

Module 13 - Critical Requirements: Safety, Security, and Privacy

TOC

TOC

Introduction

Cybersecurity has become one of our nation's most critical and pressing issues. Attacks and the threat of attacks to our critical infrastructure and DoD systems must be dealt with on a continual basis.

Since cyber attacks threaten the DoD, all areas of the federal government, the commercial and private sector, and every individual, the need is great for a unified plan of defense.

Acknowledging the need for an overarching cybersecurity plan, the Risk Management Framework (RMF) for DoD Information Technology (IT) (DoD Instruction 8510.01) was finalized in March of 2014. This new instruction seeks to change the effectiveness of the DoD's cyber defenses and the underlying culture.



TOC

Lesson Objectives

This lesson presents an overview of cybersecurity and the Risk Management Framework.

After completing this lesson, you will be able to:

- Define cybersecurity and key cybersecurity activities.
- Identify the overarching principles of the Risk Management Framework (RMF) for DoD Information Technology (IT).
- Define a Continuity of Operations Plan (COOP).
- Identify elements of a operations plan.



Objectives

Cybersecurity Defined

[TOC](#)

DoDI 8500.01 (Cybersecurity) adopted the term "cybersecurity" to be used throughout DoD instead of the term "information assurance (IA)." Cybersecurity, is defined as:

"Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

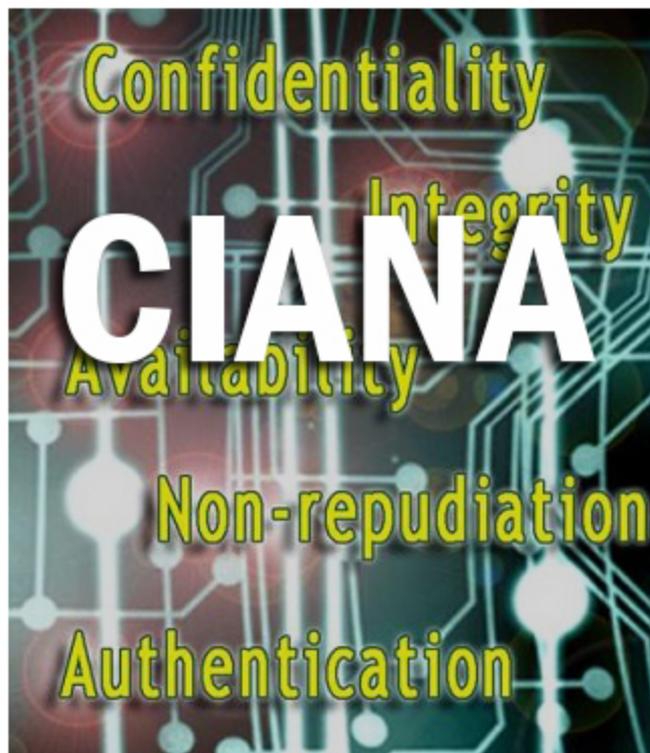
While the definition of cybersecurity is very similar to the previous definition of IA, it acknowledges the increasing need for prevention and a proactive approach to cybersecurity (i.e., intrusion prevention and software supply chain risk management), along with protecting communication and communication systems (i.e. cloud computing and smart phones).



Important Aspects of Cybersecurity

To fully understand cybersecurity, it is important to define the five key terms that are associated with it. These terms can be found below:

- Confidentiality - Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.
- Integrity - The property whereby an entity has not been modified in an unauthorized manner
- Availability - Being accessible and useable upon demand by an authorized entity.
- Non-repudiation - Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
- Authentication - Verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data



Types of Threats

[TOC](#)

Threats to our communication systems can take the form of active or passive threats.

Select each tab to learn more about these threats.

Active Threats**Passive Threats**

[Active threats](#) to our communication systems and networks can attack the integrity of the data that resides on them by modification or adding counterfeit data to our information.

Additionally, adversaries can seek to disrupt our system and keep us from communicating critical information at crucial times.



TOC

Defense in Depth

There is no single mechanism that will fully protect your system. Therefore, multiple levels of protection must be deployed. The concept of layering defense mechanisms to protect against the myriad of attacks and attack vectors that we face is known as [Defense in Depth](#).

This concept has been around for thousands of years as it applies to critical assets such as national or tribal leaders and the domains or castles in which they presided.

When applied to our communication systems, it may consist of anti-virus software, intrusion protection and prevention solutions, firewalls, passwords, common access cards, virtual and physical access control, and countless other protection mechanisms.



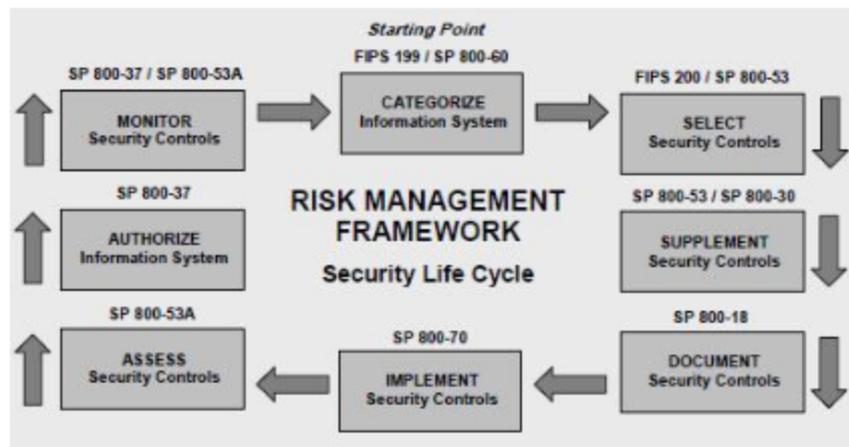
The Risk Management Framework for DoD IT

DoDI 8510.01 (The RMF for DoD IT) was signed into law on March 12 of 2014. This new policy replaced the DoD Information Assurance Certification and Accreditation Process (DIACAP) and it applies to all DoD IT that receive, process, store, display, or transmit DoD information.

This new policy is more consistent with established disciplines and best practices for effective systems engineering, systems security engineering, and program protection planning outlined in DoDI 5000.02 and the Defense Acquisition Guidebook.

The RMF also leverages and builds upon several existing Federal policies and standards. Many of these policies were written by the National Institute of Standards (NIST) and the Committee on National Security Systems (CNSS). DoD participates in CNSS and NIST policy development as a vested stakeholder with the goals of a more synchronized cybersecurity landscape and to protect the unique requirements of DoD Missions and warfighters.

Select the image for an enlarged view.



RMF Principles

The RMF includes several focus areas that have been deemed critical to the establishment of an effective cybersecurity risk management program.

Select each focus area to learn more.

Operation Resilience

Multi-tiered Risk Management

Cybersecurity Reciprocity

Integration and Interoperability

Continuous Monitoring



Cybersecurity Risk Management

TOC

RMF Key Documents

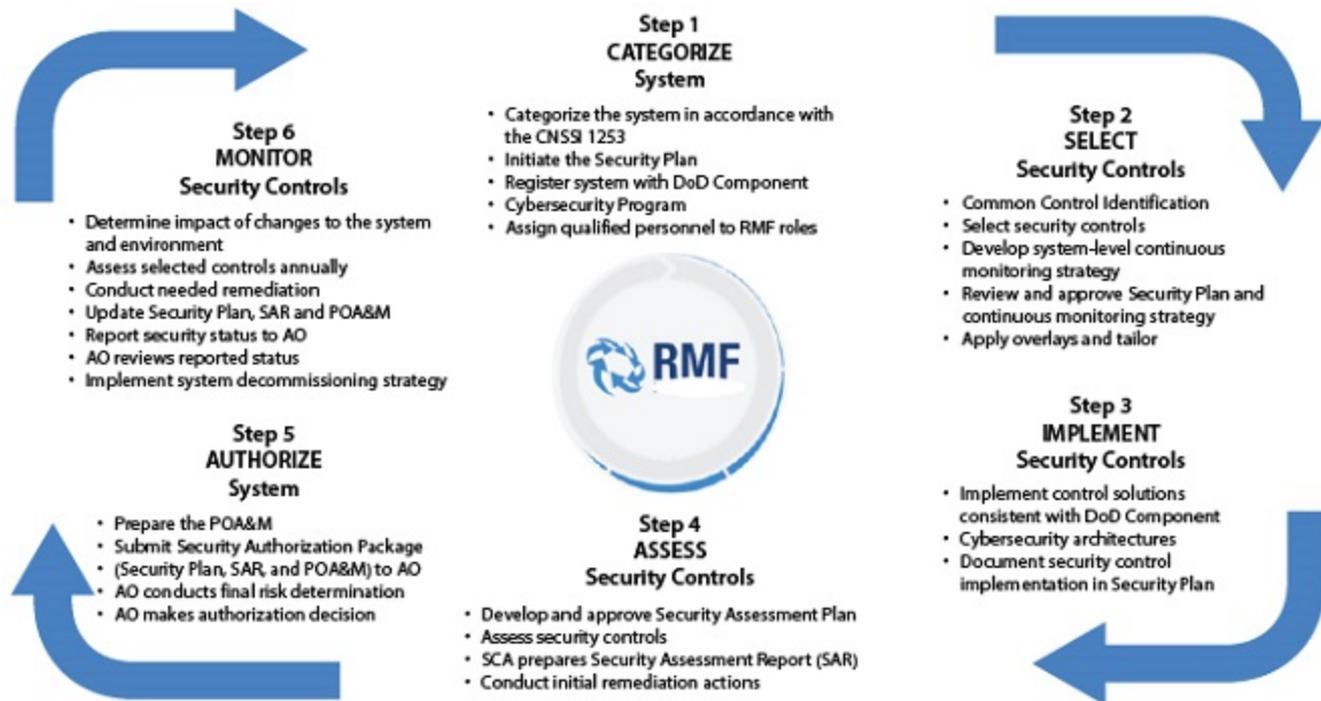
Several documents and publication were used to craft the new Cybersecurity and RMF policies. The table below list a few.

NIST Special Publications (SP)	Committee on National Security Systems (CNSS)
800-37 - Guide for Applying the RMF	Instruction 1253 - Security Categorization and Control Selection for National Security Systems
800-39 - Managing Information Security Risks	Instruction 4009 - Information Assurance Glossary
800-53 - Security and Privacy Controls	Policy 11 - National Policy Governing the Acquisition of IA and IA-Enabled IT Products
800-53A - Guide for Assessing the Security Controls	
800-60 - Guide for Mapping Types of Information and Information Systems to Security Categories	
800-137 - Information Security Continuous Monitoring	

RMF Six Step Process

The RMF process consists of six steps including Categorize the System, Select Security Controls, Implement Security Controls, Assess Security Controls, Authorize the System and Monitor Security Controls.

Select each step to learn more.



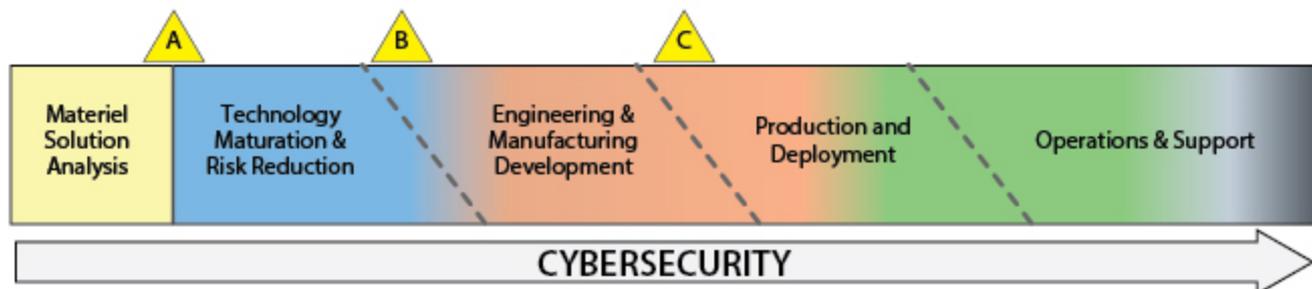
RMF and Authorizations

After going through the RMF process, a system must obtain an authorization before it can be fielded. A system may obtain an Authorization to Operate (ATO), an ATO with conditions, an Interim Authorization to Test (IATT), or a Denial of ATO (DATO). The table describes the decision criteria and authorization period.

Authorization Type	Decision Criteria	Authorization Period
Authorization to Operate (ATO)	Overall risk is determined to be acceptable, and there are no NC controls with a level of risk of "Very High" or "High".	Must specify an Authorization Termination Date (ATD) that is within 3 years of the authorization date unless the IS or PIT system has a system-level, DoD policy compliant, continuous monitoring program.
ATO with conditions (Only with permission of the DoD Component Chief Information Officer (CIO))	NC controls with "Very High" or "High" risk that can't be corrected or mitigated immediately, but overall system risk is determined to be acceptable due to mission criticality	Should specify an AO review period that is within 6 months of the authorization date. If the system still requires operation with a level of risk of "Very High" or "High" after 1 year, the DoD Component CIO must again grant permission for continued operation of the system.
Interim Authority To Test (IATT)	Risk determination is being made to permit testing of the system in an operational information environment or with live data, and the risk is acceptable	Should expire at the completion of testing (normally for a period of less than 90 days)
Denial of Authorization to Operate (DATO)	Risk is determined to be unacceptable	Immediate or in concert with a system decommissioning strategy

RMF and the Acquisition Lifecycle

Cybersecurity requirements must be identified and included throughout the lifecycle of systems to include acquisition, design, development, developmental testing, operational testing, integration, implementation, operation, upgrade, or replacement of all DoD IT supporting DoD tasks and missions.



Cybersecurity must be fully integrated into system life cycles so that it will be a visible element of organizational, joint, and DoD Component architectures, capability identification and development processes, integrated testing, information technology portfolios, acquisition, operational readiness assessments, supply chain risk management, SSE, and operations and maintenance activities.

RMF Roles and Responsibilities

Roles and responsibilities have changed with the revised 8510.01 RMF. The table lists the old and new roles of the key players in the RMF process and their responsibilities.

DIACAP role DoDI 8510.01 2007	RMF role DoDI 8510.01 2014	Responsibilities (Reference DoDI 8510.01 for a complete definition of roles and responsibilities)
Designated Accrediting Authority (DAA)	Authorizing Official (AO)	AO ensures all appropriate RMF tasks are initiated and completed, with appropriate documentation, for assigned ISs and PIT systems; monitors and tracks overall execution of system-level POA&Ms and promotes reciprocity.
Certifying Authority	Security Control Assessor (SCA)	SCA is the senior official with authority and responsibility to conduct security control assessments.
No explicit role	Information System Owner (ISO)	In coordination with the information owner (IO), the ISO categorizes systems and documents the categorization in the appropriate JCIDS document (e.g., CDD and Security Plan for systems).
Information Assurance Manager (IAM)	Information System Security Manager (ISSM)	ISSM maintains and reports IS and PIT system assessments and authorization status and issues, provides ISSO direction, and coordinates with the security manager to ensure issues affecting the organization's overall security are addressed appropriately.
Information Assurance Officer	Information System Security Officer (ISSO)	ISSO is responsible for maintaining the appropriate operational security posture for an information system or program.

RMF Knowledge Service and eMASS

The [Risk Management Framework \(RMF\) Knowledge Service](#) (KS) is DoD's official site for enterprise RMF policy and implementation guidelines. The RMF Knowledge Service provides Cybersecurity practitioners and managers with a single authorized source for execution and implementation guidance, community forums, and the latest information and developments in the RMF.

The [Enterprise Mission Assurance Support Service \(EMASS\)](#), is a government owned web based application, which provides visibility and automation for Cyber Security Management processes.



eMASS



ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE

RMF Transition

DoDI 8510.01 lays out a transition plan for systems either transitioning from DIACAP to the RMF or going through a new authorization. While RMF readiness and buy-in between DoD components has varied, it should be noted that systems accredited under DIACAP should not exist after September of 2017.

System Authorization Status		Transition Timeline And Instructions
1	New start or unaccredited	Transition to the RMF within six months
2	System has initiated DIACAP but has not yet started executing the DIACAP Implementation Plan	Transition to the RMF within six months
3	System has begun executing the DIACAP Implementation Plan	Either: a. Continue under DIACAP. 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
4	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
5	System has a DIACAP accreditation that is more than 3 years old	Transition to the RMF within six months

TOC

Knowledge Review

All of the following are BENEFITS of the Risk Management Framework (RMF) **EXCEPT** for?

- Cybersecurity Authority to Operate (ATO) Reciprocity between agencies
- Continuous Monitoring
- Single Level Risk Management vice Multi-tiered
- Operation Resilience allowing authorized services and data to be available wherever and whenever needed

[Check Answer](#)

Continuity of Operations (COOP) Plan

TOC

Continuity of Operations (COOP) is defined as an internal effort within individual DoD Components to ensure uninterrupted, essential DoD Component functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological and/or attack related emergencies.



Continuity Planning Policy

TOC

It is DoD policy ([DoDD 3020.26](#), January 9, 2009) that: All Defense continuity-related activities, programs, and requirements of the DoD Components, including those related to COOP, COG, and [Enduring Constitutional Government \(ECG\)](#), shall ensure the continuation of current approved DoD and DoD [Component Mission Essential Functions \(MEFs\)](#) under all circumstances across the spectrum of threats.

Continuity Of Government (COG). A coordinated effort within each branch of Government ensuring the capability to continue branch-minimum essential responsibilities in a catastrophic crisis. COG is dependent on effective continuity of operations plans and capabilities.



Department of Defense DIRECTIVE

NUMBER 3020.26
January 9, 2009

USD(P)

SUBJECT: Department of Defense Continuity Program

- References: (a) DoD Directive 3020.26, "Defense Continuity Program (DCP)," September 8, 2004 (hereby canceled)
 (b) DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998
 (c) National Security Presidential Directive-51/Homeland Security Presidential Directive-20, "National Continuity Policy," May 9, 2007
 (d) "National Continuity Policy Implementation Plan," August 2007
 (e) Section 2674 of title 10, United States Code
 (f) National Communications System Directive 3-10, "Telecommunications Operations," July 25, 2007

1. **PURPOSE.** This Directive:

- Revises Reference (a) and changes its title.
- Revises continuity policies and assigns responsibilities for developing and maintaining Defense Continuity Programs to enhance the DoD readiness posture.

2. **APPLICABILITY.** This Directive applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Component").

3. **DEFINITIONS.** These terms and their definitions are for the purpose of this Directive.

- continuity of government (COG).** A coordinated effort within each branch of Government ensuring the capability to continue branch-minimum essential responsibilities in a catastrophic crisis. COG is dependent on effective continuity of operations plans and capabilities.

COOP Planning

[TOC](#)

Continuity planning is conducted in order to be prepared for events such as disaster recovery, providing back-up sites, and/or incident response.

Continuity planning normally applies to the mission/business itself; it concerns the ability to continue critical functions and processes during and after an emergency event.

Contingency planning also normally applies to information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency.

Each service has COOP templates, but the general template content is consistent across the DoD.



Elements of a COOP

All DoD continuity planning and programming shall consist of the following elements in their COOP plan:

1. Be based on the assumption that no warning of attack or event will be received.
2. Ensure the performance of MEFs during any emergency for a period of up to 30 days or until normal operations can be resumed. The capability to perform MEFs at alternate sites must be fully operational as soon as possible, but no later than 12 hours after COOP activation.
3. Be based on risk-management assessments to ensure that appropriate operational readiness decisions consider the probability of an attack or incident and its consequences.
4. Emphasize the permanent and routine geographic distribution of leadership, staff, and infrastructure in order to increase survivability and maintain uninterrupted capability to accomplish DoD MEFs.
5. Maximize the use of technological solutions to provide information to leaders and other users, facilitate decision making, maintain situational awareness, and issue orders and direction. Technology, information systems and networks must be interoperable, robust, reliable, and resilient.
6. Integrate critical infrastructure protection, information assurance, operations security, and defense crisis management requirements, as appropriate.
7. Continuity requirements shall be incorporated into the daily and routine operations of all DoD Components.

TOC

Knowledge Review

Which of the following is **NOT** an element of COOP?

- Continuity requirements shall be incorporated into the daily and routine operations of all DoD Components.
- Leverages the operational expertise of the Combatant Commands and the respective Senior Warfighter Forums (SWarFs) or other forums as appropriate to identify issues, priorities, and capability and resource mismatches (gaps, shortfalls, and redundancies).
- Maximize the use of technological solutions to provide information to leaders and other users, facilitate decision making, maintain situational awareness, and issue orders and direction.
- Be based on risk-management assessments that consider the probability of an attack or incident and its consequences.

[Check Answer](#)

TOC

Summary

Cybersecurity threats to DoD systems as well as to critical assets are among the greatest threats that the DoD faces.

Attacks on confidentiality, integrity, and availability must be confronted on a daily basis. Additionally, DoD networks must provide for the non-repudiation (proof of delivery and the sender's identity) and authentication (verifying the source and integrity of data) of the information that is communicated over the network.

In order to protect against these threats, whether they are active or passive, it is still imperative that the DoD employ a multi-layered or Defense in Depth approach.



Summary

Lesson Completion

[TOC](#)

You have completed the content for this lesson.

To continue, select another lesson from the Table of Contents on the left.

If you have closed or hidden the Table of Contents, click the Show TOC button at the top in the Atlas navigation bar.