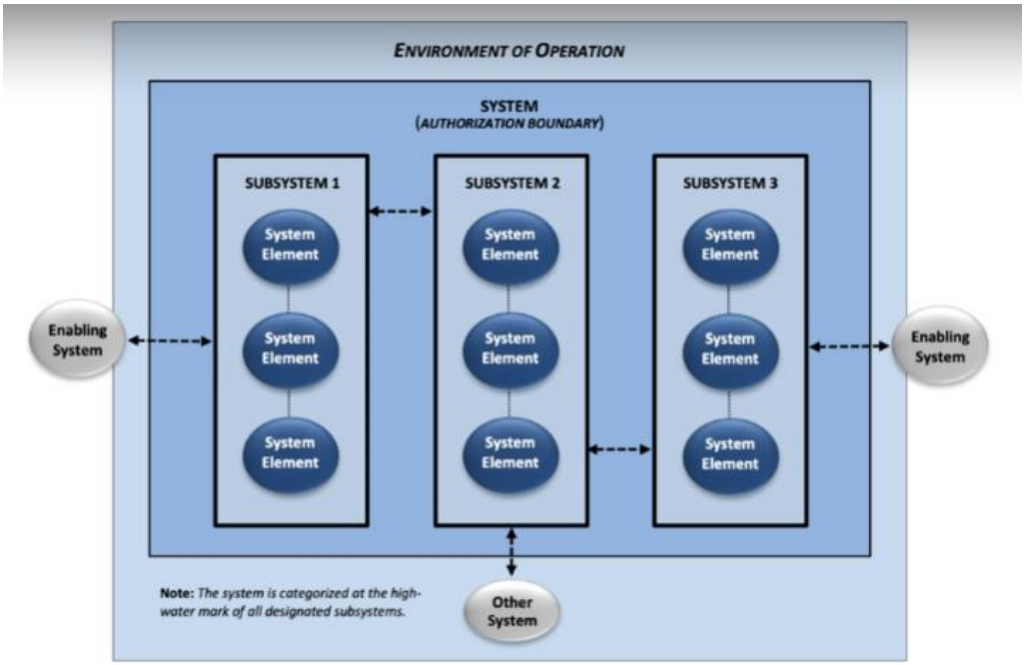


FIGURE G-1: CONCEPTUAL VIEW OF A COMPLEX SYSTEM

- **Enabling System**
  - Provides common controls and includes any type of service or functionality used by the system from some outside environment
  - It exists outside your authorization boundary, but has already been approved to be used through the RMF process

Lecture 10

Supply Chain Risk Management

- Most organizations rely on a lot of external providers and commercial off the shelf products, systems and services. These are all referred to as **third parties.**

- Because of this dependency on third parties, cyber attackers are using the supply chain as an attack vector

- Cleaning up the SolarWinds hack may cost the American economy as much as $100 billion.

- NotPetya caused over $10 billion dollars in damage.

❖ **Supply Chain Risks:**
  - Untrustworthy suppliers
  - Counterfeit parts
  - Tampering
  - Theft of trade secrets
  - Insertion of malicious code
  - Poor manufacturing and development practices

Lecture 11

Requirements Versus Controls

- Are requirements and controls different?

- The term **Requirement**, as used in RMF, includes both legal and policy requirements to protect systems and data.

- Sources in RMF include:
  - Laws
  - Executive orders
  - Directives
  - Regulations
  - Organizational policies
  - Mission needs
  - Business needs
  - Risk assessments

- **Controls**
  - The safeguards and protective capabilities that we put into place to meet our cybersecurity and privacy objectives.
  - NIST Special Publication 800-53 includes hundreds of examples of controls of all types.

Lecture 12

Thoughts on RMF

- Now for most of us who are working in the field, our goal in using RMF is to be able to gain approval to operate some kind of a **sensitive system**, or some kind of a **support system.**

- **Sensitive System**
  - A system that contains or processes sensitive data or plays a key role in mission support
- **Sensitive Data**
  - Information that must be kept safe and out of reach from any outsiders, unless they have a specific permission to be able to access it
  - It's not just classified or regulated data, there's other data that could be sensitive to your organization
- **Mission Support**
  - Any kind of system that is used to assist another system in the accomplishment of their objectives.

❖ **RMF doesn't have to be used for every single system you have, but it does have to be used to gain approval to operate any sensitive systems.**

- ✗ **A framework is not a checklist**
- ✗ **RMF is not to be followed exactly as written**
- ✗ **RMF is not a "one size fits all" type of solution**
- ✓ **RMF can be tailored for your organization**

❖ **Some organizations will be better than others at interpreting and figuring out RMF**

- **Find out with your supervisors and other senior decision makers in your organization which steps and tasks inside RMF are particularly useful**

❖ **RMF requires massive collaboration across your organization**

❖ **RMF can be used in smaller tactical style systems that are only going to be used for a handful of people to support a specific mission, and it may only last for a specific amount of time**

Implementing the NIST Risk Management Framework (RMF) Study Notes.

- **RMF is a framework, which means you can pick and choose the things you need based on your organization's requirements**
- **RMF can be done in many different ways, from a very small scale to a very large scale.**

Lecture 13

Flexibility

- The main intent is to allow organizations to implement the RMF in the most efficient, effective, and cost-effective manner.

- Flexible implementation may include completing tasks in a nonsequential order

- You can use the Cybersecurity Framework to enhance RMF task executions

- **Flexibility can also be applied to:**
    - Control Selection
    - Control Tailoring
    - Organizational security
    - Privacy needs
    - Control Assessments

- **Flexibility can also present a great challenge, as people try to tailor RMF for their situation, they might make some big mistakes.**
- **Be sure to send big tailoring decisions to the authorizing official.**

- **RMF can be difficult to use with legacy systems.**

- **Another RMF assumption is that the system is not currently breached.**

Lecture 14

Timelines

- The 7 steps are not equal in length
- One of the factors that affect the total amount of time to get a package through RMF is the size of the system you're trying to get through the process
- **Soft Skills Matter**.
    - You can use your soft skills to ethically influence the package time to completion for this process
- RMF can be a very long process.
- It's very common to see packages that take 12, 18, 24 months to go through the RMF process
- Always use your soft skills and keep those packages moving through the process

Lecture 15

The Seven Steps

- We'll start with the standard definitions and then explore the real-world RMF implications.
    - Prepare
    - Categorize
    - Select
    - Implement
    - Assess
    - Authorize
    - Monitor

Lecture 16

Step 1: Prepare your Organization

- Organizational Level Tasks
- System Level Tasks

❖ Check out appendix E in SP 800-37 for a summary of all 18 Tasks.

- Organizations have discretion over which tasks and how rigorous they're going to be when assembling a RMF approval package.

Tasks	Outcomes
TASK P-1 RISK MANAGEMENT ROLES	• Individuals are identified and assigned key roles for executing the Risk Management Framework. [*Cybersecurity Framework*: ID.AM-6; ID.GV-2]
TASK P-2 RISK MANAGEMENT STRATEGY	• A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [*Cybersecurity Framework*: ID.RM; ID.SC]
TASK P-3 RISK ASSESSMENT—ORGANIZATION	• An organization-wide risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: ID.RA; ID.SC-2]
TASK P-4 ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (OPTIONAL)	• Organizationally-tailored control baselines and/or Cybersecurity Framework Profiles are established and made available. [*Cybersecurity Framework*: Profile]
TASK P-5 COMMON CONTROL IDENTIFICATION	• Common controls that are available for inheritance by organizational systems are identified, documented, and published.
TASK P-6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)	• A prioritization of organizational systems with the same impact level is conducted. [*Cybersecurity Framework*: ID.AM-5]
TASK P-7 CONTINUOUS MONITORING STRATEGY—ORGANIZATION	• An organization-wide strategy for monitoring control effectiveness is developed and implemented. [*Cybersecurity Framework*: DE.CM; ID.SC-4]

- Make sur there are no conflicts of interest when assigning the same individual to multiple roles.

- **Risk Tolerance**
  - The degree of risk or uncertainty that is acceptable to your organization
    - Risk assessment methodologies

    - Risk response strategies.
    - Evaluating security and privacy risks
    - Monitoring risk over time.

- You are going to need:
    - System level risk assessment results.
    - Insights on risk from continuous monitoring
    - Strategic risk considerations
    - Risks from information exchanges and network connections

Lecture 17

Step 1: Prepare your System

Tasks	Outcomes
TASK P-8 MISSION OR BUSINESS FOCUS	• Missions, business functions, and mission/business processes that the system is intended to support are identified. [*Cybersecurity Framework*: **Profile**; **Implementation Tiers**; **ID.BE**]
TASK P-9 SYSTEM STAKEHOLDERS	• The stakeholders having an interest in the system are identified. [*Cybersecurity Framework*: **ID.AM**; **ID.BE**]
TASK P-10 ASSET IDENTIFICATION	• Stakeholder assets are identified and prioritized. [*Cybersecurity Framework*: **ID.AM**]
TASK P-11 AUTHORIZATION BOUNDARY	• The authorization boundary (i.e., system) is determined.
TASK P-12 INFORMATION TYPES	• The types of information processed, stored, and transmitted by the system are identified. [*Cybersecurity Framework*: **ID.AM-5**]
TASK P-13 INFORMATION LIFE CYCLE	• All stages of the information life cycle are identified and understood for each information type processed, stored, or transmitted by the system. [*Cybersecurity Framework*: **ID.AM-3**; **ID.AM-4**]
TASK P-14 RISK ASSESSMENT—SYSTEM	• A system-level risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA**; **ID.SC-2**]
TASK P-15 REQUIREMENTS DEFINITION	• Security and privacy requirements are defined and prioritized. [*Cybersecurity Framework*: **ID.GV**; **PR.IP**]
TASK P-16 ENTERPRISE ARCHITECTURE	• The placement of the system within the enterprise architecture is determined.
TASK P-17 REQUIREMENTS ALLOCATION	• Security and privacy requirements are allocated to the system and to the environment in which the system operates. [*Cybersecurity Framework*: **ID.GV**]
TASK P-18 SYSTEM REGISTRATION	• The system is registered for purposes of management, accountability, coordination, and oversight. [*Cybersecurity Framework*: **ID.GV**]

- You need to gather:
  - Mission Statements
  - Technology policies
  - Cybersecurity policies

- Stakeholders could be members of your organization or they could be on the outside.

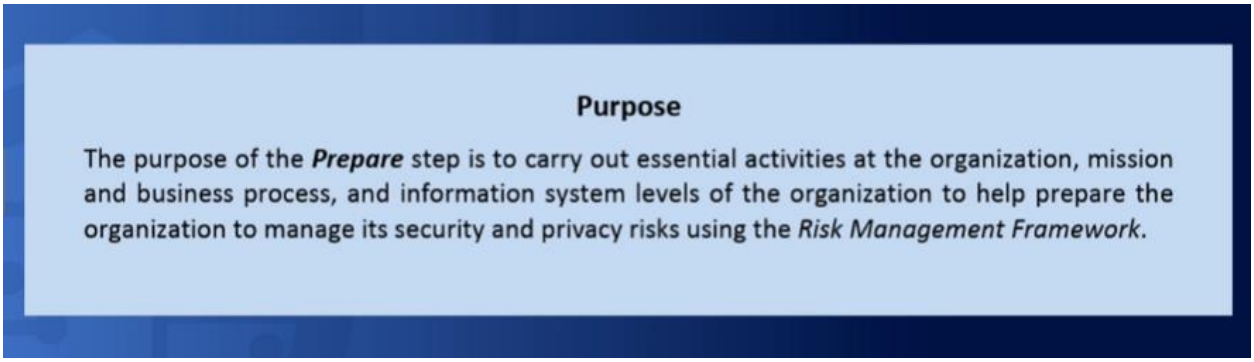
- Assets can include:
  - Software
  - Hardware
  - Computer Networks
  - Business processes
  - Business services
  - Buildings
  - Data

- You need to gather all the documentations about your systems including:
  - Network diagrams
  - Organizational charts
  - System design documents

- For Task P-13 you may need to ask these questions
  - How long are you required to safely store different types of information?
  - How is this data processed in your environment?
  - What types of data do you have to delete, and when?

❖ **Enterprise Architecture**
  - Management practice that maximizes the effectiveness of your business processes

Lecture 18
Step 1 in the Real World



- **We are trying to achieve Five key outcomes:**

1. Ensure key risk management roles are identified
2. Ensure that organizational risk management strategies have been established and that the risk tolerance has been determined.
3. Ensure an organization-wide risk assessment has occurred
4. Ensure an organization-wide strategy for continuous monitoring has been developed and implemented
5. Ensure that common controls have been identified

- **What you want to accomplish during your risk management framework steps:**
  - Ensure you understand who the people are in your organization that are going to be using RMF.
  - Identify what roles those people are going to have

- Determine who is your senior risk official or the risk executive

❖ **Make sure you're identifying who has the appropriate rank and title to be able to make that approval decision for you.**

❖ **This is a lot of pre-work that you're going to be doing before you even start diving deep into all the different concepts of RMF.**

- **Common Controls**

  - Confidentiality
  - Integrity
  - Availability
  - Identification
  - Authorization
  - Authentication
  - Access

- **Inheritance**
  - These are the things that you're going to be able to assume inside of your RMF package because you're inheriting them from a higher level control.
  - If you're inheriting things from another system that is great and you just need to make sure you document that inside of your RMF package.
  - When You use a cloud provider, they're going to be operating on what's known as a shared responsibility model.

- **We need to figure out the roles of different people involved in the RMF process**
  - Information system owner
  - Information system auditor
  - Information system assessor
    - When in the process are they going to be called upon to do those things?

- Let them know that your RMD package is going to be coming through the process and they have been identified to have a role in this project

Lecture 19

Step 2: Categorize your System

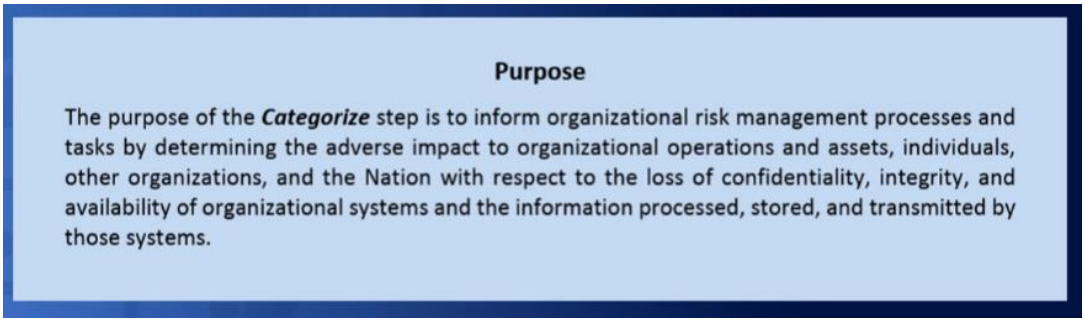
Tasks	Outcomes
TASK C-1 SYSTEM DESCRIPTION	• The characteristics of the system are described and documented. [*Cybersecurity Framework*: **Profile**]
TASK C-2 SECURITY CATEGORIZATION	• A security categorization of the system, including the information processed by the system represented by the organization-identified information types, is completed. [*Cybersecurity Framework*: **ID.AM-1**; **ID.AM-2**; **ID.AM-3**; **ID.AM-4**; **ID.AM-5**] • Security categorization results are documented in the security, privacy, and SCRM plans. [*Cybersecurity Framework*: **Profile**] • Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes. [*Cybersecurity Framework*: **Profile**] • Security categorization results reflect the organization's risk management strategy.
TASK C-3 SECURITY CATEGORIZATION REVIEW AND APPROVAL	• The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.

- Descriptive Information you can include in your security and privacy plans:
  - Name
  - Version
  - Owner
  - Custodian
  - Manufacturer
  - Organization
  - Location

❖ **Make sure that all key stakeholders are aware of what classification have been selected for your data types.**

Lecture 20

Step 2 in the Real World



- Three main outcomes:
  - The system's characteristics are documented.
  - The security categorization of the system and information has been completed.
  - The categorization decision has been reviewed and approved by the authorizing official.

❖ We have to ask: What's unique about the system? and the mission it's been designed to fulfill.

❖ Some systems have unique CIA requirements

❖ RMF users are expected to adapt RMF to their specific situation.

❖ Go through NIST SP 800-53 and start seeing the types of controls that you can select from.

❖ How to define what type of information is being used in those systems
  - Understand the risk tolerance of our organization so we can determine exactly how much we have to mitigate down that risk to what is considered unacceptable level.

- Once you decide what level of information you have, you can then figure out what things are being dictated to you and what things your organization can add on top of that.
- Figure out what level does your information need to be protected to.
- Categorize your systems based on the information it's going to be processing
- Classification of information can often be a negotiation
- As you go higher in levels, you're going to have additional controls, additional costs and additional time added to that system.
- People will try to negotiate downward the level they're going to categorize that information so they can get through the process easier.
- We're deciding how we're going to categorize the information in the system and the system that processes that information

Lecture 21

Step 3: Select Controls

- **Controls**
  - The things your organization implements to meet your cybersecurity supply chain and privacy requirements.
    - Technical
    - Administrative
    - Physical
  - Can also be sorted into:
    - Preventative
    - Detective
    - Corrective

Tasks	Outcomes
TASK S-1 CONTROL SELECTION	• Control baselines necessary to protect the system commensurate with risk are selected. [*Cybersecurity Framework*: **Profile**]
TASK S-2 CONTROL TAILORING	• Controls are tailored producing tailored control baselines. [*Cybersecurity Framework*: **Profile**]
TASK S-3 CONTROL ALLOCATION	• Controls are designated as system-specific, hybrid, or common controls. • Controls are allocated to the specific system elements (i.e., machine, physical, or human elements). [*Cybersecurity Framework*: **Profile**; **PR.IP**]
TASK S-4 DOCUMENTATION OF PLANNED CONTROL IMPLEMENTATIONS	• Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents. [*Cybersecurity Framework*: **Profile**]
TASK S-5 CONTINUOUS MONITORING STRATEGY—SYSTEM	• A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed. [*Cybersecurity Framework*: **ID.GV**; **DE.CM**]
TASK S-6 PLAN REVIEW AND APPROVAL	• Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorizing official.

❖ You can select controls in two ways:
  - Baseline control selection

        - When you choose a pre-written set of controls that was made to help your organization with their security and privacy needs.

    - Organization generated control selection
        - Do it yourself way to go and you don't start with a predefined set of controls.

- An organization generated selection could be more cost-effective

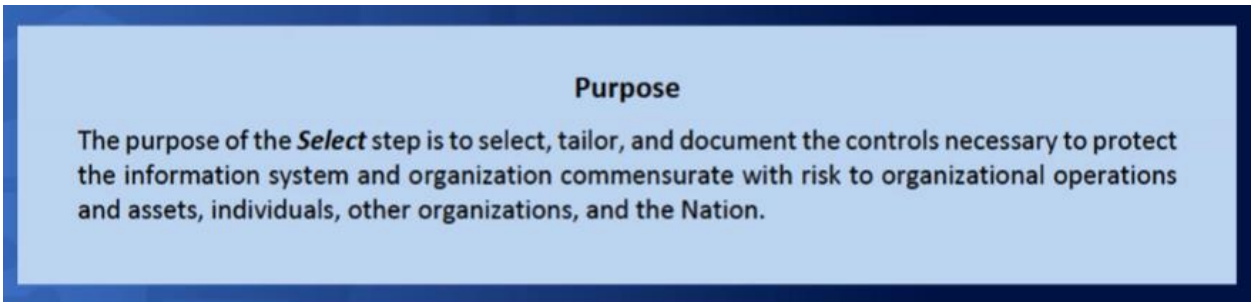
- **Common controls** satisfy security and privacy requirements at the organization level and are inherited by one or more systems

- **Hybrid controls** are partially inherited by one or more systems, which means your system may or may not inherit controls

- **System specific** controls provide a protective function for a single system.

- Continuously monitoring your controls at a system level is an important aspect of managing the ongoing risk to your system.

Lecture 22
Step 3 in the Real World



- We need five outcomes:
    1. Ensure that we have control baseline selected and tailored.
    2. Ensure the controls are designated as system specific, hybrid or common.
    3. Controls have to be allocated to specific system components.
    4. System level continuous monitoring strategies need to be developed.
    5. The security and privacy plans that reflect the control selection, designation and allocation have been reviewed and approved.
- Now we're going to select all the different controls to be able to meet that level of categorization.
- We can actually tailor the RMF process to be more or less stringent.

- Control Enhancements
    - Additional controls that allow to tune that control a little to better manage the risk that's associated with that given piece of information

- Work closely with a system administrator who has a strong technical background to be able to help you tailor these controls and get the most out of them.
    - Information System Security Engineer (ISSE)

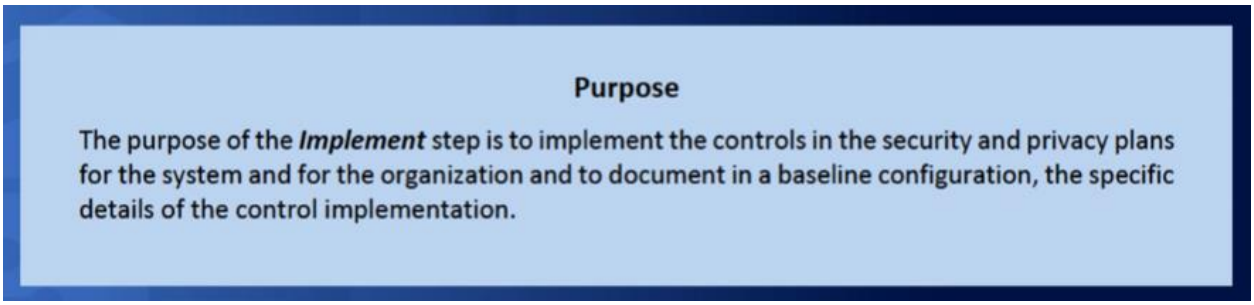
- You can also use administrative or management controls

- As you're figure out which controls you want to use, you're always focused on what is the outcome that I'm trying to achieve?
- Select, tailor, and document the controls that are necessary to protect the system

Lecture 23
Step 4: Implement Controls

Tasks	Outcomes
TASK I-1 CONTROL IMPLEMENTATION	• Controls specified in the security and privacy plans are implemented. [*Cybersecurity Framework*: **PR.IP-1**] • Systems security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans. [*Cybersecurity Framework*: **PR.IP-2**]
TASK I-2 UPDATE CONTROL IMPLEMENTATION INFORMATION	• Changes to the planned implementation of controls are documented. [*Cybersecurity Framework*: **PR.IP-1**] • The security and privacy plans are updated based on information obtained during the implementation of the controls. [*Cybersecurity Framework*: **Profile**]

Lecture 24
Step 4 in the Real World



- We want two outcomes:
  1. The control specified in the security and privacy plans have been implemented
  2. Security and privacy plans have been updated to reflect controls as implemented.

- In step 4, we are going to be focused on implementing all those different controls that we selected back in step 3.
- Oftentimes, Implementation is going to be done by more than one person across multiple disciplines depending on what type of controls you're trying to put in place.
- It's important to have specialists that do the implementation.
- We are going to be implementing all of the different controls we've selected for our system which can be very lengthy
- Most of the time the implementer is going to be a system administrator.
- We are looking at each individual security control and then we're going to figure out what the best solution is to meet that requirement.

- **STIG V-93539**
  - Windows server 2019 must restrict anonymous access to Named Pipes and Shares

- If you have multiple different systems, you're also going to have multiple different STIGs and controls that are going to be applied across those systems.
- Project management skills are going to be critically important
- When you're building out your plans, this includes your implementation plans, make sure you're giving dates for each of those

- Always ask for:
  - Estimate for the timeline
  - The Big blockers

- Adding more people isn't necessarily going to make things go faster.
- Sometimes you can make things go faster by adding money, adding resources, or eliminating other priorities from their pile.
- It's important to consider the real-world circumstances surrounding that control.
- Understand what type of environment your system is going to be used in.
- There will going to be many times where you're not able to meet the control as written because of the environment that you're operating within.

Lecture 25
Step 5: Assess Controls

Tasks	Outcomes
TASK A-1 ASSESSOR SELECTION	• An assessor or assessment team is selected to conduct the control assessments. • The appropriate level of independence is achieved for the assessor or assessment team selected.
TASK A-2 ASSESSMENT PLAN	• Documentation needed to conduct the assessments is provided to the assessor or assessment team. • Security and privacy assessment plans are developed and documented. • Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and the level of effort required.
TASK A-3 CONTROL ASSESSMENTS	• Control assessments are conducted in accordance with the security and privacy assessment plans. • Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered. • Use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments.
TASK A-4 ASSESSMENT REPORTS	• Security and privacy assessment reports that provide findings and recommendations are completed.
TASK A-5 REMEDIATION ACTIONS	• Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken. • Security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions. [*Cybersecurity Framework*: **Profile**]
TASK A-6 PLAN OF ACTION AND MILESTONES	• A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed. [*Cybersecurity Framework*: **ID.RA-6**]

- ❖ Assessors must have enough feelings of independence to be able to make truthful judgements.
- ❖ In-house versus contracted assessors

- For Task A-2
  - Single integrated plan for both security and privacy controls,
  - or two plans, one for each category.
  - Evaluation of the control objectives

- The assessment procedures for each control.

- For Task A-4
  - The amount of detail in the report should be appropriate to the type of control assessment that was conducted.
  - Control assessment results can be documented in interim reports

❖ If significant security or privacy risks are discovered during the assessment, then those should be mitigated as soon as possible.
❖ Your organization can prepare an addendum to your security and privacy assessment reports that provides an opportunity for system owners and control providers to respond to your assessment.

- A **POAM** includes:
  - Tasks to be accomplished
  - Recommendations for completion
  - Resources required
  - Milestones established
  - Scheduled completion dates

Lecture 26
Step 5 in the Real World

Purpose

The purpose of the ***Assess*** step is to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.

- We have eight main outcomes
  1. Select the assessor or assessment team
  2. Develop our security and privacy assessment plans.
  3. Review and approve those assessment plans.
  4. Control assessments are going to be conducted in accordance with the assessment plans.
  5. Security and privacy assessment reports are going to be developed.
  6. Remediation actions to address deficiencies in the controls are undertaken.
  7. Security and privacy plans are updated to reflect control implementation changes based on the assessment and remediation actions we took.
  8. Plan of action and milestones has been developed and is ready for action.

- We're verifying that we actually implemented them properly and we're getting the outcome that we expected from those controls.
- The assess phase is an open book exam
- This is done by some kind of person who doesn't report to you through the same reporting chain.

- Remember Three Keywords
  - **Observe**
  - **Interview**
  - **Test**

- You have to determine exactly what the priorities are going to be.

- Meet with the authorizing official upfront to make sure you have good scoping of your assessment plan
- It's important that you give grace to other people that you're working with during this process.
- You care whether or not that system is going to be secure.
- No system you assess is going to pass 100%
- Document everything you find that is not optimal and those things can be recommendations for improvement
- Again, it's important that you use your soft skills.

Lecture 27
Step 6: Authorize the System

Purpose

The purpose of the *Authorize* step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable.

Tasks	Outcomes
TASK R-1 AUTHORIZATION PACKAGE	• An authorization package is developed for submission to the authorizing official.
TASK R-2 RISK ANALYSIS AND DETERMINATION	• A risk determination by the authorizing official that reflects the risk management strategy including risk tolerance, is rendered.
TASK R-3 RISK RESPONSE	• Risk responses for determined risks are provided. [*Cybersecurity Framework*: **ID.RA-6**]
TASK R-4 AUTHORIZATION DECISION	• The authorization for the system or the common controls is approved or denied.
TASK R-5 AUTHORIZATION REPORTING	• Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.

- **The Authorization Package includes:**
  - Security and privacy plans
  - Assessment reports
  - Plans of action
  - Milestones
  - executive summary

- **After risk determination you can:**
  - Accept the risk
  - **Mitigate the risk**
    - The authorizing official is the only one who can approve of a risk being mitigated or accepted
    - Your planned mitigation should be included in and tracked using your POAM

Lecture 28
Step 6 in the Real World

Purpose

The purpose of the *Authorize* step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable.

- We want four outcomes:
    1. Ensure an authorization package has been created.
    2. Ensure a risk determination has been rendered.
    3. Ensure that risk responses have been provided.
    4. Ensure that the authorization for the system or common controls have been approved or denied

- Get authorization to operate the system which is known as an ATO.
- The question you need to ask is, is this an acceptable level that is low enough that we can accept the residual risk?
- These things aren't linear and we do have to circle back and start earlier again in the process
- When it comes to authorization, sometimes you are going to have difficulty figuring out who is going to be the authority for that package.
- If you do a good job in your preparation phase, you'll be able to identify these pain points early on and be able to find ways to get around these blockages
- The biggest issue these days when it comes to the authorization step, is actually finding somebody who has time to go through that package
- It's important to understand who is going to be the one making this authorization decision

- Understand what you're trying to achieve as the result of this authorized step, you want one of three possible outcomes:
    1. Your package can be accepted the way it is and you get a full ATO
    2. Denial
    3. Interim authority to operate (IATO)
        - An IATO can transition into a full ATO

Lecture 29
Step 7: Monitor the System

Purpose

The purpose of the ***Monitor*** step is to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions.

- Be on the lookout for unauthorized changes

Implementing the NIST Risk Management Framework (RMF) Study Notes.

Tasks	Outcomes
TASK M-1 SYSTEM AND ENVIRONMENT CHANGES	• The information system and environment of operation are monitored in accordance with the continuous monitoring strategy. [*Cybersecurity Framework*: **DE.CM**; **ID.GV**]
TASK M-2 ONGOING ASSESSMENTS	• Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy. [*Cybersecurity Framework*: **ID.SC-4**]
TASK M-3 ONGOING RISK RESPONSE	• The output of continuous monitoring activities is analyzed and responded to appropriately. [*Cybersecurity Framework*: **RS.AN**]
TASK M-4 AUTHORIZATION PACKAGE UPDATES	• Risk management documents are updated based on continuous monitoring activities. [*Cybersecurity Framework*: **RS.IM**]
TASK M-5 SECURITY AND PRIVACY REPORTING	• A process is in place to report the security and privacy posture to the authorizing official and other senior leaders and executives.
TASK M-6 ONGOING AUTHORIZATION	• Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.
TASK M-7 SYSTEM DISPOSAL	• A system disposal strategy is developed and implemented, as needed.

- Assessing control effectiveness is part of continuous monitoring
- The authorizing official will determine the best risk response to the new assessment findings

- In task M-5, reporting can be event driven, time driven, or a combination of both.

- Summarize changes to security and privacy plans, assessment reports, and plans of action and milestones since the last report.

- Controls addressing system disposal have to be implemented including:
  - Media Sanitization
  - Configuration management and control
  - Component authenticity
  - Record retention

- Users and application owners hosted on the system have to be notified in a timely manner
- Ensure that disposal complies with federal laws, regulations, directives, policies, and standards.

Lecture 30
Step 7 in the Real World

Purpose

The purpose of the ***Monitor*** step is to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions.

- We want five main outcomes:
  1. The system and environment of operation is going to be monitored in accordance with the continuous monitoring strategy.
  2. Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy.
  3. The output of continuous monitoring activities is analyzed and responded to.
  4. There's a process in place to report security and privacy posture to your management.
  5. Ongoing authorizations are conducted using the results of continuous monitoring activities.
- Understand all of the risk to our system and what controls are put in place and we're verifying those controls remain effective against risks.

- This is where you really want to pair RMF with the NIST Cybersecurity framework

Lecture 31
Associated Topics

- In this section we cover some topics that help you implement RMF including:
  - RMF Automation
  - Web-based portals
  - RMF and CSF integration

- There are many solutions to help with automation
  - Commercial tools
  - Government software

- Enterprise Mission Assurance Support Service (eMASS)

- RMF and CSF in the Real World

Lecture 32
Automating RMF

- Xacta 360 is a commercial tool built by telos used for automating your ATO
- Some federal agencies have built their own dedicated NIST RMF automation tools
- Other federal agencies like the Department of the Interior use the Cybersecurity Assessment and Management System.
- You can create your own automated workflow using Microsoft SharePoint web platform
- Enterprise Mission Assurance Support Service (eMASS)

Lecture 33
eMASS

- Enterprise Mission Assurance Support Service (eMASS)
  - Government-owned web-based application that provides a wide range of fully integrated comprehensive cybersecurity management services including:
    - Dashboard for reporting
    - Control scorecard measurement
    - System security authorization packages

- Government Off-The-Shelf (GOTS)allows for an easier and more automated method of gaining authorization for your RMF packages.
- The eMASS system was created by the Department of Defense, known as the DoD
- DoD Information Assurance Certification and Accreditation Process (DIACAP)
- eMASS allows cybersecurity professionals to spend more time on securing networks and their systems
- By using an automated system like eMASS, we're going to be able to improve our cycle time during the RMF approval process

- eMass has seven main capabilities
  1. eMASS can be used to automatically generate DIACAP and RMF reports to support package approval.
  2. eMASS can be used to create enterprise level visibility of all authorization packages within a given organization.
  3. eMASS can be used to manage all the cybersecurity compliance activities and automation throughout the workflow process.
  4. eMASS can also be used to maintain the enterprise baseline for security controls by storing them inside of the eMASS repository.
  5. eMASS can be used to fully automate inheritance
  6. eMASS can be integrated with a Continuous Monitoring Risk Scoring system (CMRS)
  7. eMASS can allow product teams, testers, and security control assessors to effectively collaborate and execute security assessments from geographically dispersed locations

- When categorizing your system, it's important to use the NIST SP 800-60

Implementing the NIST Risk Management Framework (RMF) Study Notes.

- How eMass works:
    1. Start out by inputting all of your data into the eMASS system.
    2. Find the baseline for your hardware and software of that proposed system
    3. Create authorization boundary
    4. Apply all the requirements and controls from your STIGs
    5. Start working on getting an ATO

- Continuous Monitoring can be:
    - Weekly
    - Monthly
    - Quarterly
    - Annually

- We can use our vulnerability scans that are inside eMASS to automate the process of identifying any security controls that are not being implemented properly

- You can use it to notify you of any software or controls that are considered noncompliant based on your listed baseline

- It also can help walk you through the RMF process as a whole

Lecture 34
eMASS Risks

- eMASS comes with benefits, but there's also increased risk
- eMASS users put every single design and system security engineering aspect into one web-based application
- How do we know eMASS is secure for our use?
- Speak with your approving official if you have any security concerns about using eMASS or any other automated system

Lecture 35
RMF and CSF

- Are they the same?
- Is one just a newer version of the other?
- Are they competing with each other?

❖ **RMF** is required for federal government organizations and it's hardly ever used in the private sector.

❖ **CSF** is voluntary and it's aimed towards organizations in critical infrastructure industries

❖ **RMF** requires far more documentation

❖ Implementing the **RMF** requires formal authorization to operate

❖ **RMF** is organized around the software development life cycle while **CSF** is organized around the life cycle of a security incident.

❖ **CSF** was created by private industry through the facilitation of NIST

❖ **RMF** was developed by the Joint Task Force, interagency working group.

❖ How can RMF and CSF be used together?

  - Use CSF to strengthen the RMF process