DoD Instruction 8510.01

Risk Management Framework for DoD Systems

Originating Component:	Office of the DoD Chief Information Officer
Effective:	July 19, 2022
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended
Incorporates and Cancels:	Directive-type Memorandum 20-004, "Enabling Cyberspace Accountability of DoD Components and Information Systems," November 13, 2020, as amended
Approved by:	John B. Sherman, DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, this issuance:

- Establishes the cybersecurity Risk Management Framework (RMF) for DoD Systems (referred to in this issuance as "the RMF") and establishes policy, assigns responsibilities, and prescribes procedures for executing and maintaining the RMF.
- Establishes and applies an integrated enterprise-wide decision structure for the RMF that includes and integrates DoD mission areas (MAs) pursuant to DoDD 8115.01 and the governance process prescribed in this issuance.
- Provides guidance on reciprocity of system authorization decisions for the DoD in coordination with other Federal agencies.
- Authorizes and designates the RMF Technical Advisory Group (TAG) as the body responsible for developing and publishing RMF implementation guidance.

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

1.2. POLICY.

a. The RMF process will inform acquisition processes for all DoD systems, including requirements development, procurement, developmental test and evaluation (DT&E), operational test and evaluation (OT&E), and sustainment; but will not replace these processes.

b. In accordance with Executive Order 13800, the National Institute of Standards and Technology (NIST) publications will be the authoritative guidelines for the DoD RMF.

c. DoD RMF must meet the requirements of Subchapter II of Chapter 35 of Title 44, United States Code, also known as and referred to in this issuance as the "Federal Information Security Modernization Act of 2014" (FISMA) and Section 11331 of Title 40, United States Code.

d. Cybersecurity requirements and cyberspace operational risk management functions will be established and applied to all programs, systems, and technologies in DoD, regardless of the acquisition or procurement method (referred to collectively in this issuance as "systems").

e. Accountability for cybersecurity risk accepted within DoD must be enforced at all levels within the OSD or DoD Component in question (e.g., executive program officers, program managers (PMs), authorizing officials (AOs), and cyberspace and functional operational commanders) and throughout the lifecycle of its systems in accordance with DoDD 3020.04, DoD Instructions (DoDIs) 8500.01, 8010.01, and 3020.45, and this issuance.

f. The DoD Information Enterprise will use cybersecurity reciprocity to reduce redundant testing, assessing, documenting, and the associated costs in time and resources.

g. The RMF system authorization information will be shared to support system to system connections across authorization boundaries and decisions for shared services within DoD, and in coordination with other Federal agencies, as appropriate.

h. The DoD Chief Information Security Officer (CISO) will charter the RMF TAG to interface with DoD Components on emerging RMF issues affecting the DoD Information Network.

i. The RMF Knowledge Service (KS) (found at https://rmfks.osd.mil) will be the authoritative source for RMF implementation guidance, standards, and tools, as governed by the RMF TAG.

j. DoD personnel making decisions affecting cybersecurity or cyber operational risk will be accountable, as appropriate, for those decisions.

SECTION 2: RESPONSIBILITIES

2.1. DOD CISO.

Under the authority, direction, and control of the DoD Chief Information Officer (CIO), the DoD CISO:

a. Develops, implements, and oversees the Cybersecurity Program for DoD.

b. Oversees implementation of this issuance and the cybersecurity risk management of DoD systems, distributes RMF standards, and supports Joint Capabilities Area (JCA) owners in developing the required RMF guidance for their respective portfolios.

c. Establishes the construct and program for AOs, including qualification and training requirements, and ensures acquisition programs and DoD systems have AOs appointed consistent with that construct. The construct must ensure the AOs, with the assistance of PMs or system owners (SOs), will:

(1) Oversee cybersecurity activities, findings, and remediation actions from developmental, operational, and cybersecurity testing or assessment activities throughout the system lifecycle.

(2) Ensure data from those activities are captured in security authorization packages to inform risk-based authorization decisions.

d. Coordinates with the Under Secretary of Defense for Research and Engineering (USD(R&E)) and the Director, Operational Test and Evaluation (DOT&E) to ensure cybersecurity DT&E and OT&E policies, procedures, and guidance integrate with the RMF policies and procedures. Additional testing, such as user or functionality testing, is in accordance with DoDI 5000.89.

e. Assists other organizations in executing the RMF by providing subject matter expertise in coordination with the Chairman of the Joint Chiefs of Staff.

f. Incorporates United States Cyber Command (USCYBERCOM) and National Security Agency/Central Security Service cyber operational risk tolerances into security authorization baselines, as applicable.

2.2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA).

Under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in Paragraph 2.7., the Director, DISA:

a. Oversees DISA control correlation identifiers, security requirements guides, and security technical implementation guides to maintain consistency with the Committee on National

Security Systems Instruction (CNSSI) 1253; NIST Special Publication (SP) 800-53 security and privacy controls; and NIST SP 800-53A assessment procedures.

b. Develops and provides:

(1) RMF training and awareness products.

(2) A distributed training capability to support the DoD Components in accordance with DoDD 8140.01.

(3) Training materials posted on the DoD Cyber Exchange at https://cyber.mil.

c. Identifies or develops and distributes DoD enterprise RMF management tools.

2.3. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT.

In addition to the responsibilities in Paragraph 2.7., the Under Secretary of Defense for Acquisition and Sustainment:

a. Coordinates with the DoD CISO to integrate RMF policies, processes, and procedures with Defense Acquisition System processes for acquisitions of DoD systems.

b. Verifies DoD Component acquisition program executive offices and PMs are accountable for coordinating tradeoff decisions during sustainment of systems (i.e., decisions to withhold or delay vulnerability remediation, which significantly impact survivability of systems under conditions of the intended operational environment) with the requirements sponsors, AO, and Component cyberspace operations forces.

2.4. USD(R&E).

In addition to the responsibilities in Paragraph 2.7., the USD(R&E):

a. Coordinates with the DoD CISO and Director, National Security Service/Chief, Central Security Service for consistent integration between:

(1) The RMF policies and procedures.

(2) Systems Engineering.

(3) Developmental test, evaluation, and assessment policies and procedures.

(4) Guidance for acquisition of DoD digital capabilities, including national security systems in coordination with the Director, National Security Service/Chief, Central Security Service.

b. Provides the RMF TAG with input as appropriate or required.

2.5. DOT&E.

In addition to the responsibilities in Paragraph 2.7., the DOT&E:

a. Reviews the plans, execution, and results of operational testing to adequately evaluate cybersecurity for all DoD information technology acquisitions subject to oversight.

b. In coordination with the DoD CISO, ensures OT&E findings are integrated into the RMF and provides the RMF TAG with input as appropriate or required.

2.6. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE.

Under the authority, direction, and control of the Under Secretary of Defense for Intelligence and Security and the DoD CIO, as applicable in accordance with Section 142(b)(1)(D) of Title 10, United States Code, in addition to the responsibilities in Paragraph 2.7., and in coordination with the DoD CISO, the Director, National Security Agency/Chief, Central Security Service:

a. Recommends solutions to mitigate vulnerabilities in current operational weapons and space systems.

b. Recommends solutions to harden the security design of future systems.

c. Assesses the overall security posture of National Security Systems, identifies their vulnerabilities, and disseminates information regarding threats to DoD.

d. In coordination with the cognizant AO, assesses cybersecurity requirements and information system security architectures of applicable National Security Systems before program initiation for new systems and all acquisition milestones.

e. Provides verified system security engineering services to support the RMF when provided to DoD Components.

f. Delivers threat and risk reports to support authorization decisions.

2.7. OSD AND DOD COMPONENT HEADS.

OSD and DoD Component heads:

a. Integrate Component cybersecurity throughout system engineering and testing processes that contribute to cyber resilience, survivability, materiel readiness, and cyberspace operational readiness.

b. Manage Component cybersecurity risks to respective systems in accordance with the principles and processes contained in this issuance.

c. Establish and maintain cybersecurity governance bodies and methods to monitor and manage system cybersecurity risks and integrate their Component governance processes with the DoD enterprise governance processes in this issuance.

d. Develop and maintain Component level guidance required by the "Prepare" step of the RMF and verify that all subcomponents build and maintain the necessary guidance for their business or mission function.

e. Categorize systems and select controls in accordance with CNSSI 1253 and implement a corresponding set of security controls in accordance with NIST SP 800-53.

f. Require use of the DoD-specific assignment values, overlays, implementation guidance, and assessment procedures found on the RMF KS.

g. Identify and allocate resources for the RMF in the DoD Planning, Programming, Budgeting, and Execution process.

h. Implement continuous monitoring activities in accordance with Office of Management and Budget Memorandum M-14-03, NIST SP 800-137, NIST SP 800-137A, and DoDIs 8530.01 and 8531.01.

i. Develop and maintain a plan of action and milestones (POA&M) to address known vulnerabilities in the system, subsystems, and system components in accordance with DoDI 8531.01.

j. Adhere to a Component cybersecurity program in accordance with DoDI 8500.01.

k. Conduct RMF activities in all phases of the DoD acquisition process (i.e., requirements development, procurement, DT&E, OT&E, and sustainment) to increase security and decrease cost.

l. Verify the appointment of a PM or SO for all Component systems.

m. Appoint an AO for every system operating within or on behalf of the Component in accordance with DoDI 8500.01 and Appendix D, Paragraph D.6 of NIST SP 800-39 and authorize systems in accordance with this issuance. The AOs must:

(1) Only be government personnel. This role cannot be re-delegated to personnel who do not meet this requirement.

(2) Possess relevant expertise with the leveraged technology as part of the system, and this must be a factor in their selection and appointment as an official responsible for authorizing systems.

(3) Manage and reduce cybersecurity risk and complete duties, which are evaluated in annual performance evaluation criteria.

(4) Complete AO training or an RMF training course offered by NIST.

n. Develop and issue systems guidance that reflects Component-unique operational and environmental demands as needed.

o. Verify that Component processes regarding the RMF, cybersecurity, systems engineering, and testing are integrated and actively share system-related data across these processes as contributors to cyber resilience, survivability, materiel readiness, and cyberspace operational readiness.

p. Direct PMs and information SOs to maintain DoD systems under their authority to comply with the RMF.

q. Operate only authorized DoD systems with a current authorization to operate (ATO), and maintain authorized DoD systems are maintained under their authority to comply with RMF.

r. Manage, maintain, and mitigate risks throughout the system lifecycle in accordance with cybersecurity operational requirements.

s. Oversee and verify that personnel engaged in, or supporting, the RMF are appropriately trained and possess professional certifications in accordance with DoDD 8140.01 and supporting issuances.

t. Ensure Component information SOs appoint user representatives (URs) for DoD systems under their purview.

u. Coordinate Component's participation in the RMF TAG.

v. Require that contracts and other agreements include specific requirements in accordance with this issuance.

w. Provide cybersecurity developmental, operational, and sustainment test and evaluation (T&E), and assessment results for acquisition and fielded programs to the appropriate AO to inform ATO decisions.

x. Ensure acquisition programs submit cybersecurity T&E results to the appropriate AO to inform ATO decisions.

y. Ensure acquisition programs develop evaluation metrics for DT&E and OT&E, and continuous monitoring, at the beginning of the development process.

2.8. CHAIRMAN OF THE JOINT CHIEFS OF STAFF.

In coordination with the DoD CISO, and in addition to the responsibilities in Paragraph 2.7., the Chairman of the Joint Chiefs of Staff:

a. Requires the Joint Capabilities Integration and Development System process to support and document system categorization in accordance with this issuance.

b. Maps systems to dependent missions.

c. Supports JCA owners in developing required RMF guidance for their portfolios.

2.9. COMMANDER, UNITED STATES STRATEGIC COMMAND.

In addition to the responsibilities in Paragraph 2.7., the Commander, United States Strategic Command:

a. Serves as the AO for nuclear command, control, and communication systems as identified by the Joint Staff (as the Warfighting MA Principal AO (PAO)).

b. Delegates system-level responsibilities, as required.

2.10. COMMANDER, UNITED STATES SPACE COMMAND.

In addition to the responsibilities in Paragraph 2.7., the Commander, United States Space Command:

a. Assigns AOs for space systems.

b. Issues authorization guidance in accordance with this issuance for space systems.

c. Resolves authorization issues for space systems used by the DoD in accordance with DoDI 8500.01 and Committee on National Security Systems Policy No. 12.

2.11. COMMANDER, USCYBERCOM.

In coordination with the DoD CISO and in addition to the responsibilities in Paragraph 2.7., the Commander, USCYBERCOM:

a. Coordinates with the other DoD Component heads to:

(1) Ensure all cybersecurity risk management decision-makers are aware of significant cybersecurity risks.

(2) Integrate the vulnerability management process into the RMF process.

b. Coordinates with the Director, National Security Agency/Chief, Central Security Service to make cyberspace operations forces' operational risk tolerances and relevant cyber threat information available to all cybersecurity risk management decision-makers to eliminate isolated processes.

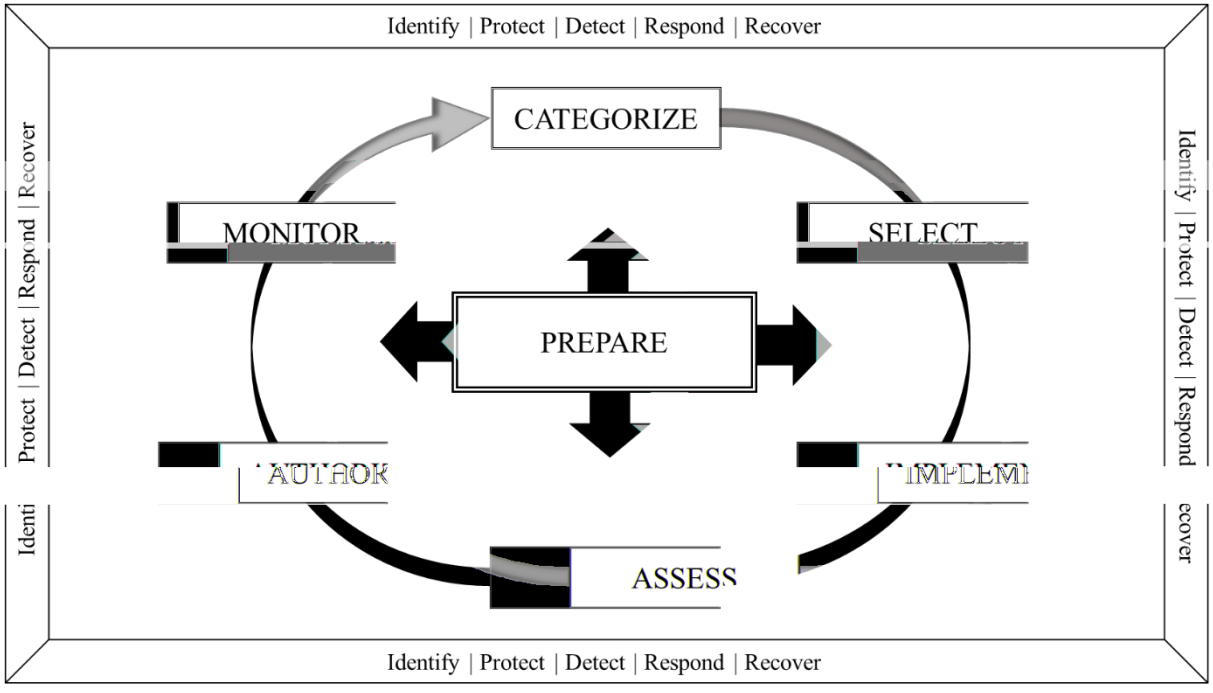
SECTION 3: DOD AND NIST RMF IMPLEMENTATION

3.1. OVERVIEW.

The RMF process for lifecycle cybersecurity risk to DoD systems is in accordance with the NIST SP 800-30, 800-37, 800-39, 800-53A, 800-137, Committee on National Security Systems Policy No. 22, CNSSI No. 1253 and 1254, DoDD 8000.01, and DoDI 8500.01. The RMF process adopts the NIST RMF in accordance with NIST SP 800-37 to comply with FISMA requirements. This process is intended to ensure DoD systems with digital capabilities, including National Security Systems, are engineered for cyber survivability. This is done by integrating controls that support security, privacy, operational resilience, supply chain risk management, and the best cyber intelligence, or commercial cyber threat information available at the system and organizational levels.

a. The RMF consists of the steps depicted in Figure 1. This process integrates with the system life-cycle and system security engineering processes. The program initiates or updates RMF activities during system inception (e.g., documented during requirements identification) and for any significant system modifications (e.g., engineering changes). Refer to the RMF KS section on 'System and Environment Changes' for further information regarding what is included in significant system modification.

Figure 1. RMF Process



b. Failure to initiate the RMF at system or program inception is not a justification for ignoring or not complying with the RMF. Systems without an ATO must begin the RMF, regardless of the system life-cycle stage (e.g., acquisition, operation). Chapter 3 of NIST SP 800-37 details the steps of the RMF, with additional guidance on the RMF KS.

c. The RMF process applies to all systems and organizations regardless of acquisition pathway in the DoD, as well as DoD partnered systems and organizations where it has been agreed that DoD standards will be followed.

(1) DoD systems (e.g., weapons systems, stand-alone systems, control systems, or any other type of systems with digital capabilities) must receive and maintain a valid authorization before beginning operations. Refer to the RMF KS for additional guidance on authorizations.

(2) Technologies below the system level (e.g., system components, hardware, software, external services) do not require an ATO. However, these technologies must still complete specific RMF assessment procedures under the "Assess Only" process. Refer to the KS for more information on these "Assess Only" processes.

3.2. RMF STEPS.

a. Prepare.

Prepare to execute the RMF from an organizational and system-level perspective by setting context and priorities for privacy and security risk management to carry out essential activities at the organization, mission and business process, and information system levels of the organization. The "Prepare" step tasks must be completed by the DoD Component CIO, DoD PAO, and JCA capability portfolio manager (CPM) to enable an effective risk-managed security authorization process. See Table 1 for "Prepare" step tasks. For additional guidance, see the RMF KS.

Table 1. Organization Prepare Step Tasks

Tasks	Outcomes	Primary Responsibility
Task P-1 Risk Management Roles	Individuals are identified and assigned key roles for executing the RMF. [Cybersecurity Framework (CSF): **ID.AM-6; ID.GV-2**]	• Head of Agency • Chief Information Officer (CIO) • Senior Agency Official for Privacy
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. [CSF: **ID.RM; ID.SC**]	Head of Agency
Task P-3 Risk Assessment – Organization	An organization-wide risk assessment is completed, or an existing risk assessment is updated. [CSF: **ID.RA; ID.SC-2**]	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency information security officer (ISO) • Senior Agency Official for Privacy
Task P-4 Organizationally – Tailored Control Baselines and CSF Profiles (Optional)	Organizationally-tailored control baselines and/or CSF profiles are established and made available. [CSF: **Profile**]	• Mission or Business Owner Senior Accountable Official for Risk Management or Risk Executive (Function)

Table 1. Organization Prepare Step Tasks, Continued

Tasks	Outcomes	Primary Responsibility
Task P-5 Common Control Identification	Common controls that are available for inheritance by organizational systems are identified, documented, and published.	• Senior Agency ISO • Senior Agency Official for Privacy
Task P-6 Impact – Level Prioritization (Optional)	A prioritization of organizational systems with the same impact level is conducted. [CSF: **ID.AM-5**]	Senior Accountable Official for Risk Management or Risk Executive (Function)
Task P-7 Continuous Monitoring Strategy – Organization	An organization-wide strategy for monitoring control effectiveness is developed and implemented. [CSF: **DE.CM; ID.SC-4**]	Senior Accountable Official for Risk Management or Risk Executive (Function)
Task P-8 Mission or Business Focus	Missions, business functions, and mission or business processes that the system is intended to support are identified. [CSF: Profile; Implementation Tiers; **ID.BE**]	Mission or Business Owner
Task P-9 System Stakeholders	The stakeholders having an interest in the system are identified. [CSF: **ID.AM; ID.BE**]	• Mission or Business Owner • SO
Task P-10 Asset Identification	Stakeholder assets are identified and prioritized. [CSF: **ID.AM**]	• SO
Task P-11 Authorization Boundary	The authorization boundary (i.e., system) is determined.	• AO
Task P-12 Information Types	The types of information processed, stored, and transmitted by the system are identified. [CSF: **ID.AM-5**]	• SO • Information Owner (IO) or Steward
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. [CSF: **ID.AM-3; ID.AM-4**]	• Senior Agency Official for Privacy • SO • IO or Steward
Task P-14 Mission-Based Cyber Risk Assessment	A system-level risk assessment is completed or an existing risk assessment is updated. [CSF: **ID.RA; ID.SC-2**]	• SO • Information System Security Officer (ISSO) • System Privacy Officer
Task P-15 Requirements Definition	Security and privacy requirements are defined and prioritized. [CSF: **ID.GV; PR.IP**]	• Mission or Business Owner • SO • IO or Steward • System Privacy Officer
Task P-16 Enterprise Architecture	The placement of the system within the enterprise architecture is determined.	• Mission or Business Owner • Enterprise Architect • Security Architect • Privacy Architect
Task P-17 Requirements Allocation	Security and privacy requirements are allocated to the system and to the environment in which the system operates. [CSF: **ID.GV**]	• Security Architect • Privacy Architect • ISSO • System Privacy Officer
Task P-18 System Registration	The system is registered for purposes of management, accountability, coordination, and oversight. [CSF: **ID.GV**]	• SO

b. Categorize

Categorize the system in accordance with CNSSI No. 1253 based on the information analyzed, stored, and relayed by the system and an analysis of the impact of potential loss of confidentiality, integrity, and availability to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems. See Table 2 for a list of tasks and outcomes.

Table 2. Categorize Tasks and Outcomes

Tasks	Outcomes	Primary Responsibility
Task C-1 System Description	The characteristics of the system are described and documented. [CSF: **Profile**]	• SO
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. [CSF: **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 supply chain risk management plans. [CSF: **Profile**] • Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission or business processes. [CSF: **Profile**] • Security categorization results reflect the organization's risk management strategy.	• SO • IO or Steward
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.	• AO or AO Designated Representative (AODR) • Senior Agency Official for Privacy (for systems processing personal identifiable information)

c. Select.

Choose an initial set of system controls and tailor the controls as necessary to reduce risk to an acceptable level based on a risk assessment. See Table 3 for a list of tasks and outcomes.

Table 3. Select Tasks and Outcomes

Tasks	Outcomes	Primary Responsibility
Task S-1 Control Selection	Control baselines necessary to protect the system commensurate with risk are selected. [CSF: **Profile**]	• SO • Common Control Provider
Task S-2 Control Tailoring	Controls are tailored, producing tailored control baselines. [CSF: **Profile**]	• SO • Common Control Provider

Table 3. Select Tasks and Outcomes, Continued

Tasks	Outcomes	Primary Responsibility
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). [CSF: Profile; PR.IP]	• Security Architect • Privacy Architect • ISSO • System Privacy Officer
Task S-4 Documentation of Planned Control Implementations	Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents. [CSF: **Profile**]	• SO • Common Control Provider
Task S-5 Continuous Monitoring Strategy – System	A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed. [CSF: **ID.GV; DE.CM**]	• SO • Common Control Provider
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 AO.	• AO or AODR

d. Implement.

Implement the controls and describe how the controls are employed within the system and its operating environment. See Table 4 for a list of tasks and outcomes.

Table 4. Implement Tasks and Outcomes

Tasks	Outcomes	Primary Responsibility
Task I-1 Control Implementation	• Controls specified in the security and privacy plans are implemented. [CSF: **PR.IP-1**] • Systems security and privacy engineering methodologies are used to implement the controls in system security and privacy plans. [CSF: **PR.IP-2**]	• SO • Common Control Provider
Task I-2 Update Control Implementation Information	• Changes to the planned implementation of controls are documented. [CSF: **PR.IP-1**] • The security and privacy plans are updated based on information obtained during the implementation of the controls. [CSF: **Profile**]	• SO • Common Control Provider

e. Assess.

Assess the controls to determine whether they are being correctly implemented, operating as intended, and producing the desired outcomes in meeting the requirements for security and privacy. See Table 5 for a list of tasks and outcomes.

Table 5. Assessment Tasks and Outcomes

Tasks	Outcomes	Primary Responsibility
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.	• AO or AODR
Task A-2 Assessment Plan	• Documentation needed to conduct the assessments is provided to the assessor or assessment team. • Security Assessment Plans include documentation of test events and resources that can support assessments, coordinated with developers and developmental and operational testers. T&E strategy includes high-level description of assessment plans. • Security, privacy, and supply chain risk management assessment activities are developed and documented. • Assessment are reviewed by the security control assessor (SCA) and approved by the AO to establish the expectations for the control assessments and the level of effort required.	• AO or AODR • Control Assessor
Task A-3 Control Assessments	• Control assessments are conducted in accordance with the security and privacy assessment plans. • Developer, engineering, developmental, and operational test events are conducted to support assessments. • 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 the speed, effectiveness, and efficiency of assessments.	• Control Assessor

Table 5. Assessment Tasks and Outcomes, Continued

Tasks	Outcomes	Primary Responsibility
Task A-4 Assessment Reports	• Assessment reports that provide findings and recommendations are completed and include results from developer, engineering, developmental, and operational test events. • Assessment reports include results from developer, engineering, developmental, and operational test events.	• Control Assessor
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. [CSF: Profile]	• SO • Common Control Provider • Control Assessor
Task A-6 A Plan of Actions and Milestones	POA&M detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed. [CSF: **ID.RA-6**]	• SO • Common Control Provider

f. Authorize.

Authorize the system based on a determination of whether the risk to organizational operations and assets, individuals, agencies, commands, and the Nation is acceptable, and cyberspace operational commanders' requirements are met. Final risk determination and authorization decision definitions (e.g., interim authorization to test, ATO, ATO with conditions, and denial ATO) and examples are on the RMF KS. See Table 6 for a list of tasks and outcomes.

Table 6. Authorization Tasks and Outcomes

Tasks	Outcomes	Primary Responsibility
Task R-1 Authorization Package	An authorization package is developed for submission to the AO.	• SO • Common Control Provider • Senior Agency Official for Privacy
Task R-2 Risk Analysis and Determination	A risk determination by the AO that reflects the risk management strategy, including risk tolerance, is rendered.	• AO or AODR
Task R-3 Risk Response	Risk responses for determined risks are provided. [CSF: **ID.RA-6**]	• AO or AODR
Task R-4 Authorization Decision	The authorization for the system or the common controls is approved or denied.	• AO
Task R-5 Authorization Reporting	Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.	• AO or AODR

(1) The security authorization documentation consists of all artifacts developed through RMF activity and is maintained throughout a system's life-cycle. The security authorization documentation package is the minimum information necessary for the receiving organization to accept a system. The security authorization documentation package is made up of:

(a) The security plan.

(b) The security assessment report.

(c) All POA&Ms.

(d) The authorization decision document.

(2) Detailed information on the content and use of the security authorization package is available on the RMF KS.

g. Monitor.

Monitor the system and associated controls on an ongoing basis, including monitoring the effectiveness of controls, documenting system and operating environment changes, conducting risk assessments and impact analyses, and reporting on system security and privacy. See Table 7 for a list of tasks and outcomes.

Table 7. Monitor Tasks and Outcomes

Tasks	Outcomes	Primary Responsibility
Task M-1 System and Environment Changes	The system and environment of operation are monitored in accordance with the continuous monitoring strategy. [CSF: **DE.CM**; **ID.GV**]	• PM or SO • Common Control Provider • Senior Agency ISO • Senior Agency Official for Privacy
Task M-2 Ongoing Assessments	Ongoing testing and assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy. [CSF: **ID.SC-4**]	• Control Assessor
Task M-3 Ongoing Risk Response	The output of continuous monitoring activities is analyzed and responded to appropriately. [CSF: **RS.AN**]	• AO • PM or SO • Common Control Provider
Task M-4 Authorization Package Updates	Risk management documents are updated based on continuous monitoring activities. [CSF: **RS.IM**]	• PM or SO • Common Control Provider
Task M-5 Security and Privacy Reporting	A process is in place to report the security, privacy, and supply chain risk management posture to the AO and other senior leaders and executives.	• PM or SO • Common Control Provider • Senior Agency ISO • Senior Agency Official for Privacy
Task M-6 Ongoing Authorization	AOs conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.	• AO
Task M-7 System Disposal	A system disposal strategy is developed and implemented, as needed.	• PM or SO

3.3. INTEGRATING THE RMF INTO THE DEFENSE ACQUISITION MANAGEMENT SYSTEM.

a. Overview.

The RMF is designed to complement and support the Defense Acquisition System activities, milestones, and phases.

(1) RMF activities must be initiated as early as possible in the DoD acquisition process to increase security and decrease cost.

(2) Requirements, development, procurement, and T&E processes must apply the RMF in the acquisition of DoD information technology.

(3) Risks to systems must be designated consistent with the most severe threat to any individual component or subcomponent for consideration of requirements, acquisition, and T&E.

b. Life-Cycle.

(1) The Adaptive Acquisition Framework is defined and illustrated in DoDI 5000.02.

(2) Alignment of RMF steps to the acquisition lifecycle can be found on the RMF KS.

(3) DoDI 5000.90 establishes policy for the acquisition PM's role and responsibilities for managing cybersecurity, including the RMF, throughout the program's acquisition lifecycle.

(4) See DoDIs 5000.82, 5000.83, 5000.89, and 5000.90 for details on integrating RMF in acquisition functional processes.

SECTION 4: CYBERSECURITY RISK GOVERNANCE

4.1. CYBERSECURITY RISK GOVERNANCE.

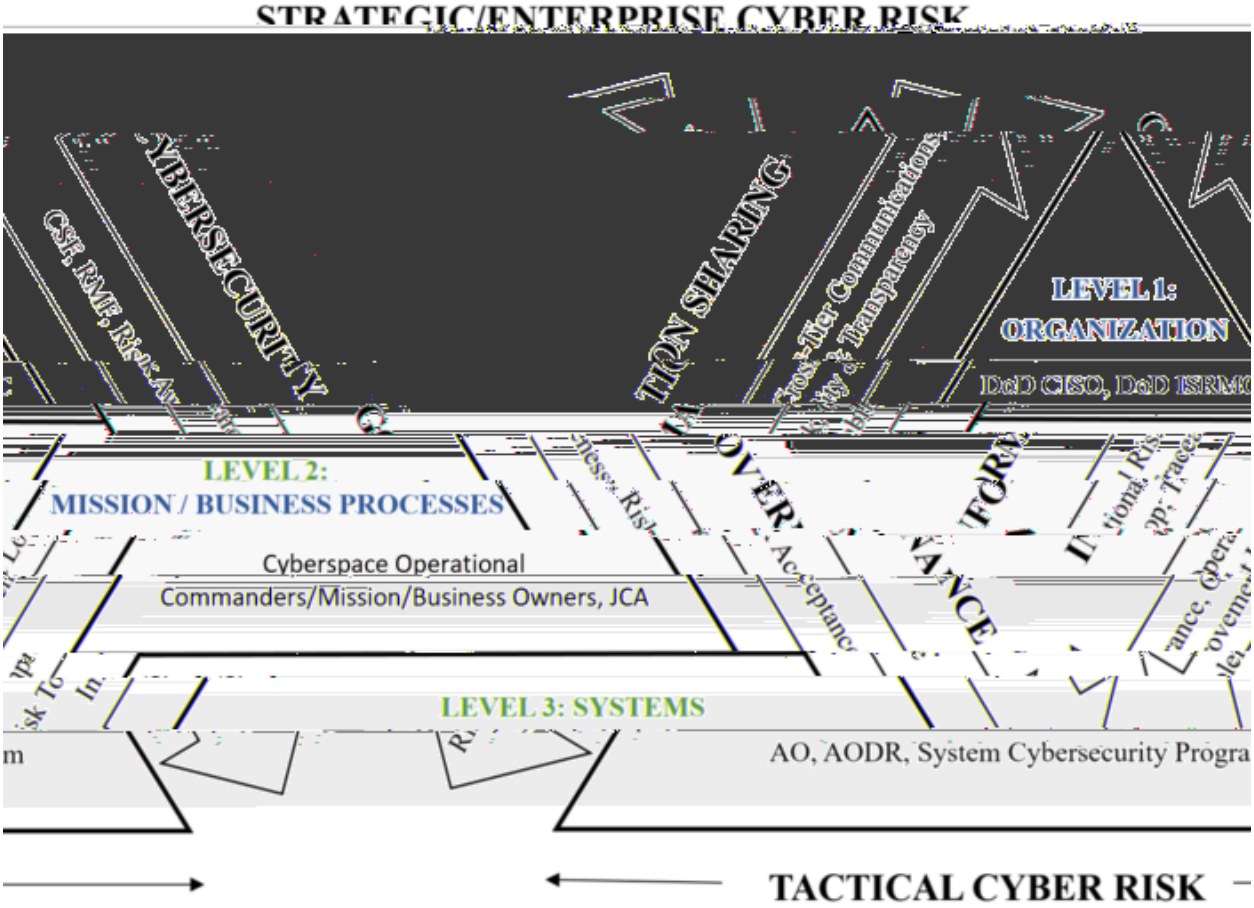
The DoD cybersecurity risk governance structure implements the three-level approach to the cybersecurity risk management described in NIST SP 800-39. It synchronizes and integrates cybersecurity activities across all phases of the system life-cycle, spanning logical and organizational entities.

a. Within the cybersecurity risk governance structure, governance bodies (e.g., DoD Information Security Risk Management Committee (DoD ISRMC), Defense Security/Cybersecurity Authorization Working Group (DSAWG)) play a critical role in cybersecurity risk acceptance for the DoD, mitigating critical vulnerabilities, integrating information sharing, and ensuring a balance between organizational and tactical cybersecurity risk.

b. Successful cybersecurity risk governance requires cooperation across all levels, including governance bodies, organizational leadership, IOs or stewards, operational commanders, and system-level owners and operators.

c. Governance elements are illustrated in Figure 2 and further explained in this section.

Figure 2. Cybersecurity Risk Governance



4.2. LEVEL 1 – ORGANIZATION.

The organization described in Level 1 is the OSD or strategic level. It addresses risk management at the DoD enterprise level. The key governance elements and resources in Level 1 are:

a. DoD CISO.

The DoD CISO:

(1) Directs and oversees the cybersecurity risk management of DoD information technology and directs and coordinates the DoD Cybersecurity Program, which includes establishing and maintaining the RMF.

(2) Advises and informs the PAOs and their representatives.

(3) Oversees the RMF TAG and the RMF KS.

(4) Presents escalation procedures to resolve disputes among RMF processes and system development, acquisition and sustainment processes, cyberspace operations, functional operational processes, and assessments for DoD mission assurance, where necessary.

b. Risk Executive Function.

The Risk Executive Function consists of the DoD ISRMC supported by the DSAWG.

(1) DoD ISRMC:

(a) Provides strategic guidance to Levels 2 and 3, assesses Level 1 risk, and authorizes information exchanges and connections for DoD enterprise systems, cross-mission area systems, cross security domain connections, and mission partner connections.

(b) Performs the Risk Executive Function as described in DoDI 8500.01 and NIST SP 800-39, and makes enterprise level risk acceptance determinations for authorized enterprise systems, satisfying the requirements of cybersecurity reciprocity. If the DoD ISRMC accepts the risk on behalf of the DoD Information Enterprise, the receiving organization may not refuse to deploy the system.

(c) Identifies and manages enterprise level cybersecurity risks.

(d) Oversees cybersecurity risk guidance development for DoD business and mission functions.

(e) Interfaces with the Mission Assurance Coordination Board regarding cybersecurity risk, requirements, and implementation in accordance with DoDI 3020.45.

(2) The DSAWG, in support of the DoD ISRMC:

(a) Is the community forum for reviewing and resolving authorization issues related to sharing community risk.

(b) Develops and provides guidance to the AOs for system connections to the DoD Information Enterprise. AOs who disagree with DSAWG decisions may appeal to the DoD ISRMC.

(3) Reference the RMF KS for additional processes needed for environment specific requirements.

c. DoD Cybersecurity Architecture.

The DoD cybersecurity architecture represents the functions, relationships, and form of DoD cybersecurity capabilities and is informed by the strategies, standards, and plans developed for achieving an assured, integrated, and survivable information enterprise.

d. RMF TAG.

The RMF TAG provides implementation guidance for the RMF by interfacing with the DoD Component cybersecurity programs, cybersecurity communities of interest, and other entities, such as the DSAWG, to address common issues across all entities. In doing so, the RMF TAG:

(1) Provides a detailed analysis and authoring support for the RMF KS.

(2) Recommends changes to security controls, security control baselines, and overlays in DoD assignment values, and associated implementation guidance and assessment procedures to the DoD CISO.

(3) Recommends changes to cybersecurity risk management processes to the DoD CISO.

(4) Advises DoD forums established to resolve RMF priorities and cross-cutting issues.

(5) Develops and manages automation requirements for DoD services that support the RMF.

(6) Develops guidance for facilitating RMF reciprocity throughout the DoD.

(7) Implements updates of reference security control documents.

(8) Coordinates with privacy counterparts to manage privacy risks throughout the RMF process when appropriate.

e. RMF KS.

The RMF KS:

(1) Is a dynamic online knowledge base that supports the RMF implementation, planning, and execution by functioning as the authoritative source for RMF procedures and guidance.

(2) Supports RMF practitioners by providing access to DoD security control baselines, security control descriptions, security control overlays, and implementation guidance and assessment procedures, all in accordance with CNSSI 1253, NIST SP 800-53, 800-53A, and 800-53B.

(3) Supports the RMF TAG by enabling TAG functions and activities, including maintaining membership, voting, analysis, authoring, and configuration control of RMF KS enterprise content and functionality.

4.3. LEVEL 2 – MISSION OR BUSINESS PROCESSES.

The key governance elements and resources in Level 2 are:

a. JCA CPM.

(1) JCA CPMs:

(a) Provide recommendations and advice regarding capability requirements for business mission functions in accordance with DoDD 7045.20.

(b) Under the direction of the DoD ISRMC, are responsible for recommending cybersecurity risk requirements for their respective JCA.

(c) Supported by the Office of the DoD CIO and Joint Staff J-6, develop and maintain cybersecurity risk guidance required by the RMF "Prepare" step for their JCA.

(2) The existing JCA structure will serve as the DoD's common framework and lexicon for organizing capability portfolios in accordance with DoDD 7045.20. Civilian and military CPMs manage JCA capability portfolios. JCA CPMs may:

(a) Provide recommendations on the cybersecurity requirements for their respective portfolios to the DoD ISRMC.

(b) Develop Level 2 prepare step guidance for systems within their area of responsibility in accordance with NIST SP 800-37. Reference DoDD 7045.20, Enclosure 2, Table 1 for JCA CPM lead officials.

b. PAO.

A PAO is appointed for each of the DoD MAs (e.g., warfighting MA, business MA, enterprise information environment MA, and DoD portion of the intelligence MA) and their representatives are DoD ISRMC members. The alignment of DoD MAs with RMF activities promotes consideration of cybersecurity risk when conducting risk assessments for IT portfolio management. PAOs:

(1) Represent the interests of their MA, in accordance with DoDD 8115.01 and, as required, issue cybersecurity risk guidance specific to their MA, in accordance with this issuance.

(2) Resolve authorization issues within their respective MAs and work with other PAOs to resolve problems among MAs, as needed.

(3) Designate AOs for MA systems supporting MAs communities of interest specified in DoDI 8320.07 in coordination with appropriate DoD Component heads, if required.

(4) Designate information security architects or systems security engineers for MA segments or systems, as needed.

c. DoD Component CIO.

Each DoD Component CIO:

(1) Supported by the DoD Component CISO appointed in accordance with DoDI 8500.01, is responsible for:

(a) Administering the RMF within the DoD Component cybersecurity program.

(b) Participation in the RMF TAG.

(c) The visibility of, and sharing, the RMF status of assigned systems.

(d) Enforcing training requirements for persons participating in the RMF.

(2) Maintains visibility of assessment and authorization status of DoD Component systems through automated assessment and authorization tools or designated repositories for their Component to the DoD CIO and PAOs.

(3) Verifies an SO and/or PM is appointed in writing for each DoD Component system.

(4) Communicate organizational risk tolerance.

(5) Establish and maintain processes and procedures to manage DoD Component POA&Ms.

(6) Appoint a DoD Component CISO to direct and coordinate the DoD Component cybersecurity program.

(7) Review and document concurrence or non-concurrence, and provide directions as merited, before ATOs are issued for DoD Component systems with a level risk of "Very High" or "High."

(8) Develop and implement the "Prepare" step guidance for their organizational elements.

(9) Include performance of cybersecurity functions under the RMF, (e.g., AO, SCA, ISSM) in the annual evaluation criteria.

d. DoD Component CISO.

DoD Component CISOs:

(1) Have authority and responsibility for security controls assessment and establish and manage a coordinated security assessment process for systems governed by the DoD Component cybersecurity program.

(2) Implement and enforce the RMF within the DoD Component cybersecurity program.

(3) Perform as the SCA or formally delegate the security control assessment role for governed systems.

(4) Track the assessment and authorization status of systems governed by the DoD Component cybersecurity program.

(5) Establish and oversee a team of qualified cybersecurity professionals responsible for conducting security assessments.

(a) CISOs may task, organize, staff, and centralize or direct assessment activities to representatives as appropriate.

(b) Regardless of the adopted model, the CISO is responsible for assessing quality, capacity, visibility, and effectiveness of security control assessments.

(6) Identify and recommend changes and improvements to the security assessment process, security test and evaluation, and risk assessment methodology, including procedures, risk factors, assessment approach, and analysis approach to the RMF TAG for inclusion in the RMF KS.

(7) Advise AOs on the adequacy of acquisition program implementation of cybersecurity requirements.

(8) Serve as the single cybersecurity coordination point for joint or DoD-wide programs that deploy systems to DoD Component enclaves.

(9) Verify that DoD Component RMF guidance is posted to the DoD Component portion of the RMF KS, and is consistent with this issuance and supporting guidance.

(10) Oversee DoD Component-level participation in the RMF TAG.

4.4. LEVEL 3 – SYSTEMS.

The key governance elements and resources in Level 3 are:

a. AOs.

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 the business owner and mission owner organizations (as opposed to limiting appointments to CIO organizations) to promote accountability in authorization decisions that balance mission and business needs and security concerns. In addition to the responsibilities established in DoDI 8500.01, AOs:

(1) Comply with DoD ISRMC direction issued on behalf of the JCA CPMs.

(2) Initiate and complete all appropriate RMF tasks, with appropriate documentation, for assigned systems.

(3) Monitor and track the overall execution of system-level POA&Ms.

(4) Promote reciprocity as much as possible.

(5) Do not delegate authorization decisions. Other AO responsibilities and tasks may be delegated to formally appointed and qualified AODRs.

(6) Review the security authorization documentation package in light of mission and information environment indicators and determine a course of action provided to the responsible CIO or CISO for reporting requirements described in FISMA. An AO may downgrade or revoke an authorization decision at any time if risk conditions or concerns so warrant.

(7) Coordinate authorization activities and results with the system acquisition or procurement representatives.

(8) Verify the system meets cyberspace operational commander requirements. When risks are not fully mitigated, AOs inform operators of potential impacts.

(9) Verify the cyberspace and functional operational commanders have the necessary cyber risk information on the system.

(10) When a cybersecurity risk affects an operational requirement, facilitate coordination with:

(a) Cyberspace and functional operational commanders.

(b) Acquisition or procurement representatives.

(11) Verify that decisions:

(a) Incorporate the best cyber intelligence or commercial cyber threat information available.

(b) Are recorded, tracked, and made available to all parties throughout the system's lifecycle.

b. System Cybersecurity Program.

The system cybersecurity program:

(1) Consists of the policies, procedures, and activities of the SO, PM, UR, ISSM, and ISSO at the system level.

(2) Implements and executes policy and guidance from Levels 1 and 2 and augments them as needed.

(3) Is responsible for establishing and maintaining system security, including monitoring and reporting the system security status.

(4) SOs:

(a) In coordination with the IOs, data owners or stewards, categorize systems in accordance with CNSSI 1253 and document the categorization in the appropriate Joint Capabilities Integration and Development System capabilities document (e.g., capabilities development document).

(b) Appoint a UR for assigned systems.

(c) Develop, maintain, and track the security plan for assigned systems (e.g., common security controls owner performs this function for inherited controls).

(d) Oversee and manage the system's cybersecurity posture, operations, and sustainment activities (e.g., system patching, account management, updates, and required maintenance) in accordance with the AO directions and approvals outlined in formal ATO documentation.

(e) Document operations and sustainment activities delegated to external partners.

(5) PMs (or SO, if no PM is assigned):

(a) Appoint an ISSM for each assigned system with the support, authority, and resources to satisfy the responsibilities established in this issuance.

(b) Verify each program acquiring a system has an assigned system security engineer who is fully integrated into the systems engineering process.

(c) Implement the RMF for assigned systems.

(d) Verify that the planning and execution of all RMF activities are aligned, integrated with, and supportive of the system acquisition process.

(e) Enforce AO authorization decisions for hosted or interconnected systems.

(f) Implement and assist the SO in maintaining and tracking the security plan for assigned systems.

(g) Oversee POA&M development, monitoring, resolution, and resources.

(h) Oversee periodic reviews, testing, and assessment of assigned systems, conducted at least annually.

(i) Provide the system description.

(j) Register the system in the DoD Component registry.

(k) Verify T&E of the assigned system includes planning, resourcing, and documentation in the T&E master plan in accordance with applicable pathway policies and DoDI 5000.89.

(6) URs represent the operational and functional requirements of the user community in the RMF process.

(7) ISSMs, in addition to the responsibilities established in DoDI 8500.01:

(a) Support implementing the RMF.

(b) Maintain and report systems assessment and authorization status and issues in accordance with DoD Component guidance.

(c) Provide direction to the ISSO in accordance with DoDI 8500.01.

(d) Address issues affecting the organization's overall security through coordination with the SO, PM, ISSO, and UR, as appropriate.

4.5. RMF ROLE APPOINTMENT.

Table 8 identifies the appropriate authority for appointing RMF roles. Refer to the RMF KS for additional guidance.

Table 8. Appointment of RMF Roles

Role	Appointed By
PAO	DoD MA owner
DoD CISO	DoD CIO
DoD Component CIO	DoD Component head
AO	DoD Component head; PAO for MA- managed information systems
AODR	AO
DoD Component CISO	DoD Component CIO or, in organizations in which the position of DoD Component CIO does not exist, the DoD Component head.
SCA	DoD Component CISO is the Component SCA but may formally delegate the SCA role as appropriate.
PM	DoD Component Acquisition Executive
ISSM	PM or SO
UR	ISO
RMF TAG Representative	DoD Component CISO
SO	DoD Component head
ISSO	PM or SO

SECTION 5: RMF KS

5.1. OVERVIEW.

DoD RMF practitioners need access to RMF direction, standards, and tools to effectively and efficiently apply the appropriate methods, standards, and practices required to protect DoD information technology. RMF implementation must reflect the most up-to-date DoD intent on evolving security objectives and risk conditions.

5.2. RMF KS.

The RMF KS was established as the web-based resource to serve as the authoritative source for standardized implementation of RMF and the repository for DoD RMF policy and procedures.

a. The RMF KS:

(1) Serves as the authoritative source for providing direction, standards, and tools for implementing and executing the RMF.

(2) Is available to all individuals with information technology risk management responsibilities.

(3) Provides convenient access to security controls baselines, overlays, individual security controls, and security control implementation guidance and assessment procedures.

(4) Supports automated and non-automated implementation of the RMF.

(5) Provides cybersecurity accountability information.

(6) Provides reciprocity guidance.

(7) Is accessible by individuals with a DoD public key infrastructure certificate (e.g., common access card), or external certification authority certificate in conjunction with DoD sponsorship (e.g., for DoD contractors without a common access card and who work offsite).

(8) Hosts a library of tools, diagrams, process maps, documents, and other items to support and aid in RMF execution.

(9) Serves as a collaborative workspace for the RMF user community to develop, share, and post lessons learned, best practices, cybersecurity news and events, and other cybersecurity-related information resources.

b. The RMF TAG is responsible for the functional configuration and content management of the RMF KS and provides detailed analysis and authoring support for the enterprise portion of the RMF KS content.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AO	authorizing official
AODR	authorizing official designated representative
ATO	authorization to operate
CIO	chief information officer
CISO	chief information security officer
CNSSI	Committee on National Security Systems Instruction
CPM	capability portfolio manager
CSF	cybersecurity framework
DISA	Defense Information Systems Agency
DoD ISRMC	DoD Information Security Risk Management Committee
DoDD	DoD directive
DoDI	DoD instruction
DOT&E	Director, Operational Test and Evaluation
DSAWG	Defense Security/Cybersecurity Authorization Working Group
DT&E	developmental test and evaluation
FISMA	Federal Information Security Modernization Act of 2014
IO	information owner
ISO	information security officer
ISSM	information system security manager
ISSO	information system security officer
JCA	Joint Capability Area
KS	knowledge service
MA	mission area
NIST	National Institute of Standards and Technology
OT&E	operational test and evaluation
PAO	principal authorizing official
PM	program manager
POA&M	plan of action and milestones
RMF	risk management framework (for DoD systems)

ACRONYM	MEANING
SCA	security control assessor
SO	system owner
SP	special publication
T&E	test and evaluation
TAG	Technical Advisory Group (RMF)
UR	user representative
USCYBERCOM	United States Cyber Command
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
ATO	Defined in NIST SP 800-39 under "Security Authorization (to Operate)."
CSF	Defined in NIST SP 800-37.
cyber risk	A measure of the extent to which an entity is threatened by a potential circumstance or event in information technology.
cyber operational risk	A measure of the extent to which an entity is threatened by a potential circumstance or event in information technology relating to routine function and activities of an organization.
cyberspace operational risk	A measure of the extent to which an entity is threatened by a potential circumstance or event in the interdependent network of information technology infrastructures, and includes telecommunications networks, computer systems, and embedded processors and controllers.
cybersecurity risk	The probability of exposure, loss of critical assets and sensitive information, or reputational harm as a result of a cyber-attack or breach within an organization's network.
DoD Information Enterprise	Defined in DoDD 8000.01.
enterprise architect	Defined in NIST SP 800-37.

TERM	DEFINITION
ISO	Defined in NIST SP 800-37.
MA	Defined in United States Code, Title 40, Section 11331.
PM	Defined in NIST SP 800-39.
privacy architect	Defined in NIST SP 800-37.
privacy engineer	Defined in NIST SP 800-37.
security architect	Defined in NIST SP 800-37.
Senior Accountable Official for Risk Management or Risk Executive (Function)	Defined in NIST SP 800-37.
system component	Defined in NIST SP 800-37.
system element	Defined in NIST SP 800-37.
system privacy officer	Defined in NIST SP 800-37.

REFERENCES

Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Security Systems," current edition

Committee on National Security Systems Instruction 1254, "Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems," August 2016.

Committee on National Security Systems Instruction 4009, "Committee on National Security Systems (CNSS) Glossary," March 2, 2022

Committee on National Security Systems Policy Number 12, "Cybersecurity Policy for Space Systems Used to Support National Security Missions," February 6, 2018

Committee on National Security Systems Policy Number 22, "Cybersecurity Risk Management Policy," September, 2021

DoD Directive 3020.04, "Order of Succession Pursuant to Executive Order 13533 and the Federal Vacancies Reform Act of 1998," August 25, 2010

DoD Directive 5000.01, "The Defense Acquisition System," September 9, 2020

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 7045.20, "Capability Portfolio Management," September 25, 2008, as amended

DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016, as amended

DoD Directive 8115.01, "Information Technology Portfolio Management," October 10, 2005

DoD Directive 8140.01, "Cyberspace Workforce Management," October 5, 2020

DoD Instruction 3020.45, "Mission Assurance (MA) Construct," August 14, 2018

DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," January 23, 2020, as amended

DoD Instruction 5000.82, "Acquisition of Information Technology, "April 21, 2020

DoD Instruction 5000.83, "Technology and Program Protection to Maintain Technological Advantage," July 20, 2020, as amended

DoD Instruction 5000.89, "Test and Evaluation," November 19, 2020

DoD Instruction 5000.90, "Cybersecurity for Acquisition Decision Authorities and Program Managers," December 31, 2020

DoD Instruction 8010.01, "Department of Defense Information Network (DODIN) Transport," September 10, 2018

DoD Instruction 8320.07, "Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense," August 3, 2015, as amended

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

DoD Instruction 8531.01, "DoD Vulnerability Management," September 15, 2020

Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017

National Institute of Standards and Technology Special Publication 800-30, "Guide for Conducting Risk Assessments," September 17, 2012

National Institute of Standards and Technology Special Publication 800-37, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 20, 2018

National Institute of Standards and Technology Special Publication 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011

National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations," December 10, 2020

National Institute of Standards and Technology Special Publication 800-53A, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," December 18, 2014

National Institute of Standards and Technology Special Publication 800-53B, "Control Baselines for Information Systems and Organizations," December 10, 2020

National Institute of Standards and Technology Special Publication 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," September 30, 2011

National Institute of Standards and Technology Special Publication 800-137A, "Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing and ISCM Program Assessment," May 21, 2020

Office of Management and Budget Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems," November 18, 2013

United States Code, Title 10, Section 142

United States Code, Title 40, Section 11331

United States Code, Title 44, Chapter 35, Subchapter II (also known as the "Federal Information Security Modernization Act of 2014")