

Introduction to the Risk-Management Framework (RMF) for DOD Information Technology (IT)

The RMF provides a disciplined and structured process that combines information system (IS) security and risk-management activities into the system-development lifecycle and authorizes their use within DOD. The RMF changes the traditional focus of certification and accreditation as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage IS-related security risks in diverse environments of complex and sophisticated cyber threats and ever-increasing system vulnerabilities.

The RMF applies to all DOD IT that receives, processes, stores, displays, or transmits DOD information. These technologies are broadly grouped as DOD ISS, platform IT (PIT), IT services, and IT products.

The RMF has the following characteristics:

- Promotes the concept of ongoing risk management and ongoing IS authorization through the implementation of continuous monitoring processes.
- Encourages the use of automation to provide senior leaders the information necessary to make cost-effective, risk-based decisions with regard to the organizational IS supporting their core missions and business functions.
- More fully integrates information security into the enterprise architecture and system-development lifecycle.
- Promotes reciprocity and reuse of test results and assessment documentation as the norm, thus saving time and resources while enhancing interoperability.
- Links risk-management processes at the IS level to risk-management processes at the organization level through a risk executive (function).
- Establishes responsibility and accountability for security controls deployed within organizational IS and inherited by those systems (that is, common controls).



RMF Steps

1. Categorize the IS and the information processed, stored, and transmitted by that system based on an impact analysis.
2. Select an initial set of baseline security controls for the IS based on the security categorization, tailoring and supplementing the security-control baseline as needed based on an organizational risk assessment and local conditions.
3. Implement the security controls and describe how the controls are employed within the IS and its environment of operation.
4. Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements of the system.
5. Authorize IS operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from operating the IS and the decision that this risk is acceptable.
6. Monitor the security controls in the IS on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.



Introduction to RMF Governance

The DOD RMF governance structure implements the three-tiered approach to cybersecurity-risk management described in National Institute of Standards and Technology Special Publication (NIST SP) 800-39, synchronizes and integrates RMF activities across all phases of the IT lifecycle, and spans logical and organizational entities. The three tiers are—

- Tier 1—Organizational
- Tier 2—Mission/Business Processes
- Tier 3—IS and PIT Systems

RMF Roles

The RMF team is responsible for implementing the RMF for a specific DOD IS or PIT system. Personnel assuming RMF roles must qualify for and be assigned to positions on the RMF team and will be listed in the security plan. The RMF team includes the following:

- Chief Information Officer
- Senior Information Security Officer
- Authorizing Official
- Authorizing Official Designated Representative
- Security Control Assessor
- Information System Owner
- Program Manager/System Manager
- Information System Security Manager
- Information System Security Officer
- User Representative

More detailed information about the RMF team can be found in NIST SP 800-37, appendix D.