From DIACAP to RMF

A Clear Path to a New Framework

Major Henry R. Salmans III, USMC, Retired
Andrew C. Tebbe, MCICOM, USMC
William J. Witbrod, Computing Technologies, Inc.

Abstract. Department of Defense Instruction (DoDI) 8510.01, dated March 12, 2014, announced the adoption of the Risk Management Framework (RMF) for Department of Defense (DoD) Information Technology. The National Institute of Standards and Technology (NIST) Special Publication 800-39 fully articulates the RMF process which is a key input into DoDI 8510.01.
This article highlights what the transition from Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) to "the RMF" means to Marine Corps "Information Assurance" and the DoD community at large[1]

"Speed of action in cyberspace is critical to maintaining the advantage against adversaries and disruptions to service. Processes must be in place to facilitate this speed of action to allow for operational commander's mission needs while balancing security. The adoption of RMF hopefully further streamlines the critical accreditation of systems. One objective being to give commanders an ability to manage risk in cyberspace in a way that makes sense as in other warfighting domains."
-Colonel David W. McMorries (former Commanding Officer, Marine Corps Network Operations and Security Center)

RMF Transition

The DoD transition to the RMF is an evolution in the DoD Cybersecurity[2] program to address the changing risk to information systems. RMF is a Federal standard and DoD's adoption of it will enable greater interoperability, knowledge sharing, and reciprocity across the Federal government. Using a more robust system lifecycle approach for risk assessment, along with a more scrutinized continuous monitoring program, the Marine Corps can react more quickly and efficiently to changes within our Cyber environments. The RMF better aligns the DoD Cybersecurity language and practices with guidance provided by the National Institute of Standards and Technology (NIST) consistent for Federal information systems.

Although guidance from the Marine Corps regarding the transition to the RMF has not been released, the DoD has begun to update key instructions related to Cybersecurity under the RMF as presented in Table 1.

Figure 1 illustrates external publications used as the basis for the revised Cybersecurity Instructions.

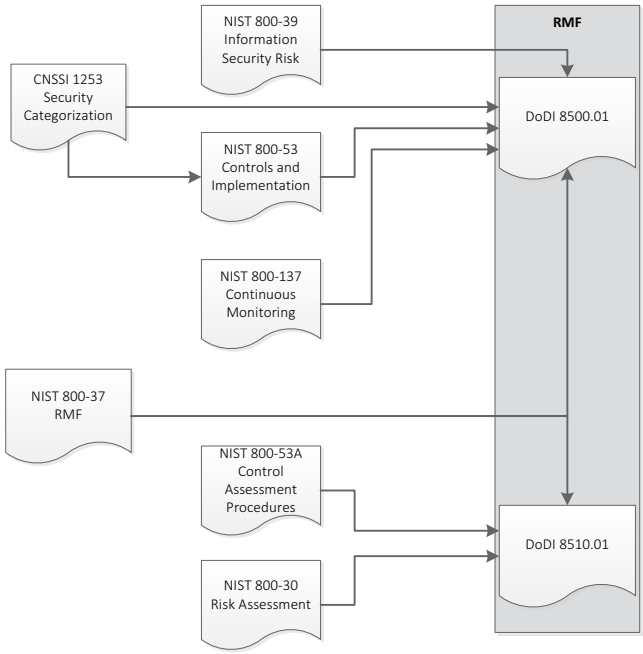


Figure 1: DoDI Publication Dependencies[4]

The Knowledge Service Website[5], managed by the Department of the Navy for DIACAP, will be updated to reflect the transition to the RMF. The updated site serves as the authoritative source on guidance for implementing and executing the RMF according to the DoD Instructions and includes tools and templates for RMF execution and production of key artifacts.

Changes in Framework

Both DIACAP and RMF seek to identify and manage information system (IS) risks associated with system vulnerabilities and adversary threats. Vulnerabilities primarily consist of weak IS security procedures or internal controls. Threats exploit those vulnerabilities and include environmental disruptions, system or human errors, as well as purposeful attacks. The goal of both DIACAP and RMF is to mitigate vulnerabilities to an acceptable level of risk. Cybersecurity experts and practitioners transitioning from DIACAP will appreciate that the shared goal of risk management is equally true under RMF. Their knowledge and expertise, accrued under the previous framework, will be useful if not critical to the transition to this new paradigm.

Terminology

DoDI 8500.01 adopts the term "cybersecurity" throughout the DoD replacing "Information Assurance". The traditionally used Certification & Accreditation (C&A) process will be referred to

DoDI	Title	Reissue Date
8510.01	*Risk Management Framework (RMF) for DOD Information Technology*	03/12/2014
8500.01	*Cybersecurity*[3]	03/14/2014

Table 1: RMF DoD Instructions

as Assessment & Authorization (A&A) under RMF. Cybersecurity role titles have been changed, and in some cases responsibilities combined or divided among roles as presented in Table 2.

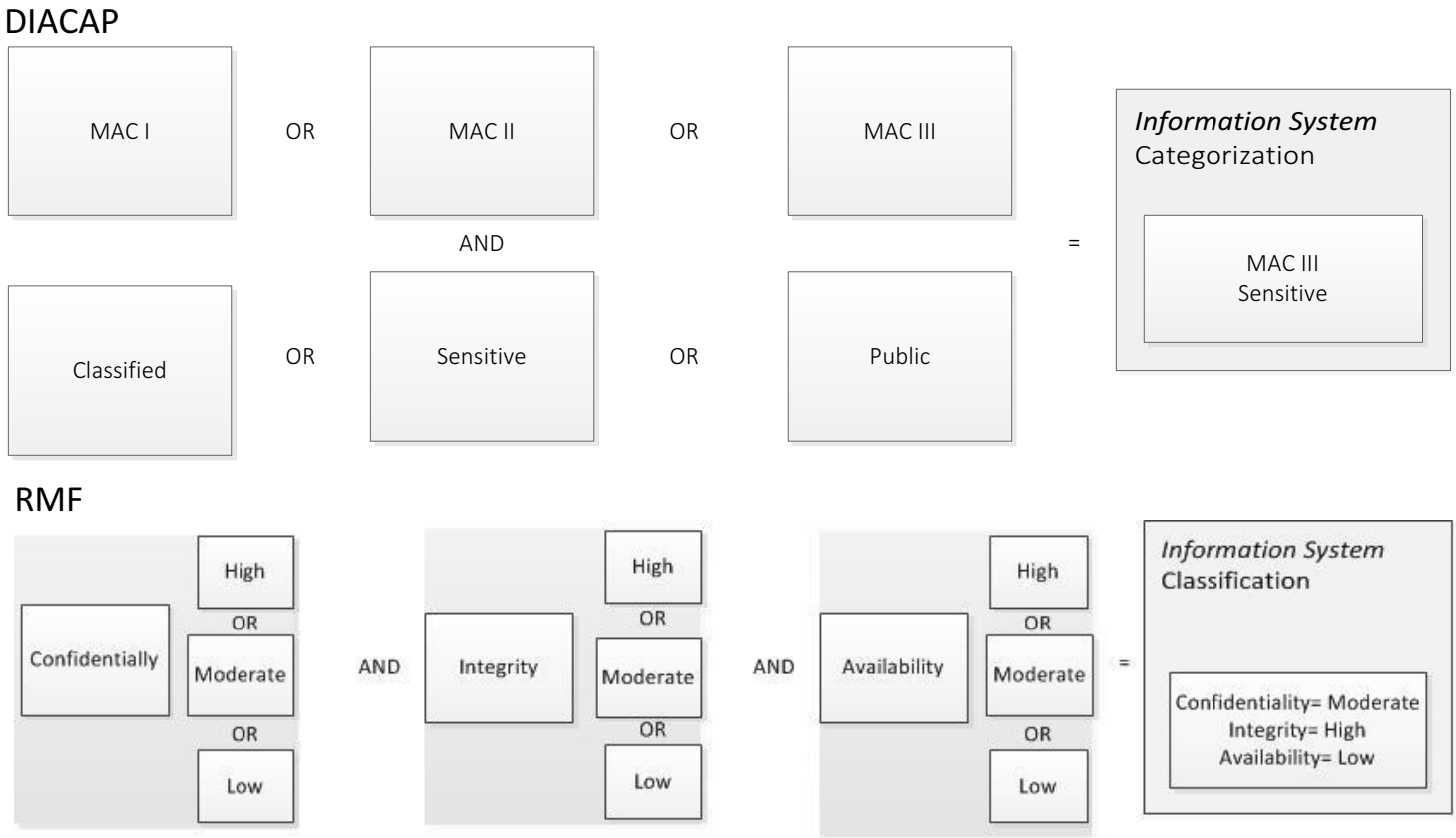
Security Controls

Security Controls, the cornerstone of any Cybersecurity program, conform to a new set of features and requirements for the RMF. Similar to the function of DoDI 8500.2 under DIACAP, the security control descriptions under the RMF are found in NIST Special Publication (SP) 800-53 (at time of this writing the publication was under Revision 4). The security controls within the publications that an IS is required to adhere to depends on the system categorization.

The process for determining an IS's Categorization has changed under RMF. DIACAP uses Mission Assurance Category levels (MAC I, II, III) to define the requirements for availability and integrity. The Classification Level (Classified, Sensitive, or Public) determines the confidentiality requirements. The combination of one MAC level AND one Classification level results in the IS's Categorization (i.e. MAC III, Sensitive). The RMF provides an evaluation of the three security objectives, Confidentiality, Integrity, and Availability individually and an impact level (Low, Moderate, or High) is assigned to each objective (i.e. Confidentiality= Moderate; Integrity= High; Availability= Low). The impact is based on what affect a realized threat will have on the system. The Committee on National Security Systems Instruction (CNSSI) No. 1253 directs the RMF system categorization.

DIACAP Role	RMF Role
DoD Chief Information Officer (CIO)	DoD Chief Information Officer (CIO)
Principal Accrediting Authority (PAA)	Principal Authorization Official (PAO)
DoD Component CIO	DoD Component CIO
Senior Information Assurance Officer (SIAO)	Senior Information Security Officer (SISO)
Principal Accrediting Authority (PAA) & Designated Accrediting Authority (DAA)[6]	Authorizing Official (AO)
Program Manager (PM)/ Systems Manager (SM)	Program Manager (PM)/ Systems Manager (SM) or Information System Owner (ISO)
Information Assurance Manager (IAM) & Information Assurance Officer (IAO)	Information System Security Manager (ISSM)
Information Assurance Manager (IAM) & Information Assurance Officer (IAO)	Information System Security Officer (ISSO)
Certifying Authority (CA) & Validator	Security Control Assessor (SCA)

Table 2: Security Roles Terminology Change



Figures 2a and 2b: DIACAP and RMF System Categorization

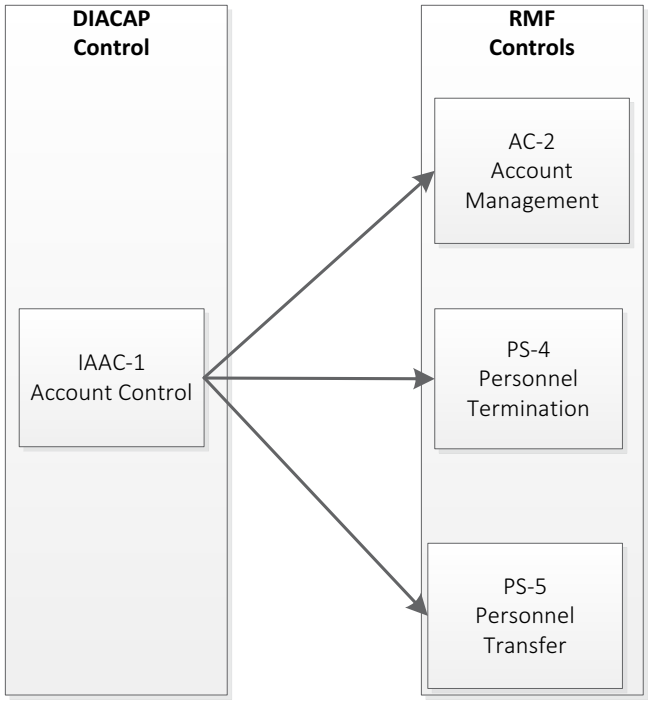


Figure 3: Example of control requirement granularity change from DIACAP to RMF

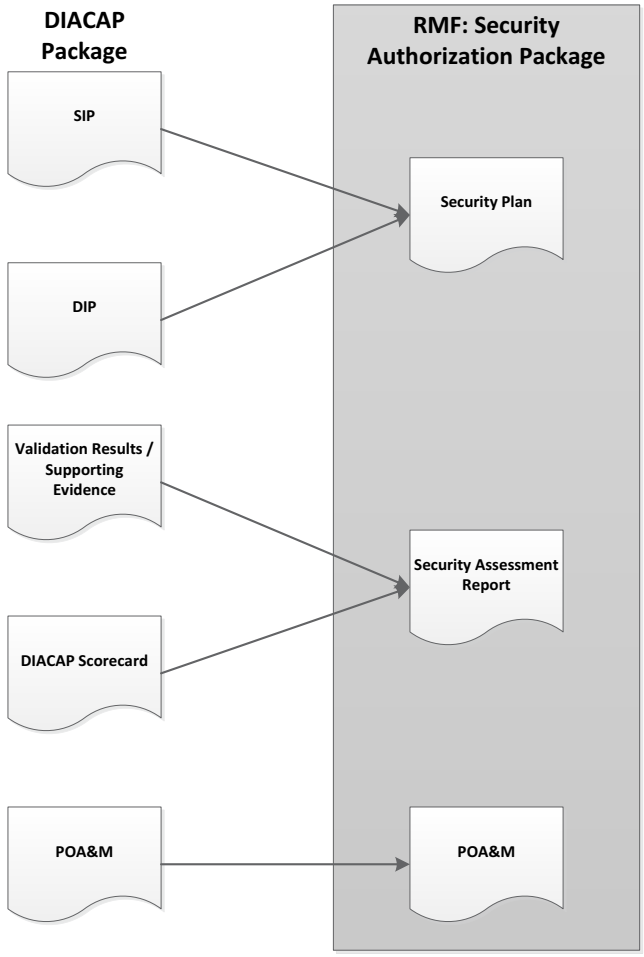


Figure 4: Artifact Transition DIACAP to RMF

A pronounced distinction between the DoDI 8500.2 catalog and NIST SP 800-53 is that it defines controls to mitigate risk in more detail. As a result, the IS's under the RMF have more controls required in order to meet the more well defined security requirements. In many cases the IS's could require triple the amount of controls under the RMF methodology. For example, the security requirements covered in DIACAP control, "Account Control" (IAAC-1), maps to multiple 800-53 controls, "Account Management" (AC-2), "Personnel Termination" (PS-4), and "Personnel Transfer" PS-5, as shown in Figure 3.

Although the number of required controls increases under RMF, because they are written at a more granular level, that does not signify an increased workload. The reality is that the overall security requirements are consistent between the two frameworks.

Artifacts

RMF reduces the artifact generation and submission process by removing the need for two separate package submissions. Under the RMF, artifacts have been streamlined leaving only one package per IS (not a Comprehensive and Executive package as with DIACAP). The three required artifacts under the RMF are the Security Plan, Security Assessment Report, and the Plan of Action and Milestones (POA&M). The relationship between the DIACAP Package artifacts and the RMF Security Authorization Package artifacts is illustrated in Figure 4.

Note that under the DIACAP model, while not required, it was common for an organization to have a formalized Security Plan at the discretion of the ISSM/ISSO. For the Cybersecurity teams developing a program under the RMF, the Security Plan is the cornerstone artifact in the program.

The Security Plan[7] provides an overview of the system, its security requirements and details the security controls in place.

"The fact that the Security Plan is the cornerstone of the RMF effort is an improvement over the DIACAP model. We needed to streamline this process and will need to evaluate how well the RMF works over time to see if we have it right. Just like we need continuous monitoring of our security efforts, we also need a periodic evaluation of our processes to ensure they are simple, understandable and executable. The security of our data systems is a daily battle that requires agile processes to meet the ever-changing cybersecurity demands." -Colonel Gregory T Breazile (Director, Cyber & Electronic Warfare Integration Division)

Continuous Monitoring

A component within the Security Plan receiving a new emphasis under the RMF is the Continuous Monitoring Strategy (CMS). CMS provides system-level strategy for evaluating the effectiveness of security controls and the observing of any changes to the system and environment. The strategy includes a plan for the annual assessments of implemented security controls.

The "assessor" must be independent of the IS requiring an external party to the organization not affiliated with either the control design or control execution. Other control elements implemented under the CMS may vary depending on the risk factors of the IS and the discretion of the ISSM.

Figure 5, illustrates three example elements of a CMS. Executing the CMS becomes critical under the RMF between the Authority to Operate (ATO) granted and expiration dates.

Along with the Security Plan, the CMS will be scrutinized and approved by the AO prior to proceeding further with the RMF. This new scrutiny, early in the RMF, further emphasizes the enhanced focus of the organization's continuous monitoring processes and the importance of identifying and coordinating resources needed to adequately execute the CMS.

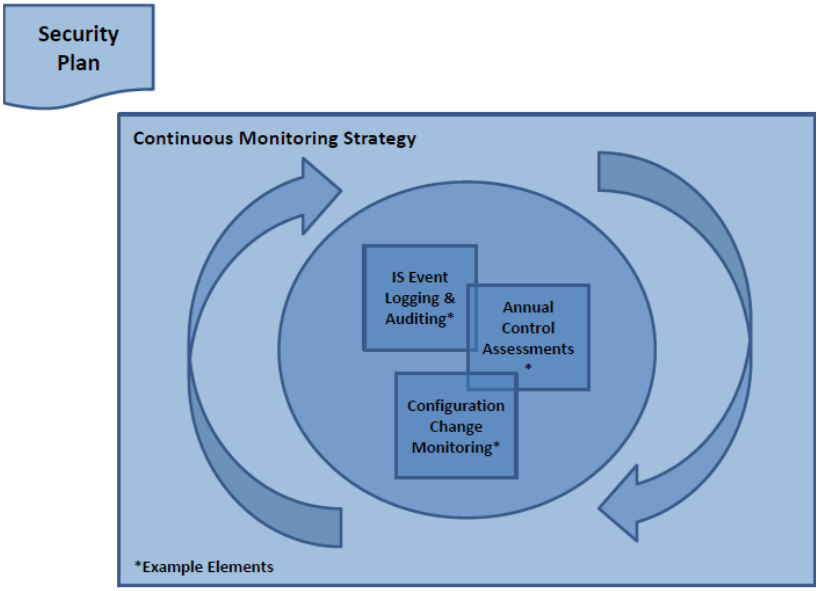
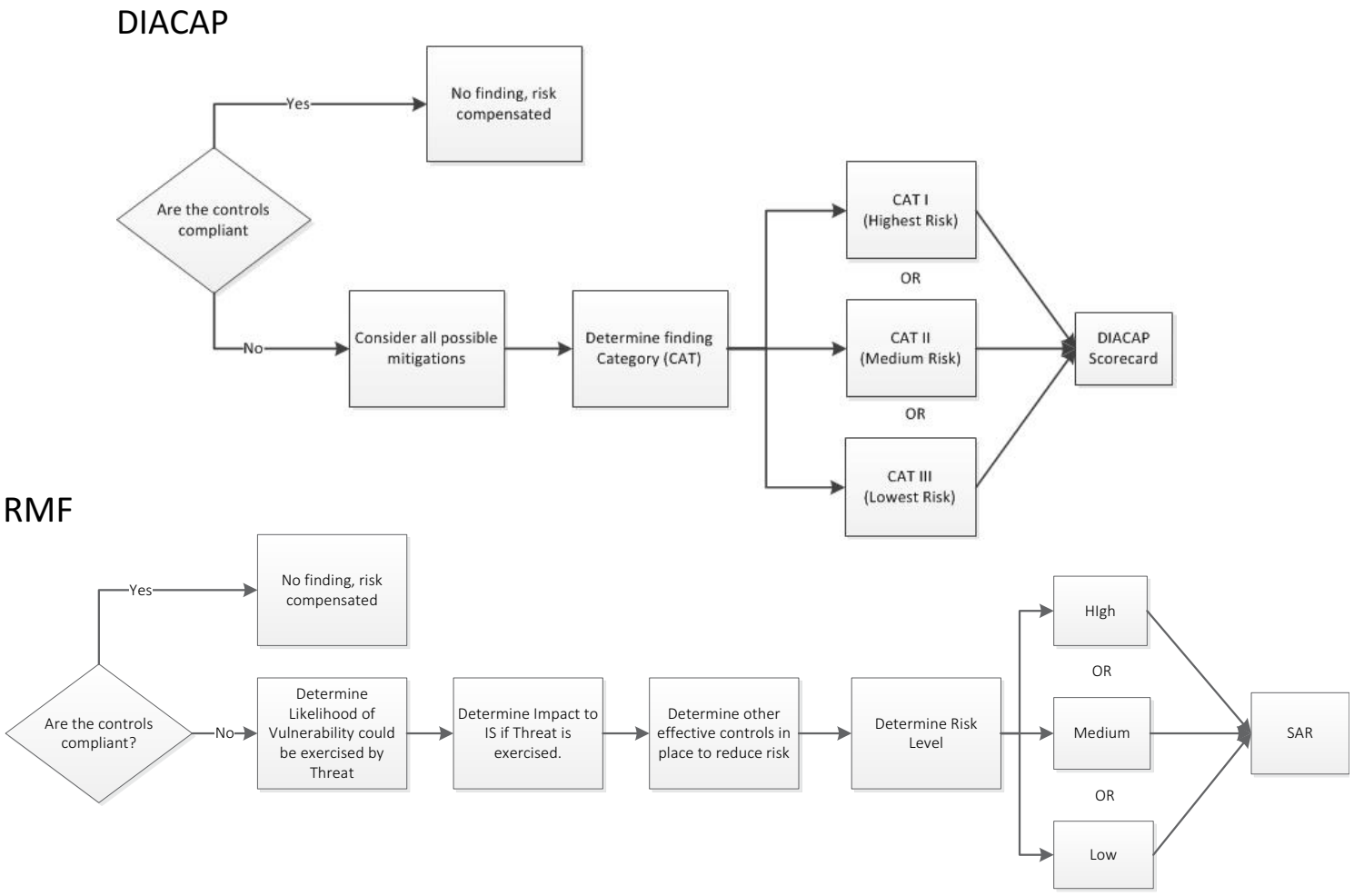


Figure 5: Continuous Monitoring Strategy with Example Elements.

Security Assessment Report and POA&M

The Security Control Assessor (SCA) develops a plan for executing the Security Assessment, in order to populate the Security Assessment Report. The Security Assessor's role and the security assessment serve the same purposes as the Validator and validation process did within DIACAP. As in DIACAP every non-compliant control will have an associated risk level.

The DIACAP risk Categories (CAT I, CAT II, and CAT III) have been replaced in the RMF with the Security Assessor's evaluation of several factors determining the risk level. The risk level factor determination includes an analysis of the vulnerabilities caused by non-compliant controls and the threats that could exploit the vulnerabilities. Figure 6 presents the evaluation of non-compliant controls, different risk designations between DIACAP and RMF, and where these risk designations are recorded.



Figures 6a and 6b: Non-compliant risk determinations

The Validator captures non-compliant controls and risk determinations in the DIACAP Scorecard. Conversely, the SCA documents these results within the RMF's Security Assessment Report (SAR). Both the DIACAP Scorecard and the RMF SAR include an assessment of the overall system level of risk as well and both are required artifacts for an ATO decision.

In the same manner as the Test Plan findings in DIACAP, any non-compliant controls from the RMF's SAR carry in to the POA&M. The POA&M is a key artifact in the authorization package and the submitter maintains it throughout the system lifecycle.

Authorization Decision

The ISSM submits the Security Authorization Package, containing the Security Plan, SAR, and POA&M, to the AO for an authorization decision only when all three of these artifacts are complete. Figure 7 shows the logical progression of these artifacts, highlighting that the POA&M cannot be generated without the SAR which is dependent on the Security Plan.

Figure 7: RMF Security Authorization Package Contents

Upon review by the AO, the authorization decision is codified as an Authorization To Operate (ATO), an Interim Authorization to Test (IATT), or a Denial of Authorization to Operate (DATO). IATTs should only be granted when an operational environment or live data is required to complete specific test objectives. IATT should normally expire in 90 days. Unlike DIACAP, RMF does not technically allow for an Interim Authority to Operation (IATO). RMF relies on the convention of issuing an "ATO with conditions" which must be met within a defined period of time. If those conditions are not met the AO may issue a DATO.

Reciprocity

An important design of the RMF is to improve efficiencies through reciprocity. Although the DoD branches followed common processes under DIACAP, the reissuance of DoDI 8510.01 for RMF provides explicit guidance on "reciprocity" that was formerly not as clear. Specifically, the guidance addresses coordination between deploying ISOs and PMs with receiving ISOs and PMs throughout the system development and the process for a receiving organization to accept an ATO. Ultimately, reciprocity increases transparency ensuring that AOs are equipped to make better informed decisions when accepting an existing ATO.

The transition to RMF enables reciprocity between the DoD and other Federal agencies. As stated above, the RMF will adhere to the security requirements under NIST 800-53 which is used as the Federal Government's common guidance for implementing security controls.

Conclusion

The transition to the RMF allows the Marine Corps to adopt a framework that dynamically responds to changes in risk. The RMF aligns itself with NIST publications that remain current in the face of emerging technologies. Ultimately, the RMF gives the Marine Corps a Cybersecurity program that is better designed to support the evolving Information Technology landscape.

Disclaimer

The views expressed are of the authors and do not represent any official position within the Department of Defense or the United States Marine Corps.

Acknowledgement

The authors would like to acknowledge LtCol Jeffrey Hammond (USMC), LtCol Michael Cho (USMC, Ret.), LtCol Floyd Means (USMC, Ret.) Marine Corps Information Technology Center Site Director, Captain Richard Wolferd (USMC) and Mr. James Klanke (President Global Project Management Group, Ltd.), and Dr. Jim Lee (Deputy Cyber Engineering, Marine Corps Systems Command) for their constructive criticism, comment, and review. Any errors remain the responsibility of the authors.

NOTES

1. Though written in the context of the DoD's adoption of RMF, the authors day to day work interactions are in direct support of the USMC and the nuances in this article may reflect or be biased toward that relationship.
2. Cybersecurity as opposed to Cyber Security is the parlance found in DoDI 8500.01; both terms are used interchangeably in many of the resources we reviewed.
3. Incorporates and cancels DoDI 8500.02, DoDD C-5200.19, DoDI 8552.01, et al.
4. This is a corrected diagram. The original reviewed for this paper shows DoDI 8500.02 as a publication applicable to RMF. It should also be noted that CNSSI 1253 is dependent on NIST 800-53, however under RMF, CNSSI 1253 guidance must be evaluated first prior to utilizing NIST 800-53.
5. At the time this article was written, the RMF Knowledge Service Website was still under development. Proposed URL is <https://rmfks.osd.mil>
6. The Marine Corps has already adopted the AO, ISSM and ISSO roles rather than using the DoD DIACAP terminology of PAA/DAA, IAM and IAO, respectively. The intention of this table is to be consistent with the DoDI for both DIACAP and RMF as a specific directive from the Marine Corps for RMF has yet to be released.
7. The RMF 'Security Plan' acts as a "road map" that guides reviewers to other important risk management and security design procedures such as the risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, configuration management plan, and incident response plan. Once established, the Security Plan continues to be a dynamic document updated as needed to remain current, presenting an accurate picture of the ever evolving risk within the environment.

ABOUT THE AUTHORS

Major Henry R. Salmans III (USMC, Retired) of CSC is a former 4002/0602 Data Systems Officer/Communications Officer. His award winning work includes From Technological Triage To Maturing A Collaborative Environment (DoD International Command & Control Research and Technology Symposium), The American Way of War (War On The Rocks) and is an occasional guest writer for Ranger Up and the infamous Rhino Den. Currently, he advises the Technology Services Organization and the Cybersecurity Council of the Marine Corps Information Technology Center in Kansas City, Missouri.
Phone: 785-840-7066
Email: henryrsalmansiii@gmail.com

Mr. Andrew C. Tebbe, formerly of COmputing TechnologieS, Inc. (CoTs), is a civilian cybersecurity professional with the Marine Corps Installation Command (MCICOM) in Kansas City, Missouri, specializing in cybersecurity compliance and control assessment. Prior to joining MCICOM, he worked as an internal auditor for the USDA focusing on FISMA and FedRAMP compliance. As an IT security control auditor and consultant, Mr. Tebbe's private sector experience was with the public accounting firm KPMG LLP, the U.S. member of the International Cooperative.
Phone: 816-541-8848
Email: andrew.tebbe@mcw.usmc.mil

Mr. William J. Witbrod of COmputing TechnologieS, Inc. (CoTs) is a Fully Qualified Navy & Marine Corps Validator working for Installations & Logistics, Headquarters Marine Corps, for the Marine Corps Installation Command, Facilities Systems Branch in Kansas City, Missouri. Prior to joining CoTs in support of CSC, William served in the United States Army Signal Corps and held various executive security and audit positions in both the government and private sectors.
Phone: 913-244-4600
Email: witbrod@gmail.com