

# How to Apply the Risk Management Framework to Control Systems within DoD



**Mr. Kevin Dulany, CISSP, CISM, CISA, CAP**  
Chair, RMF TAG, Department of Defense (DOD) Chief  
Information Officer (CIO)  
Deputy CIO for Cybersecurity  
Cybersecurity Policy & Strategy Directorate



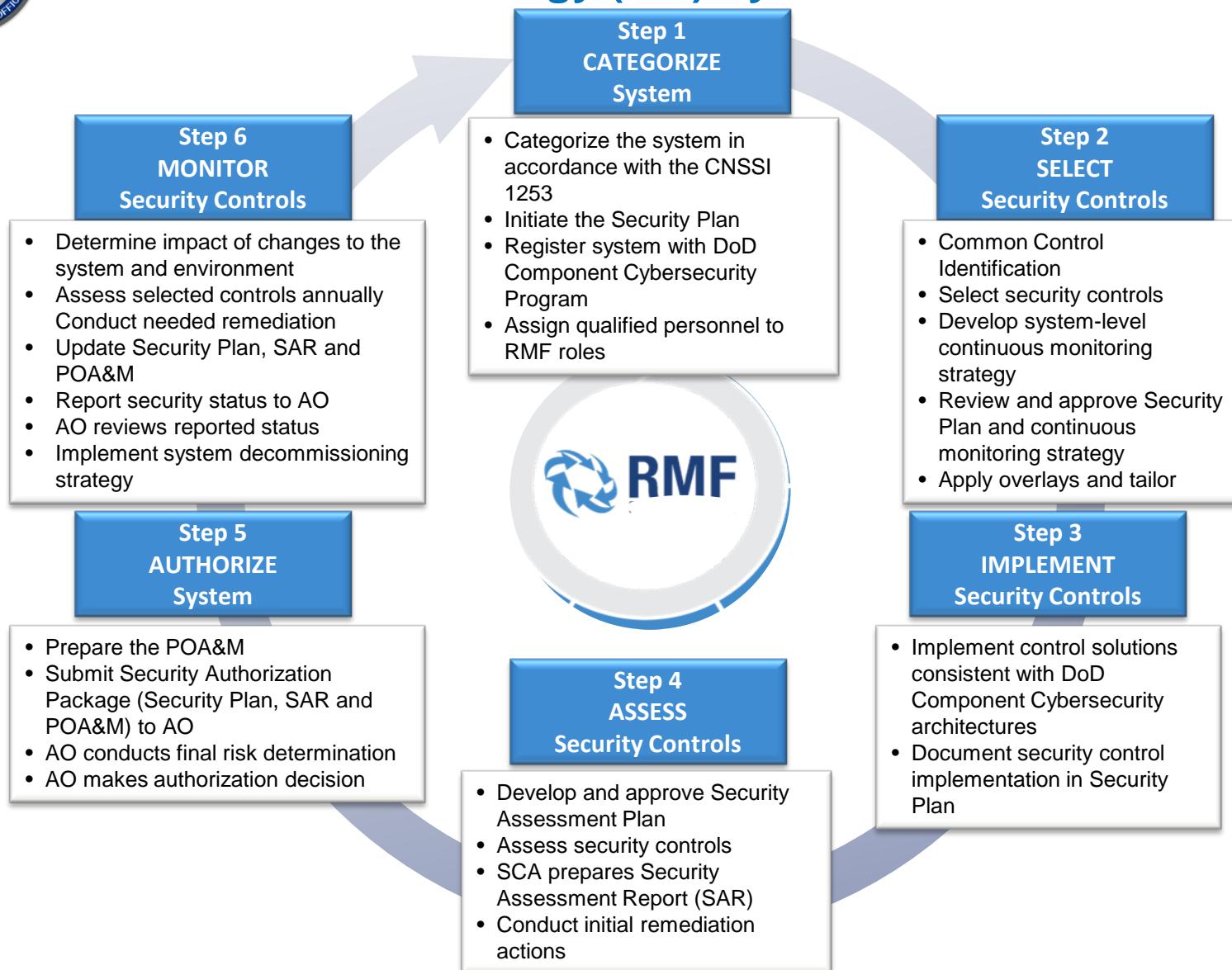


## DoDI 8510.01 “RMF for DoD IT”

- Incorporates **cybersecurity** early and robustly in the **acquisition** and system development lifecycle
- Implements a **three-tiered approach to risk management** that addresses risk-related concerns at the enterprise level, the mission and business process level, and the information system level
- Focuses on **risk to the mission** and buying down **cybersecurity risks** through the right mitigations
- Provides a **risk management methodology** that gives organizations a true picture of vulnerabilities caused by non-compliant controls as it relates to other risk factors (i.e. likelihood, threat, and impact)
- **Codifies** system authorization **reciprocity**, enabling organizations to accept approvals by other organizations for interconnection or reuse of IT without retesting
- Emphasizes **information security continuous monitoring** and timely correction of deficiencies, including active management of vulnerability and incidents
- **Applies to all IT** which reduces exploitation of vulnerabilities in PIT, Services, or Products previously not secured or assessed



# RMF Lifecycle for DoD Information Systems and Platform Information Technology (PIT) Systems





# Challenges and Solutions

- **Challenges:**
  - How to assess non-traditional IT
  - Integrating current security requirements and performing a gap analysis
- **Solutions:**
  - Establishment of guidance through the RMF KS (e.g., EI&E PIT Control Systems page)
  - Establishment of focus groups to address: defining the process for DoD IT that is designated as "Assess Only" and cybersecurity of DoD PIT systems



**Mr. Kevin M. Dulany**  
**Chief, Risk Management Framework Division**  
DOD CIO, DCIO(CS), CSPS  
[Kevin.M.Dulany.civ@mail.mil](mailto:Kevin.M.Dulany.civ@mail.mil)

**Email RMF Implementation Questions to:**

RMF TAG Secretariat ([OSD.RMFTAG-Secretariat@mail.mil](mailto:OSD.RMFTAG-Secretariat@mail.mil)) or  
via the RMF KS Help and Feedback Form (<https://rmfks.osd.mil>)



# BACK-UP



# DIACAP / RMF Knowledge Service

The authoritative source for information, guidance, procedures, and templates on how to execute the DIACAP and Risk Management Framework

The screenshot shows the DIACAP Knowledge Service homepage. At the top, there's a navigation bar with links for 'Governing Policy', 'Implementation Guidance', 'Collaboration', and 'Site Resources'. Below the navigation is a search bar. The main content area features a 'Welcome to the DIACAP Knowledge Service' message, a 'C&A News' section with a note that there are no items to show, and a 'Most Viewed Pages' list. The 'Most Viewed Pages' list includes links to 'IA Controls', 'IA Controls Explorer', 'Security Controls Explorer', 'Reference Library', 'DODACAP Activities', 'Implementation Guidance', 'DODACAP to Risk Management Framework Transformation', 'Complete List of 8900.2 IA Controls', and 'HAC (E-Classified) IA Controls'. At the bottom of the page, there's a 'Resources' sidebar with links to 'Acronyms', 'Glossary', and 'References', and a 'Roadmap' section with a 'Step by Step Execution' diagram. A large green arrow points from the DIACAP site to the RMF site.

The screenshot shows the RMF Knowledge Service homepage. At the top, there's a navigation bar with links for 'RMF General', 'RMF Implementation Steps', 'Policy & Guidance', 'Collaboration', and 'Site Resources'. Below the navigation is a search bar. The main content area features a 'Welcome to the RMF Knowledge Service' message, a 'RMF Knowledge Service' section, and an 'Announcements' section. The 'Announcements' section lists three items: 'Title : DoD Cybersecurity Culture and Compliance Initiative (1)', 'Title : "New" DoD RMF Authorizing Official (AO) Training Course (1)', and 'Title : \*NEW\* DoD CIO Official RMF Transformation Briefing (1)'. On the right side, there's a sidebar with links to 'Acronyms', 'Glossary', and 'Page Links', and a note to 'Click to view page updates'. A large green arrow points from the DIACAP site to the RMF site.

<https://rmfks.osd.mil>



# RMF Technical Advisory Group (RMF TAG)

- Mission: Strengthen and evolve the ability for DoD to rapidly deploy secure IT systems that enable information sharing between the Department, the IC, and other entities.
- Duties:
  - Provide implementation guidance for the RMF
  - Provide detailed analysis and authoring support for the enterprise portion of the Knowledge Service (KS)
  - Recommend changes to security controls, baselines, and RMF policy
  - Advise DoD forums established to resolve RMF priorities and cross-cutting issues
  - Develop and manage RMF automation requirements
- Chair: DoD SISO appointed
- Members: All DoD Components are authorized to be represented by one primary and one alternate cybersecurity SME.