Introduction to the Risk Management Framework

Welcome to the Introduction to the Risk Management Framework.

Overview

Paul: Hey Mary - did you hear that DoD is adopting something called RMF? What is that?

Mary: Oh, Hi Paul. Sure, I was just working on developing some training for RMF. RMF stands for Risk Management Framework which is a new method of conducting the Certification & Accreditation process for DoD Information Systems.

Paul: Uh-oh… I guess that means big changes for us, huh?

Mary: Well, Yes and no. The changes are an evolution of existing practices, but they're also a step forward. They advance the practice of Information Assurance at DoD. The changes recognize cyber defense as an integral component of Information Assurance policies and procedures government wide.

Paul: So, I guess Certification and Accreditation is no longer just about checking off boxes for compliance.

Mary: You're right. DoD has recognized that the threat environment demands a more mature and integrated process. Understanding RMF is mission critical for us all. Here let me show you what I was just working on…

Paul: Sure.

RMF Topics

The Risk Management Framework or RMF is the common information security framework for the federal government. RMF aims to improve information security, strengthen the risk management processes, and encourage reciprocity among federal agencies.

The topics we will cover include:

- Policies and regulations that govern the DoD Transition to RMF
- Categories of DoD Information Technology affected by RMF
- The six steps in the implementation of RMF
- RMF applicability to the DoD Acquisition Process
- RMF Transition Timelines

Course Objectives

At the end of this course you will be able to identify policies and regulations that govern the DoD Transition to RMF, define DoD Information Technology affected by RMF, and understand the implementation of RMF.

Please allow 30 minutes for completion of this course. Follow the on-screen instructions to advance through the course. You will also find options for course resources and transcripts of the course material.

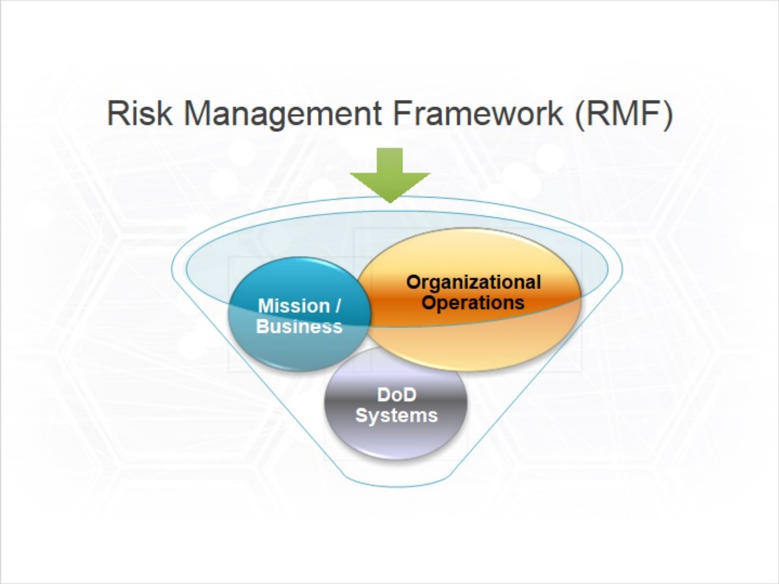
To receive a certificate of completion for this course, you must also take the final exam.

RMF Introduction

RMF Introduction

Let’s begin by looking back to see how the DoD transformation to the Risk Management Framework started.

RMF Introduction Cont'd



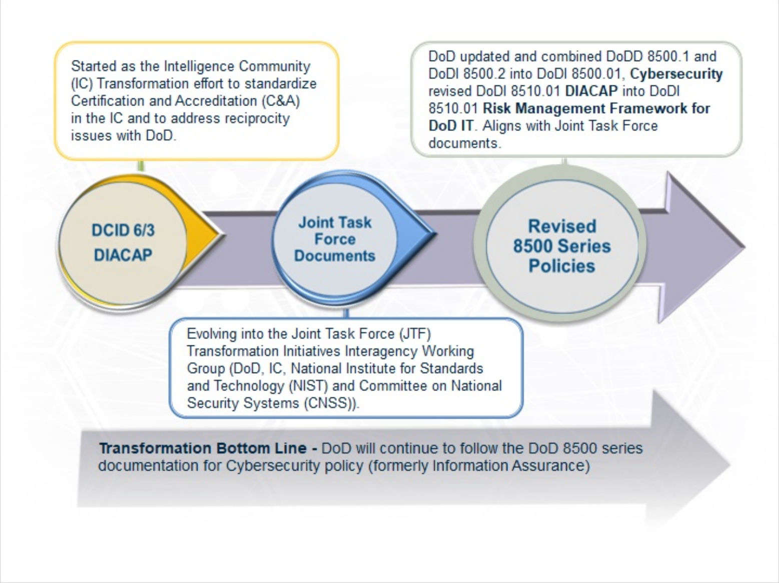
Risk Management Framework (RMF)

Everybody knows that Information technology and systems are integral to operations at DoD. While these systems have brought great benefits to the battlefield and the office, they also represent a vulnerability.

DoD systems are subject to threats that can have adverse effects on organizational operations and assets, individuals, and the Nation.

These threats can compromise the confidentiality, integrity, or availability of information processed, stored, or transmitted by DoD systems.

Transformation to the RMF



Started as the Intelligence Community (IC) Transformation effort to standardize Certification and Accreditation (C&A) in the IC and to address reciprocity issues with DoD.

DoD updated and combined DoDD 8500.1 and DoDI 8500.2 into DoDI 8500.01, **Cybersecurity** revised DoDI 8510.01 **DIACAP** into DoDI 8510.01 **Risk Management Framework for DoD IT**. Aligns with Joint Task Force documents.

Evolving into the Joint Task Force (JTF) Transformation Initiatives Interagency Working Group (DoD, IC, National Institute for Standards and Technology (NIST) and Committee on National Security Systems (CNSS)).

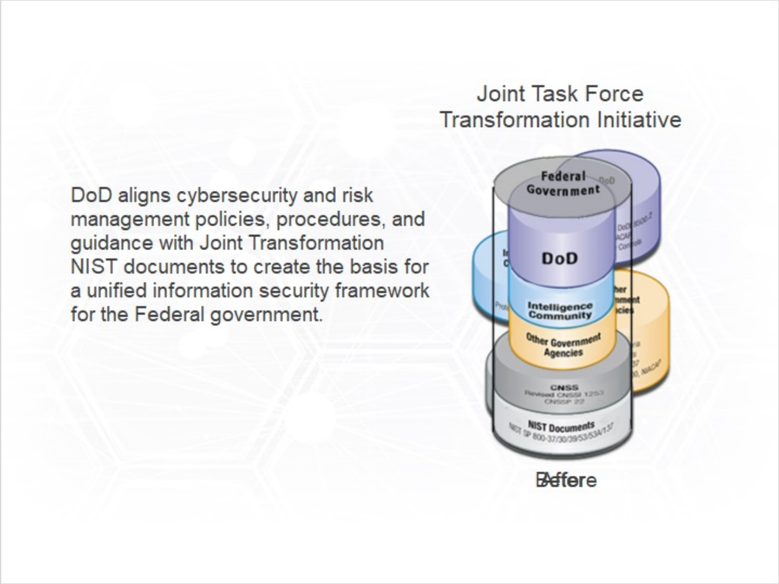
Transformation Bottom Line - DoD will continue to follow the DoD 8500 series documentation for Cybersecurity policy (formerly Information Assurance)

In an effort to counter these threats, DoD has transformed its cybersecurity policy - employing a joint task force in its evolution from the Defense Information Assurance Certification & Accreditation Process (DIACAP) to the adoption of new Cybersecurity policy under DoDI 8500.01 and the Risk Management Framework under DoD 8510.01.

The Risk Management Framework, supported by the National Institute of Standards and Technology (NIST) 800-series publications and already in use by other federal agencies under the Federal Information Security Management Act, provides a structured, yet flexible approach for managing risk resulting from the incorporation of information systems into the mission and business processes of an organization.

Even with the changes, DoD will continue to follow the DoD 8500 series documentation for cybersecurity policy.

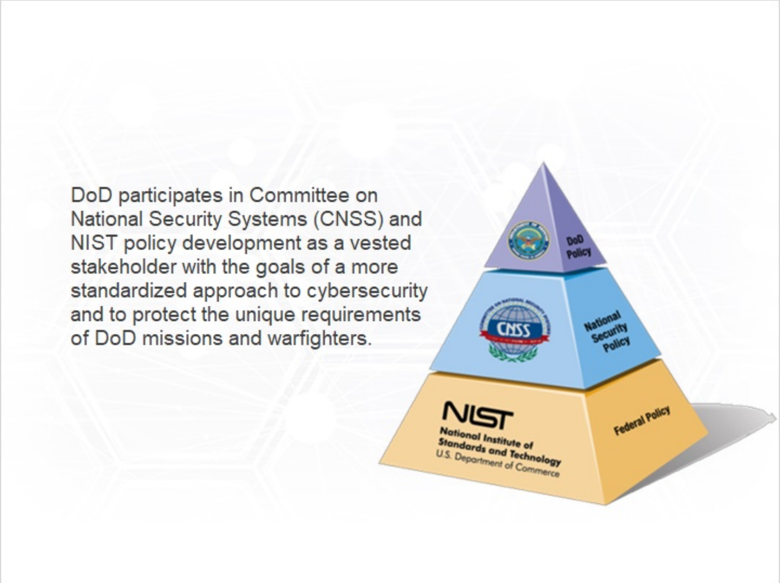
Policy Alignment



DoD aligns cybersecurity and risk management policies, procedures, and guidance with Joint Transformation NIST documents to create the basis for a unified information security framework for the Federal government.

DoD is not reinventing the wheel, it is simply aligning cybersecurity and risk management policies, procedures, and guidance with Joint Transformation NIST documents to create the basis for a unified information security framework for the Federal government.

Policy Partnerships

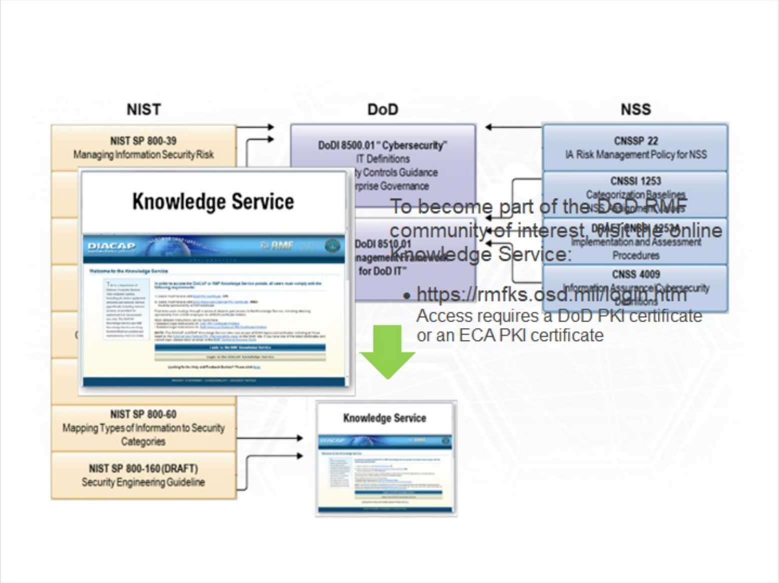


DoD participates in Committee on National Security Systems (CNSS) and NIST policy development as a vested stakeholder with the goals of a more standardized approach to cybersecurity and to protect the unique requirements of DoD missions and warfighters.

DoD Policy
CNSS
National Security Policy
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Federal Policy

DoD participates in Committee on National Security Systems (CNSS) and NIST policy development as a vested stakeholder with the goals to create a more standardized approach to cybersecurity and to protect the unique requirements of DoD missions and warfighters.

RMF Guidance Alignment



To become part of the DoD RMF community of interest, visit the online Knowledge Service:

- https://rmfks.osd.mil/login.htm
  Access requires a DoD PKI certificate or an ECA PKI certificate

The NIST and CNSS policy partnerships ensure that DoD RMF guidance is aligned with NIST and CNSS standards and guidance.

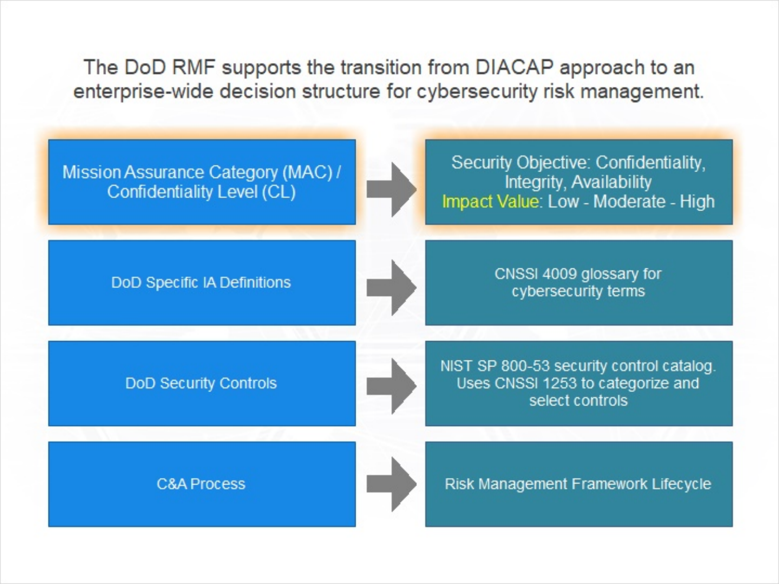
DoD is committed to making the transition to RMF seamless and, to that end, will be deploying an RMF Knowledge Service.

Many of you may be familiar with the DIACAP Knowledge Service. The RMF Knowledge Service is currently being developed and will be housed in a new portal as soon as the initial content is finalized.

Once content has been deployed, a link to the new portal will be provided on the main DIACAP Knowledge Service splash page at the website identified on your screen.

The DIACAP Knowledge Service will remain online to support current systems.

DIACAP Transition to RMF



The DoD RMF supports the transition from DIACAP approach to an enterprise-wide decision structure for cybersecurity risk management.

Mission Assurance Category (MAC) / Confidentiality Level (CL) → Security Objective: Confidentiality, Integrity, Availability Impact Value: Low - Moderate - High

DoD Specific IA Definitions → CNSSI 4009 glossary for cybersecurity terms

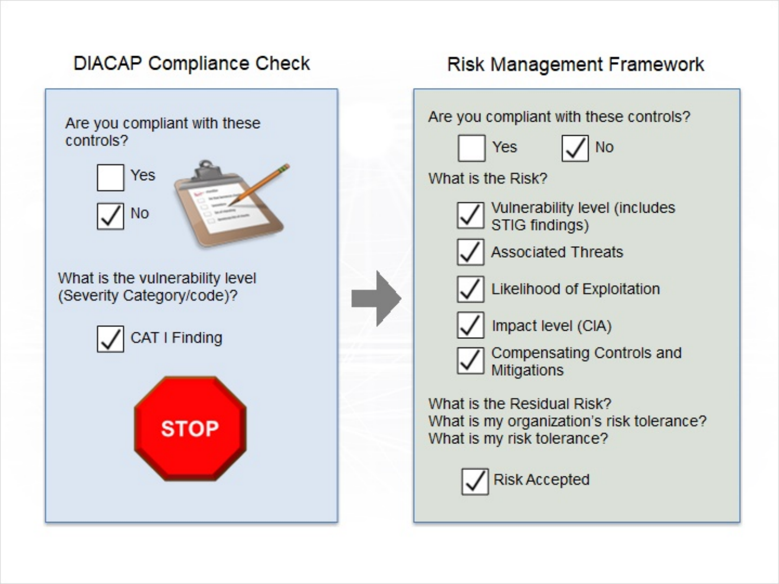
DoD Security Controls → NIST SP 800-53 security control catalog. Uses CNSSI 1253 to categorize and select controls

C&A Process → Risk Management Framework Lifecycle

The DoD RMF supports the transition from a DIACAP approach to an enterprise wide decision structure for cybersecurity risk management.

Although some of the terminology and processes may change - for example Mission Assurance Categories will now be known as Impact Values - the concepts behind them remain the same.

DIACAP to RMF



DIACAP Compliance Check

Are you compliant with these controls?

☐ Yes

☑ No

What is the vulnerability level (Severity Category/code)?

☑ CAT I Finding

Risk Management Framework

Are you compliant with these controls?

☐ Yes ☑ No

What is the Risk?

☑ Vulnerability level (includes STIG findings)

☑ Associated Threats

☑ Likelihood of Exploitation

☑ Impact level (CIA)

☑ Compensating Controls and Mitigations

What is the Residual Risk?
What is my organization's risk tolerance?
What is my risk tolerance?

☑ Risk Accepted

Under the RMF, technical and non-technical features of DoD Information systems will be comprehensively evaluated in the intended environment.

This allows an Authorizing Official, formerly referred to as the Designated Approving Authority, to determine whether or not the system is approved to operate at an acceptable level of security risk based on the implementation of an approved set of technical, managerial, and procedural countermeasures or mitigations.

We'll explore the specifics of these controls under the Implementation Guidance portion of this course.

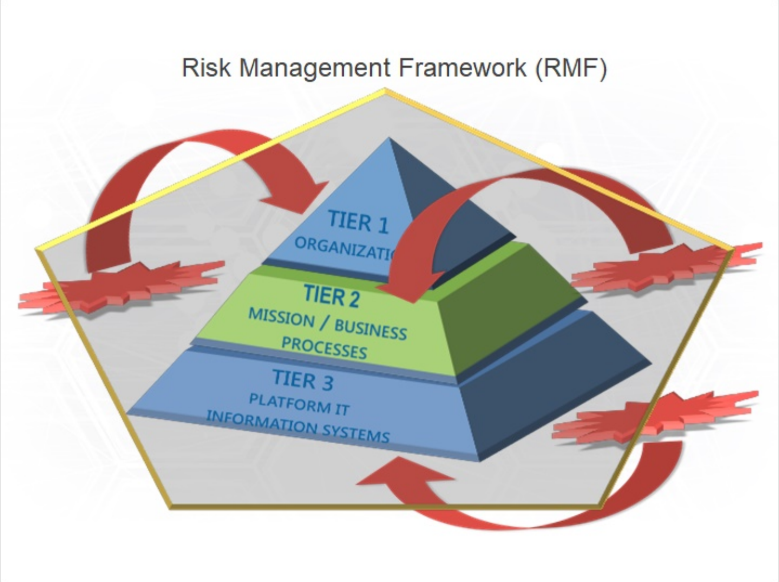
So while it sounds complex, the Risk Management Framework builds on existing information assurance policy by providing a structured, yet flexible approach for managing risk.

RMF Governance

RMF Governance

Now, let's talk about the governance of the risk management framework under the Department of Defense.

RMF Governance Overview



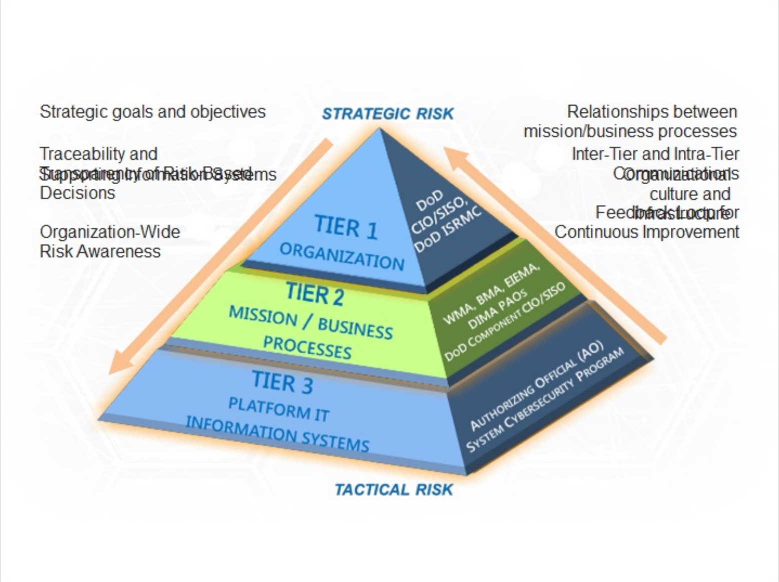
Governance of RMF is strategic in nature and recognizes that managing risk from the operation and use of information systems is critical to your organization's goals and mission.

Risk management should be considered within the enterprise architecture. It requires an organization-wide perspective to ensure that day-to-day operations are conducted within a secure environment commensurate with risk.

Attacks on information systems today are often well-organized, disciplined, aggressive, well-funded, and extremely sophisticated. Successful attacks on public and private sector information systems can result in harm to U.S. national and economic security interests.

Given the significant danger of these attacks, all individuals within the organization must understand their responsibilities in managing the risk from operating information systems that support the mission / business functions of the organization, and take responsibility for risk consequences and mitigation.

DoD RMF Guidance


Strategic goals and objectives
Traceability and Transparency of Risk-Based Decisions
Supporting Information Systems
Organization-Wide Risk Awareness
STRATEGIC RISK
Relationships between mission/business processes
Inter-Tier and Intra-Tier Communications
Organizational culture and infrastructure
Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
DoD CIO/SISO, DoD ISRMC
TIER 2
MISSION / BUSINESS PROCESSES
WMA, BMA, EIEMA, DIMA PAOs
DoD COMPONENT CIO/SISO
TIER 3
PLATFORM IT
INFORMATION SYSTEMS
AUTHORIZING OFFICIAL (AO)
SYSTEM CYBERSECURITY PROGRAM
TACTICAL RISK

The complex, many-to-many relationships among mission or business processes and the information systems supporting those processes require a holistic, organization-wide view for managing risk. A holistic approach requires the management of risk at both the enterprise-level and system-level. This approach takes into account the organization as a whole, including strategic goals and objectives and relationships between mission/business processes and the supporting information systems.

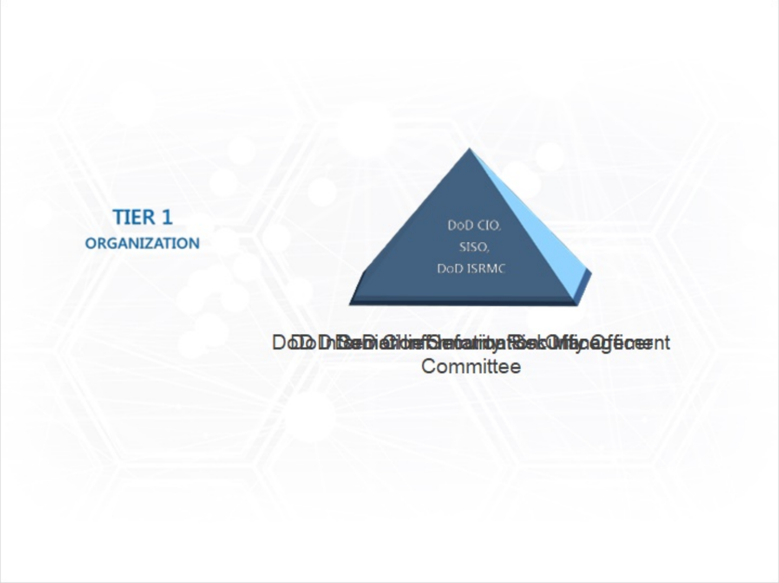
Organizational culture and infrastructure should also be considered.

The security controls and safeguards selected by the organization must take into account:

- Potential mission or business impacts;
- Risk to organizational operations and assets, individuals, other organizations, and the Nation.

These roles and responsibilities have been delegated enterprise wide and are arranged into tiers.

Guidance Tier 1

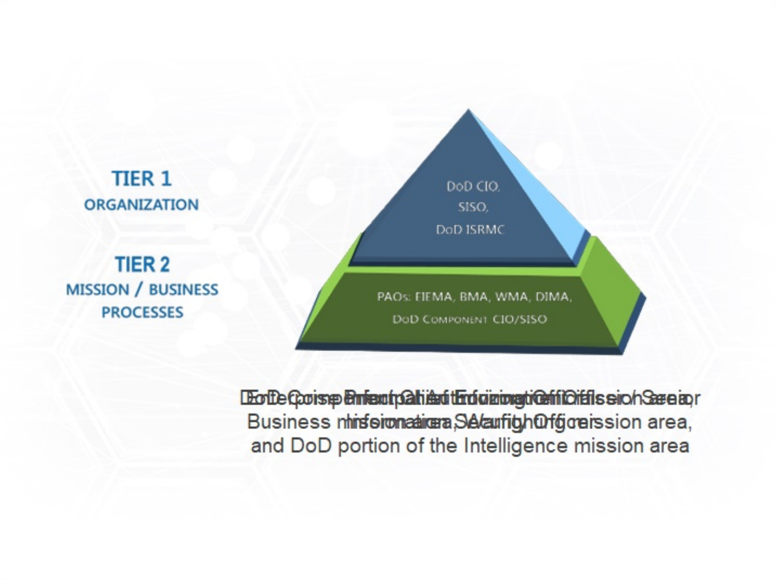


Tier 1 is the Office of Secretary of the Defense and it addresses risk management at the DoD enterprise level.

Key governance elements in Tier 1 are:

- DoD Chief Information Officer who Directs and oversees the cybersecurity risk management of DoD IT
- DoD Senior Information Security Officer or SISO who:
  - Represents the DoD CIO
  - Directs and coordinates the DoD Cybersecurity Program
  - Establishes and maintains the DoD RMF
- DoD Information Security Risk Management Committee that performs the DoD Risk Executive Function

Guidance Tier 2


TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS
PROCESSES
DoD CIO,
SISO,
DoD ISRMC
PAOs: EIEMA, BMA, WMA, DIMA,
DoD Component CIO/SISO
For Principal Authorizing Officials
DoD Component Chief Information Officer and Senior Information Security Officer
Enterprise Information Environment mission area,
Business mission area, Warfighting mission area,
and DoD portion of the Intelligence mission area

Tier 2 is the Mission Area and Component levels, and addresses risk management at these levels.

The key governance element in Tier 2 is the Principal Authorizing Official (PAO).

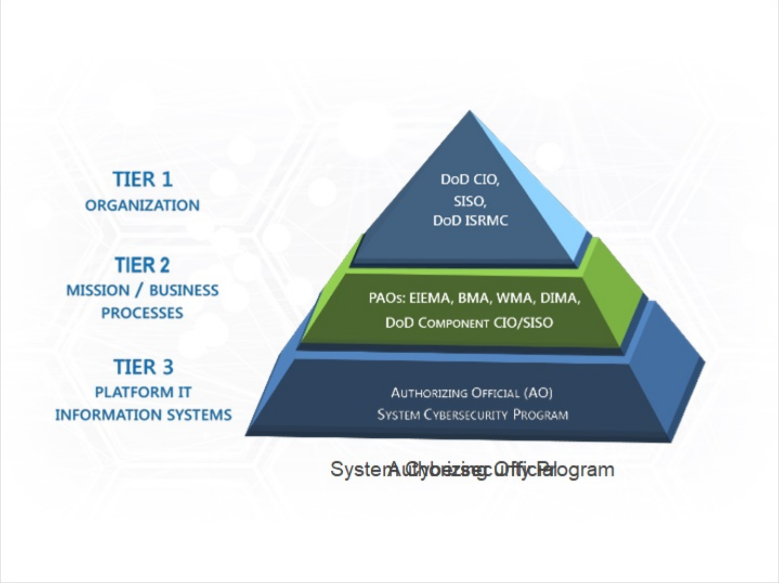
A PAO is appointed for each of the 4 DoD Mission Areas:

- The Enterprise Information Environment Mission Area
- Business Mission Area
- Warfighting Mission Area
- DoD portion of the Intelligence Mission Area

Tier 2 also contains the DoD Component Chief Information Officer (CIOs) who are responsible for administration of RMF within the DoD Component Cybersecurity Programs.

Component SISOs have authority and responsibility for security controls assessment.

Guidance Tier 3


TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
PLATFORM IT INFORMATION SYSTEMS
DoD CIO,
SISO,
DoD ISRMC
PAOs: EIEMA, BMA, WMA, DIMA,
DoD Component CIO/SISO
Authorizing Official (AO)
System Cybersecurity Program
System Cybersecurity Program
Authorizing Official

Finally, Tier 3 addresses risk management at the System Level. The key governance elements in Tier 3 include the Authorizing Official (AO). DoD Component heads are responsible for appointing trained and qualified AOs for all DoD systems within their Component. AOs should be appointed from senior leadership positions within business owner and mission owner organizations.

The system cybersecurity program consists of the policies, procedures, and activities of the Information System Owner who Appoints a User Representative for assigned systems.

The program Manager or System Manager ensures an IS Systems Engineer implements the RMF.

This tier also includes the Information Security System Manager (ISSM) - formerly known as an Information Assurance Manager and the information system Security Officer.

So let’s see if you understand organizational risk management under the Risk Management Framework.

Knowledge Check 1

What regulations will DoD follow for cybersecurity policy? Select the best answer.

A. DIACAP

B. DoD 8500 Series

C. DCID 6/3

D. DoD 6500 Series

Knowledge Check 2

What policy partnerships has DoD developed to standardize cybersecurity and protect the unique requirements of DoD missions and warfighters? Select the best answer.

A. CNSS and NIST

B. Tier 1, Tier 2, and Tier 3

C. DIACAP and RMF

D. Platform, Process, and Organization

Knowledge Check 3

What factors do organizations need to take into account when implementing a holistic approach to organizational risk management? Select all that apply.

A. Strategic Goals and Objectives

B. Relationships between mission/business process

C. Supporting Information Systems

D. Organizational culture and infrastructure

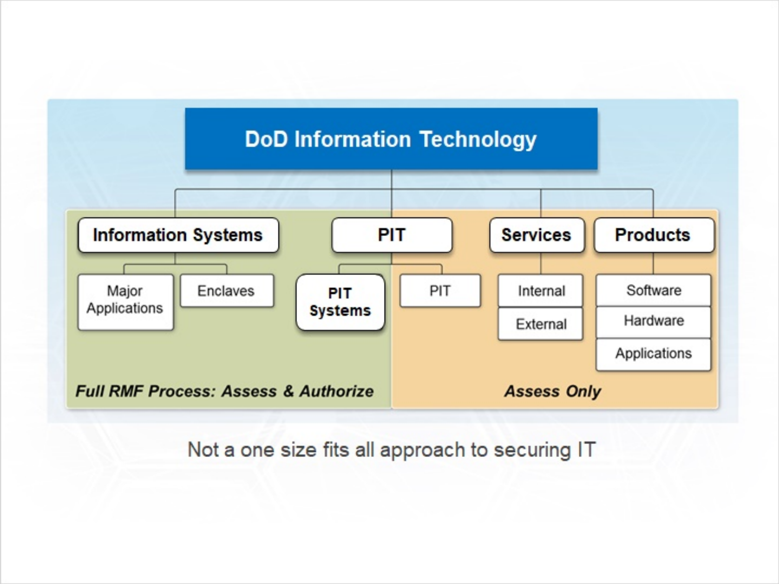
DoD Information Technology

RMF to DoD
Information Technology

Now that we have a good understanding of the policy and governance related to the Risk

Management Framework, let’s discuss the application of the RMF to DoD Information Technology.

DoD Information Technology Defined



Not a one size fits all approach to securing IT

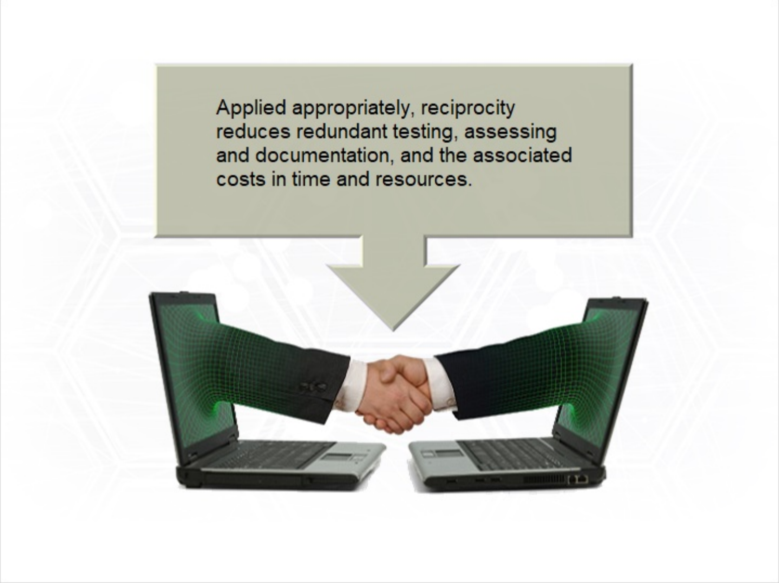
DoD Information technology refers to all DoD-owned IT or DoD-controlled IT that receives, processes, stores, displays, or transmits DoD information.

DoD information technology is broadly grouped as DoD information systems, platform information technology (PIT), PIT systems, IT services, and products. These groupings include all DoD information in electronic format; IT supporting research, development, test and evaluation; and DoD-controlled IT operated by a contractor or other entity on behalf of the DoD.

Remember, Special Access Program or SAP information technology, other than SAP information systems handling sensitive compartmented information, will be processed pursuant to the Joint SAP Implementation Guide (JSIG).

Also, please note that the risk assessment process extends to the logistics support of fielded equipment and the need to maintain the integrity of supply sources.

Reciprocity



Applied appropriately, reciprocity reduces redundant testing, assessing and documentation, and the associated costs in time and resources.

The DoD RMF presumes acceptance of existing test and assessment results and authorization documentation. See DoD Instruction 8510, Enclosure 5, for cases describing the proper application of DoD policy on reciprocity in the most frequently occurring scenarios.

One of the primary reasons for the transition to the RMF is to enable reciprocity between Federal agencies, including the DoD. It gives Federal agencies common processes, security controls, testing activities and outcomes, as well as a common lexicon among organizations. Moving to a common process will reduce costs related to the activities associated with system authorization.

Let’s review the definition of DoD Information Technology.

Knowledge Check 4

PIT systems refer to: Select the best answer.

A. Priority Information Technology

B. Proprietary Information Technology

C. Platform Information Technology

D. Process Information Technology

Knowledge Check 5

What broad groups does DoD use to categorize information technology? Choose the best answer.

A. Information Systems and PIT

B. Information Systems and Products

C. PIT and Services

D. (a) and (b)

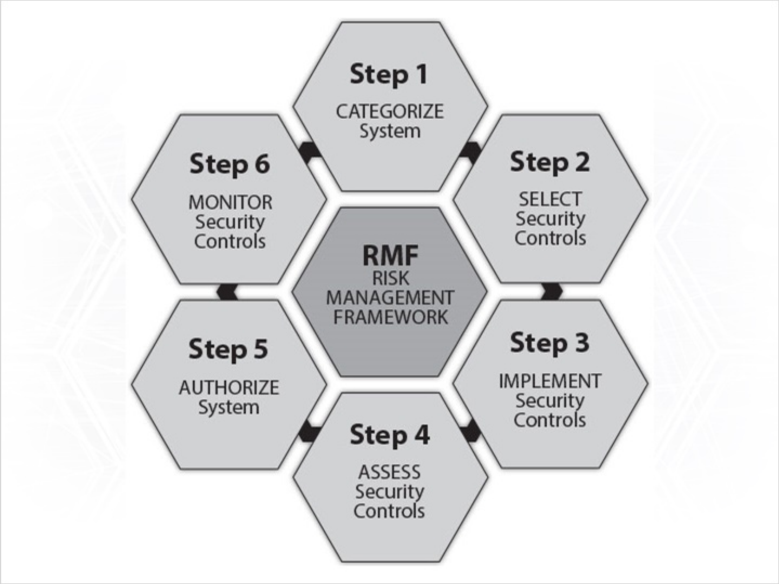
E. (b) and (c)

Implementation Guidance

Implementation Guidance

Let’s talk about RMF Implementation Guidance.

Implementation Guidance Cont'd



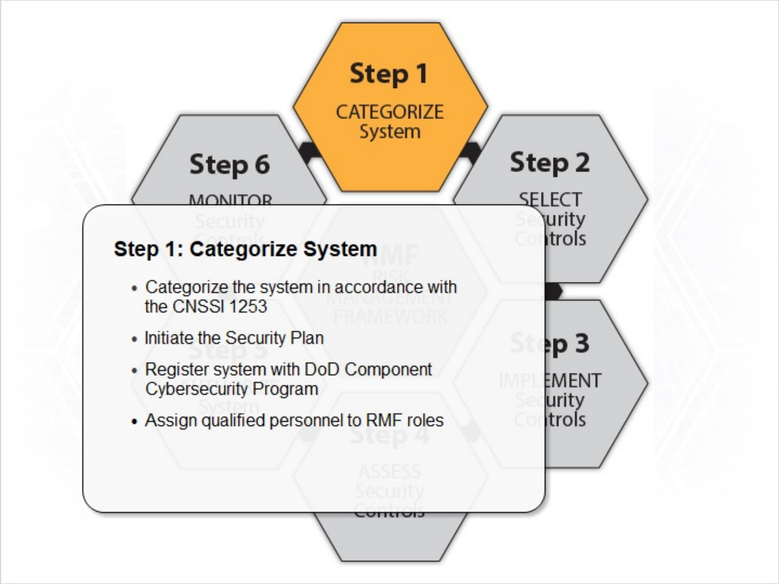
Integrating information security into organizational infrastructure requires a carefully coordinated set of activities to ensure that fundamental requirements for information security are addressed and risk to the organization from information systems is managed efficiently and cost-effectively.

In response to the need for organizations to develop an organization-wide approach for managing risk, DoD has adopted the Risk Management Framework. The Risk Management Framework methodology incorporates Federal Information System Management Act security standards and guidance to provide a holistic solution for managing risk to an organization's information and information systems.

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

Let’s discuss the steps individually.

RMF Step 1



Step 1: Categorize System

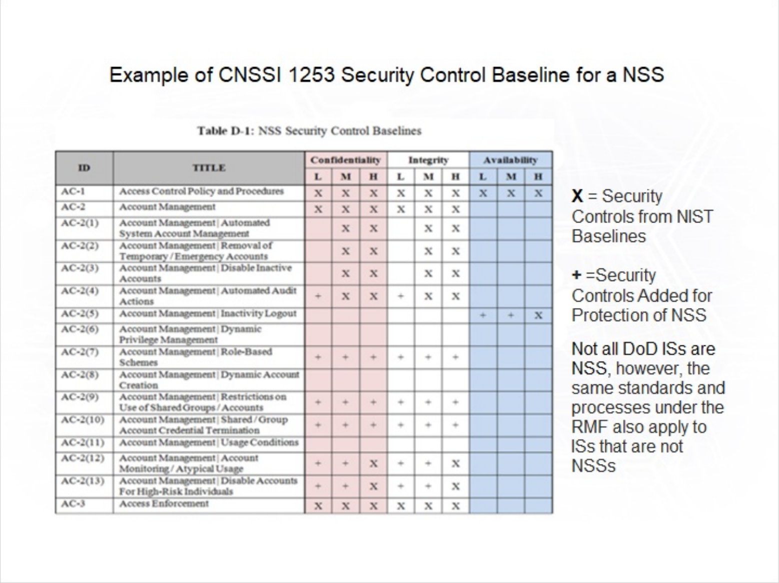
- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Categorization is the key first step in the Risk Management Framework because of its effect on all other steps in the framework, from selection of security controls to level of effort in assessing security control effectiveness.

Categorization entails a thorough analysis of the organization's mission / business processes to identify the types of information that will be processed, stored or transmitted by the information systems supporting the mission/business processes.

Categorization provides a means for selecting an initial baseline of security controls for protecting the information system and the organization.

Sample Control Baseline



Example of CNSSI 1253 Security Control Baseline for a NSS

Table D-1: NSS Security Control Baselines

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management | Automated System Account Management		X	X		X	X			
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts		X	X		X	X			
AC-2(3)	Account Management | Disable Inactive Accounts		X	X		X	X			
AC-2(4)	Account Management | Automated Audit Actions	+	X	X	+	X	X			
AC-2(5)	Account Management | Inactivity Logout							+	+	X
AC-2(6)	Account Management | Dynamic Privilege Management									
AC-2(7)	Account Management | Role-Based Schemes	+	+	+	+	+	+			
AC-2(8)	Account Management | Dynamic Account Creation									
AC-2(9)	Account Management | Restrictions on Use of Shared Groups / Accounts	+	+	+	+	+	+			
AC-2(10)	Account Management | Shared / Group Account Credential Termination	+	+	+	+	+	+			
AC-2(11)	Account Management | Usage Conditions									
AC-2(12)	Account Management | Account Monitoring / Atypical Usage	+	+	X	+	+	X			
AC-2(13)	Account Management | Disable Accounts For High-Risk Individuals	+	+	X	+	+	X			
AC-3	Access Enforcement	X	X	X	X	X	X			

X = Security Controls from NIST Baselines

+ =Security Controls Added for Protection of NSS

Not all DoD ISs are NSS, however, the same standards and processes under the RMF also apply to ISs that are not NSSs

Not all DoD Information Systems are National Security Systems or NSS; however, the same standards and process for categorizing NSS apply to non-NSS.

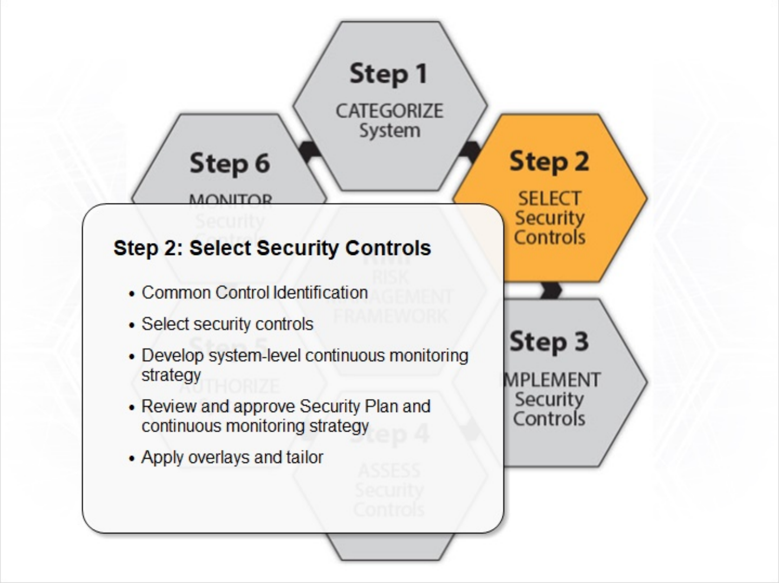
DoD 8510.01 requires all information systems and PIT systems for both NSS and non-NSS to be categorized in accordance with CNSSI 1253.

The CNSSI 1253 System Categorization process builds on and is a companion document to NIST Special Publication SP 800-53. It should be used as a tool to select and agree upon appropriate protections for an IS or PIT system.

Based upon Federal Information processing Standard Publication (FIPS 199), Categorization of systems uses the three security objectives (confidentiality, integrity, and availability) with one impact value (low, moderate, or high) for each of the security objectives. System categorization further defines and provides guidance on developing and implementing overlays.

Results of the process must be documented in the security plan, to include system description and boundaries; registration of the system in the DoD component cybersecurity program; and the assignment of qualified personnel to risk management framework roles.

RMF Step 2



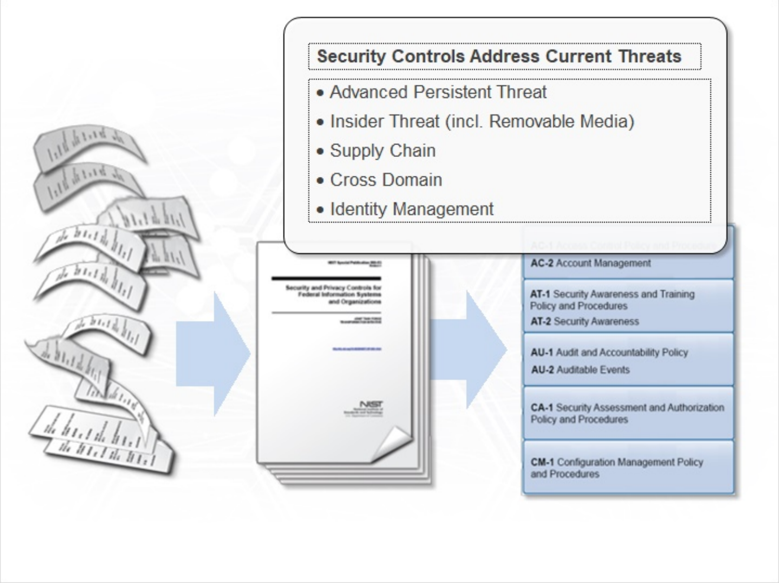
Step 2: Select Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

The purpose of Step 2, the Select Step, is to specify appropriate security controls to meet the minimum-security requirements as defined by DoD baseline configuration standards and to ensure the integrity, confidentiality, and availability of the information and information system in accordance with the organization's protection strategy.

The security control selection process includes activities designed to determine the required controls that will be implemented to reduce threats and manage risks from operating the organization's information systems.

Security Control Catalog



Security Controls Address Current Threats

- Advanced Persistent Threat
- Insider Threat (incl. Removable Media)
- Supply Chain
- Cross Domain
- Identity Management

Security and Privacy Controls for Federal Information Systems and Organizations
NIST
AC-1 Access Control Policy and Procedure
AC-2 Account Management
AT-1 Security Awareness and Training Policy and Procedures
AT-2 Security Awareness
AU-1 Audit and Accountability Policy
AU-2 Auditable Events
CA-1 Security Assessment and Authorization Policy and Procedures
CM-1 Configuration Management Policy and Procedures

During the Security Control Selection Process Common Controls, the Security Control Baseline and any applicable overlays will be selected and tailored to the IS System.

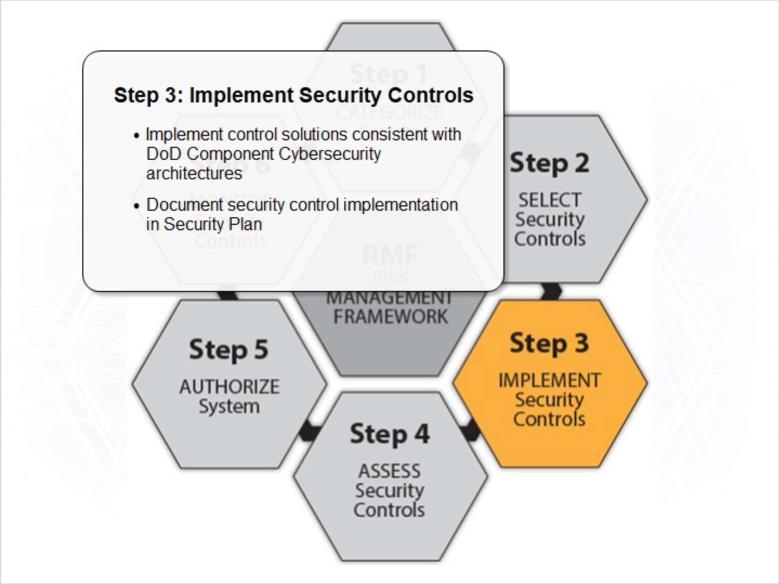
Tailoring of security controls is essential to address the diverse and specialized nature of DoD systems.

Overlays can be applied for unique characteristics such as medical, industrial control, or weapons systems.

Of the 900+ controls and enhancements in the NIST SP 800-53 Catalog, about 400 typically apply to an Information System.

Of the 400, many are “common controls” inherited from the hosting environment; this is a great use of the “build once/use many” approach and will hopefully minimize the complexity of control selection.

RMF Step 3



Step 3: Implement Security Controls

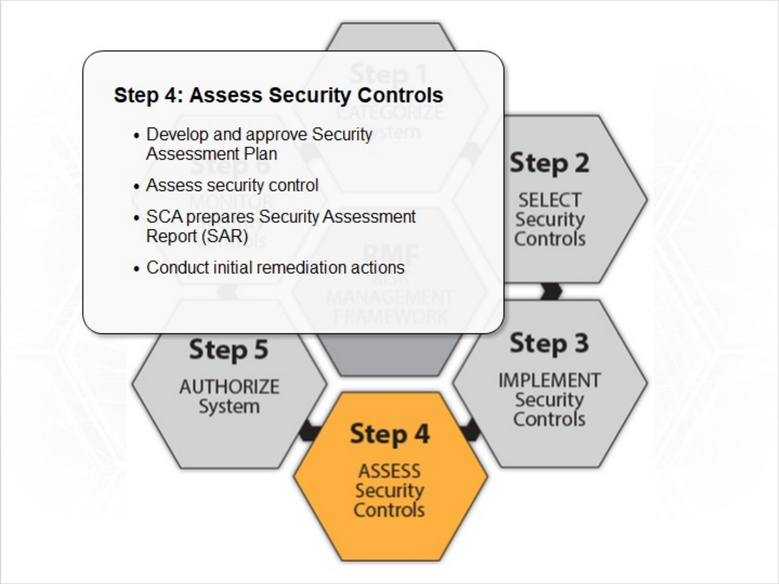
- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

In Step 3, Implementation is used in the Risk Management Framework in a broad sense to encompass all of the activities necessary to translate the security controls identified in the system security plan into an effective implementation.

Once the appropriate baseline and common security controls have been identified, and tailoring and supplemental guidance have been applied, the security controls are implemented.

Effective implementation of security controls in the system components is a critically important activity that can affect the security state and risk posture of the entire organization.

RMF Step 4



Step 4: Assess Security Controls

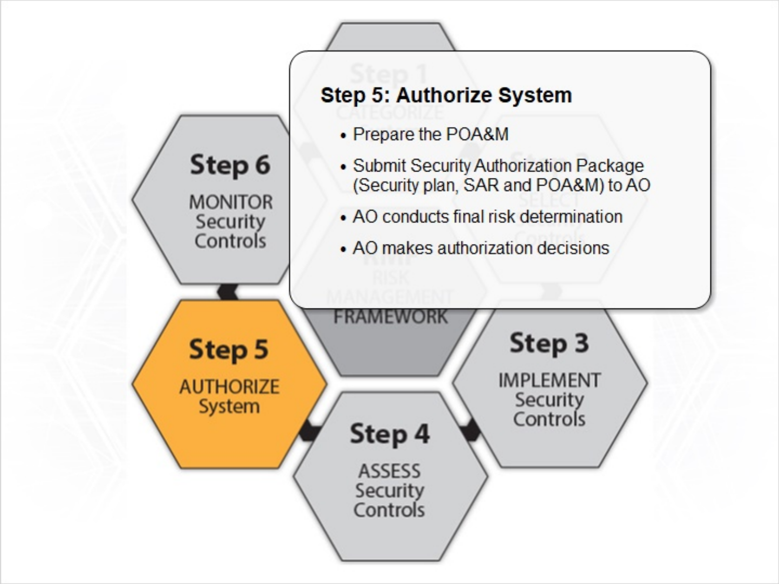
- Develop and approve Security Assessment Plan
- Assess security control
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 4 in the Risk Management Framework is Assess. Once security controls are implemented, they should be assessed for effectiveness.

Security control assessment is a process employed by an organization to review the management, and operational and technical security controls in an information system. The assessment determines the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

The Security Control Assessor (SCA) will develop, review, and approve a plan to assess the security controls. The plan will ensure assessment activities are coordinated for interoperability and identify appropriate procedures to assess those controls. The Authorizing Official approves the Security Assessment Plan.

RMF Step 5



Step 5: Authorize System

- Prepare the POA&M
- Submit Security Authorization Package (Security plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decisions

Step 5, Security authorization is the official management decision of a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

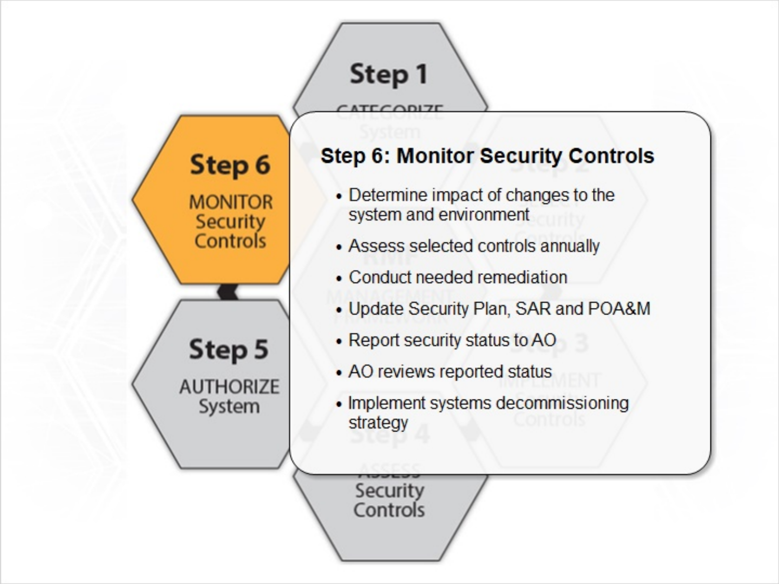
The Security Assessment Report completed in Risk Management Framework Step 4 provides authorizing officials with the information needed for understanding the current security state of the organization's information systems and supporting infrastructure and the current risk posture of the organization.

Security authorization requires managers at all levels to implement the appropriate security controls for the information system, given

- Mission or / and business requirements
- Technical constraints
- Operational constraints
- Cost/schedule constraints
- Risk-related considerations

When performing security authorization activities, the level of effort, resources expended, and actions taken should be commensurate with the security category of the information system.

RMF Step 6



Step 6: Monitor Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement systems decommissioning strategy

The final step, Step 6, is a critical aspect of the security authorization process. It is the post-authorization period involving the continuous monitoring of an information system's security controls, which includes analyzing and documenting any proposed or actual changes to the information system or its environment of operation.

Conducting a thorough point-in-time assessment of the security controls in an organizational information system is necessary, but not sufficient to demonstrate security due diligence.

Information system monitoring activities are most effective when integrated into the broader life cycle management processes carried out by the organization and not executed as stand-alone, security-centric activities.

The ultimate objective of the continuous monitoring program is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes to hardware, software, and firmware that occur in the system, as well as changes in the environment in which the system operates.

The Risk Management Framework is a six-step process that addresses the lifecycle of an information system.

Let’s take a moment to review some facts about the RMF process.

Knowledge Check 6

In what Step of the Risk Management Framework is continuous monitoring employed? Select the best answer.

A. Step 1

B. Step 4

C. Step 5

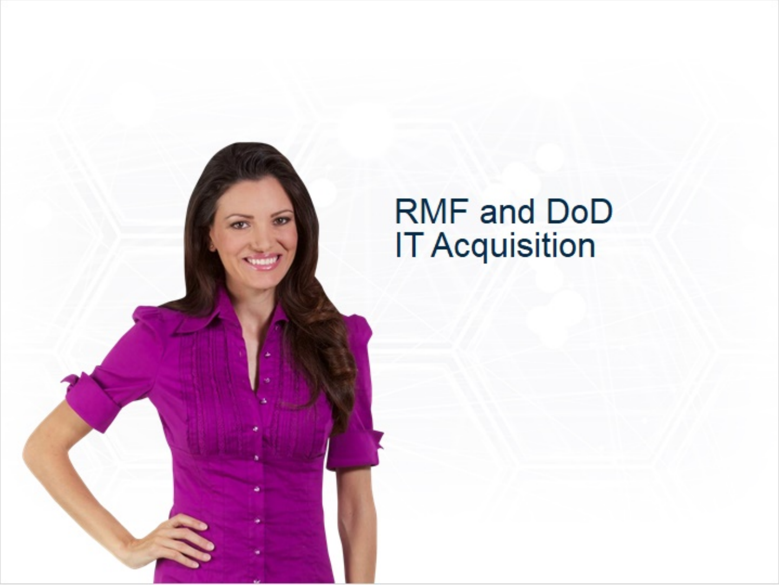
D. Step 6

Knowledge Check 7

Match the following Steps of the Risk Management Framework to associated Activities

Steps	**Activities**
Step 1 Categorize System	AO Conducts Final Risk Determination
Step 2 Select Security Controls	Determine Impact of changes to the system & environment
Step 3 Implement Security Controls	Develop & Approve Security Assessment Plan
Step 4 Assess Security Controls	Implement Control Solutions
Step 5 Authorize System	Register System with DoD
Step 6 Monitor Security Controls Activities	Common Control Identification

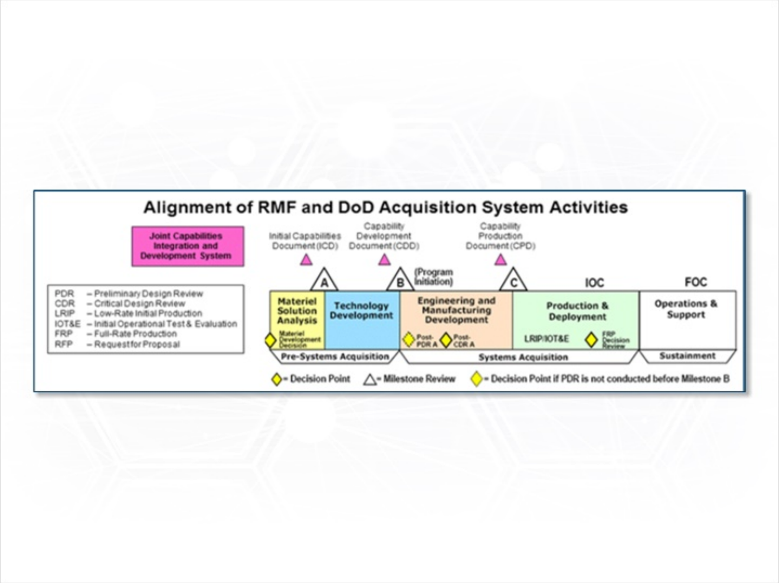
RMF and DoD IT Acquisition



RMF and DoD IT Acquisition

Now that we have an understanding of the Risk Management Framework, let's consider how it applies to the DoD IT Acquisition process.

DoD Acquisition Cycle



Alignment of RMF and DoD Acquisition System Activities

PDR – Preliminary Design Review
CDR – Critical Design Review
LRIP – Low-Rate Initial Production
IOT&E – Initial Operational Test & Evaluation
FRP – Full-Rate Production
RFP – Request for Proposal

Joint Capabilities Integration and Development System
Initial Capabilities Document (ICD)
Capability Development Document (CDD)
Capability Production Document (CPD)
A
B
(Program Initiation)
C
IOC
FOC
Materiel Solution Analysis
Materiel Development Decision
Technology Development
Engineering and Manufacturing Development
Post-PDR A
Post-CDR A
Production & Deployment
LRIP/IOT&E
FRP Decision Review
Operations & Support
Pre-Systems Acquisition
Systems Acquisition
Sustainment
◆ = Decision Point
△ = Milestone Review
◆ = Decision Point if PDR is not conducted before Milestone B

Cybersecurity risk management is a subset of the overall risk management process for all DoD acquisitions and includes cost, performance, and schedule risk for programs of record and all other acquisitions of the DoD.

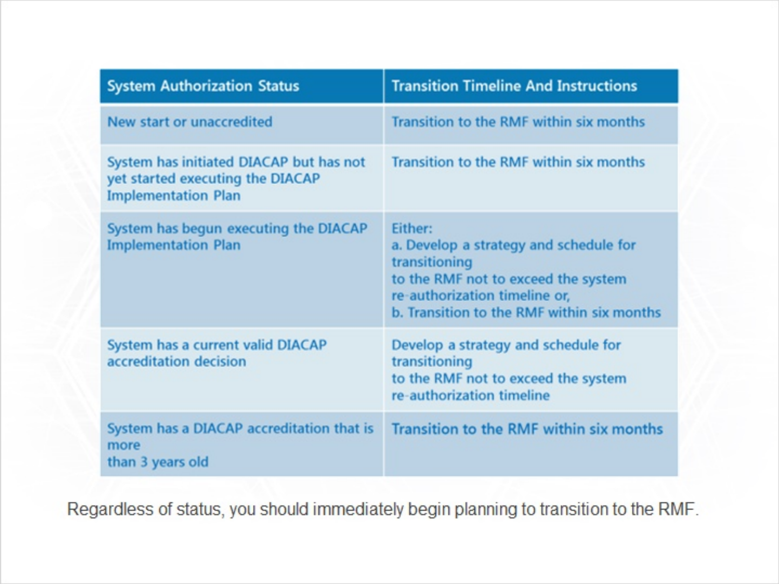
Consideration for risk in the acquisition process for DoD Information Technology is built into the risk management framework and aligned with DoD system activities.

RMF Transition Timelines

RMF Transition Timelines

So, when does your office have to transition to RMF?

Transition Timelines Cont'd



System Authorization Status	Transition Timeline And Instructions
New start or unaccredited	Transition to the RMF within six months
System has initiated DIACAP but has not yet started executing the DIACAP Implementation Plan	Transition to the RMF within six months
System has begun executing the DIACAP Implementation Plan	Either: a. Develop a strategy and schedule for transitioning to the RMF not to exceed the system re-authorization timeline or, b. Transition to the RMF within six months
System has a current valid DIACAP accreditation decision	Develop a strategy and schedule for transitioning to the RMF not to exceed the system re-authorization timeline
System has a DIACAP accreditation that is more than 3 years old	Transition to the RMF within six months

Regardless of status, you should immediately begin planning to transition to the RMF.

DoD has identified a transition timeline for DoD IT systems that is dependent upon system authorization status.

Regardless of status, you should immediately begin planning to transition to RMF.

Summary

Paul: Well, Mary I feel like I have a good grounding in the concepts for the Risk Management Framework. I truly believe it represents a critical update.

Mary: Risk management is critical to your organization’s ability to achieve its mission and goals. Because of the severity of the security threats faced by DoD organizations, use of the Risk Management Framework to implement information security safeguards for DoD information technology systems is essential.

Mary: Application of the Risk Management Framework will ensure that DoD Information Systems remain secure and that our organization is always mission ready.

Hey, why don’t you try the final quiz I created.

Conclusion

This concludes the Introduction to the Risk Management Framework course.

You should now be able to:

- Identify policies and regulations that govern the DoD Transition to RMF
- Define DoD Information Technology affected by RMF
- Understand the implementation of RMF

To receive a certificate of completion for this course, you must also take the final exam.

Answer Key Knowledge Checks:

Question 1:

What regulations will DoD follow for cybersecurity policy? Select the best answer.

A. DIACAP

B. DoD 8500 Series

C. DCID 6/3

D. DoD 6500 Series

Answer Expansion: DoD will continue to follow the DoD 8500 series documentation For Cybersecurity policy (formerly Information Assurance)

Question 2:

What policy partnerships has DoD developed to standardize cybersecurity and protect the unique requirements of DoD missions and warfighters? Select the best answer.

A. CNSS and NIST

B. Tier 1, Tier 2, and Tier 3

C. DIACAP and RMF

D. Platform, Process, and Organization

Answer Expansion: DoD participates in Committee on National Security Systems and NIST policy development as a vested stakeholder with the goals of a more standardized approach to cybersecurity and to protect the unique requirements of DoD missions and warfighters.

Question 3:

What factors do organizations need to take into account when implementing a holistic approach to organizational risk management? Select all that apply.

A. Strategic Goals and Objectives

B. Relationships between mission/business process

C. Supporting Information Systems

D. Organizational culture and infrastructure

Answer Expansion: A holistic approach to organizational risk management considers all of these factors - Strategic goals and objectives, Relationships between mission/business processes and their supporting information systems, and Organizational culture and infrastructure.

Question 4:

PIT systems refer to: Select the best answer.

A. Priority Information Technology

B. Proprietary Information Technology

C. Platform Information Technology

D. Process Information Technology

Answer Expansion: Platform Information Technology (PIT) is a category of DoD information technology. DoD information technology refers to all DoD-owned IT or DoD-controlled IT that receives, process, store, displays, or transmits DoD information

Question 5:

What broad groups does DoD use to categorize information technology? Choose the best answer.

A. Information Systems and PIT

B. Information Systems and Products

C. PIT and Services

D. (a) and (b)

E. (b) and (c)

Answer Expansion: DoD information technology is broadly grouped as DoD information systems, platform information technology or PIT, PIT systems, IT services, and products

Question 6:

In what Step of the Risk Management Framework is continuous monitoring employed? Select the best answer.

A. Step 1

B. Step 4

C. Step 5

D. Step 6

Answer Expansion: Step 6 “Monitor Security Controls” implements the continuous monitoring process. Continuous monitoring provides on-going, up-to-date information about the organization's security state and risk posture. It also enables the organization to make credible, risk-based decisions regarding the continued operation of the organization's information systems. Finally, continuous monitoring provides organizations with an effective tool for producing ongoing updates to system security documentation.

Question 7:

Match the following Steps of the Risk Management Framework to associated Activities

Steps	**Activities**
Step 1 Categorize System	**Register System with DoD**
Step 2 Select Security Controls	**Common Control Identification**
Step 3 Implement Security Controls	**Implement Control Solutions**
Step 4 Assess Security Controls	**Develop & Approve Security Assessment Plan**
Step 5 Authorize System	**AO Conducts Final Risk Determination**
Step 6 Monitor Security Controls Activities	**Determine Impact of changes to the system & environment**