Risk Management Framework

THE CHALLENGE

CSCI is responsible for the Information Assurance (IA) on numerous Unclassified, Sensitive but Unclassified, Classified, and Compartmented Information Systems (IS). Through participation in Department of Defense (DoD)-sponsored working groups starting in 2013, CSCI IA professionals recognized that the Certification and Accreditation (C&A) processes currently utilized under Director of Central Intelligence Directive (DCID) 6/3, Joint DoD Intelligence Information System (JDoDIIS), DoD Information Assurance Certification and Accreditation Process (DIACAP), and National Industrial Security Program Operating Manual (NISPOM) were going to transition to a Risk Management Framework (RMF) approach created by the National Institute of Standards and Technology (NIST).

To prepare for the continued IS Authority to Operate (ATO) accreditations to numerous corporate and government-sponsored systems, CSCI IA professionals understood the need to rapidly adapt and implement the new government-mandated RMF process.

THE STRATEGY

To meet this challenge, CSCI had to gain a fundamental understanding of the NIST's RMF implementation. CSCI analyzed the NIST 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" and the Committee on National Security Systems (CNSS) Instruction 1253 "Security Categorization and Control Selection for National Security Systems." CSCI also studied the DoD Intelligence Communities (IC) RMF implementation maintained in the DoD Joint Security Implementation Guide (DJSIG) that was approved in 2011.

CSCI Cyber Security professionals reviewed and provided input to the initial Joint Special Access Program (SAP) Implementation Guide (JSIG) RMF working group. CSCI Cyber Security professionals attended JSIG RMF training provided by the working group and participated on the Intelink Joint-Air Force-Army-Navy (JAFAN) Community Website created to assist with the transition to RMF within the SAP community.

While supporting a Top Secret (TS)/Sensitive Compartment Information (SCI)/SAP modeling and simulation environment on behalf of the Chairman of the Joint Chiefs of Staff (CJCS), CSCI Cyber Security professionals became early adopters of the RMF. Recognizing both the opportunity and challenge of transitioning from DCID 6/3 guidance to the emerging RMF guidance, CSCI was one of the first companies within the DoD community to successfully complete and submit an RMF package for a system high hybrid Linux and Windows Local Area Network (LAN).

From 2012-2018, CSCI Cyber Security Professionals have achieved the following:

- Twelve (12) Interim-Approvals-To-Test (IATT) for Marine Aviation Weapons and Tactics Squadron One's (MAWTS-1) Tactical Demonstrations (TACDEMOs)
- One (1) Conditional Authority-To-Operate (CATO) for United States Marine Corp's (USMC) Meshed Network Manager (MNM) for a Field User Evaluation (FUE)
- One (1) IATT and one (1) CATO for Defense Advanced Research Projects Agency (DARPA) for RadioMap
- Two (2) IATTs for United States Navy's (USN) Trident Warrior 2015 & 2017
- One (1) IATT for Naval Research Lab's (NRL) Automated Tactical Optical Line of sight Links (ATOLL) for a FUE at Marine Expeditionary Force Exercise (MEFEX) 18 and One (1) CATO for 3rd Marine Expeditionary Force (MEF)

THE RESULTS

CSCI had previously supported multiple information systems throughout the DoD that were based on legacy C&A processes defined in the DCID 6/3, JDoDIIS, DIACAP, and the NISPOM. The knowledge gained supporting DoD customers in different environments and early participation in RMF policy development and training prepared CSCI Cyber Security professionals to meet the challenge of developing a consistent process for adapting to the RMF for IS authorization and monitoring. Their approach has been successfully reviewed and evaluated by multiple DoD entities including the DoD SAP Central Office (SAPCO), USN CSD, United States Marine Corps (USMC) C4 Cyber Security Division, and Office of the Designated Approving Authority (ODAA) Defense Security Service (DSS). CSCI has achieved IS Authorizations for multiple classified information systems following a strict implementation of the six steps of the RMF security lifecycle.

CSCI's involvement with the early adoption of RMF within the IC, SAP, Collateral, and Industry environments enabled the development of a professional Cyber Security workforce that is knowledgeable in the RMF processes defined in the NIST, DJSIG, JSIG, and DSS Assessment and Authorization Process Manual (DAAPM). CSCI now has a cadre of RMF-experienced cyber security professionals deployable to multiple Federal Government, DoD, or contractors to assist with the transition to RMF and the proper maintenance/monitoring of required security controls.

Copyright © 2018 Computer Systems Center Incorporated (CSCI™) – All rights reserved.
6225 Brandon Avenue, Suite 520, Springfield, VA 22150-2519.
CSCI™ is a trademark of Computer Systems Center Incorporated. All other trademarks and registered trademarks are owned by their respective companies.