Risk Management Framework (RMF) Transition Impacts in Training Simulation Systems

Graham Fleener
U.S. Army PEO STRI
Orlando, FL
graham.g.fleener@mail.mil

Marco Mayor
U.S. Army PEO STRI
Orlando, FL
marco.mayor.civ@mail.mil

Dr. Cliff Zou
University of Central Florida
Orlando, FL
czou@cs.ucf.edu

ABSTRACT

The Department of Defense (DOD) Information Assurance Certification and Accreditation Process (DIACAP) is undergoing its first transition and update since 2007. The new process is titled Risk Management Framework (RMF) and there are significant changes in the new guidance. Given the transition there are a number of implications for the training and simulation community for ensuring training systems maintain both their certification and their information security posture. Guidance for the transition has been evolving slowly with each the agencies initiating RMF implementation individually. The Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) follows Army guidance for the transition. This paper will define the formal requirements, new terminology, and discuss how the RMF risk assessment is determined. Additionally, we will capture the transition and migration of how PEO STRI will implement the Risk Management Framework. This paper will describe the tools that support the RMF implementation, such as the Knowledge Service (KS) and the Enterprise Mission Assurance Support Service (eMASS). We will describe the transition impacts for PEO STRI stakeholders such as contractors doing business with PEO STRI, system users, and Project Managers (PM). Each of the stakeholders will have unique concerns, impacts, and questions during the transition. There will be a number of challenges associated with transitioning to a new process that will be discussed. To conclude, we'll provide guidelines to help the training and simulation community make the transition to RMF.

ABOUT THE AUTHORS

Mr. Graham Fleener is the IA Manager (IAM) for Project Manager Training Devices (PM TRADE) in the U.S. Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI). Mr. Fleener served in the U.S. Marine Corps and then worked as a contractor for the Army before joining the Army Acquisition Corps as a Government employee. Mr. Fleener obtained both his Project Management Professional (PMP®) and Certified Information Systems Security Professional (CISSP®) certifications. Mr. Fleener holds a Bachelor of Science in Information Systems Technology and a Master of Science in Modeling and Simulation from the University of Central Florida.

Mr. Marco Mayor works as an Information Security Analyst for the Chief Information Office (CIO) in the U.S. Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI). Mr. Mayor worked four years as an Information Assurance Analyst and then transitioned to Government civil service as a certifier. Mr. Mayor is both Security+ and Certified Information Systems Security Professional (CISSP®) certified. He holds a Bachelor of Science in Information Technology (IT) and a Master of Science in Modeling and Simulation from the University of Central Florida.

Dr. Cliff C. Zou is an associate professor in the Department of Electrical Engineering and Computer Science, University of Central Florida. He received the PhD degree in the Department of Electrical and Computer Engineering from the University of Massachusetts, Amherst, MA, in 2005. His research interests include computer and network security, computer networking, and performance evaluation. He is a member of Association for Computing Machinery (ACM) and senior member of The Institute of Electrical and Electronics Engineers (IEEE).

Risk Management Framework (RMF) Transition Impacts in Training Simulation Systems

Graham Fleener
U.S. Army PEO STRI
Orlando, FL
graham.g.fleener@mail.mil

Marco Mayor
U.S. Army PEO STRI
Orlando, FL
marco.mayor.civ@mail.mil

Dr. Cliff Zou
University of Central Florida
Orlando, FL
czou@cs.ucf.edu

INTRODUCTION

The Department of Defense (DOD) has been following the DOD Information Assurance Certification and Accreditation Process (DIACAP) since 2007. On March 12, 2014, the DOD released guidance to supersede DIACAP. The process is now titled Risk Management Framework (RMF) for DOD Information Technology (IT) and numbered DOD Instruction 8510.01 (DOD, 2014). There are a number of changes associated with transitioning to the RMF process to include migrating from DOD security controls to National Institute of Standards and Technology (NIST) Security Controls. The transition will be an evolving process that will take place incrementally with systems currently accredited under DIACAP phased in under RMF. The training and simulation community is made up of a number of stakeholders that have unique impacts and challenges they will face with the transition to RMF. This paper will document impacts from the industry contractor, training system user, and Project Manager (PM) perspectives. To conclude, this paper will outline the evolving guidelines and best practices for understanding RMF as it is known at the date of publication.

The background of the DOD migrating from DIACAP to RMF began in an effort to consolidate and standardize information risk management for the federal government. Prior to RMF, the DOD used a unique certification and accreditation process for Information Assurance, which differed from other federal agencies. There are a number of benefits to having the entire federal government under one process (DISA, 2012). First, RMF is intended to provide a greater degree of confidence for users, to include warfighters, that the systems they are operating on a daily basis are more secure. Next, reciprocity, or the ability to leverage a previously granted authorization across agencies could be realized under a single process. Using the same security control requirements would enable a more standard approach to measuring cybersecurity risk. Additionally, this will standardize the language used for information assurance across the entire federal government. DIACAP was largely a static process with time driven milestones to include triennial reaccreditations, annual security reviews and few requirements for continuous monitoring of the security posture of a system. RMF is placing a significant emphasis on real time security. The continuous monitoring of the security posture of a system, to include reporting metrics and compliance to a higher agency, is one of the cornerstones for the transition to RMF.

There will be a number of challenges DOD wide with the transition to a new process for information security compliance. This paper will concentrate on the challenges the cyber community within the U.S. Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) will face with the transition to RMF. However, many of the challenges will not necessarily be unique to PEO STRI. Figure 1, DIACAP to RMF Transition, documents a brief snapshot of the key differences in the migration to the new process.

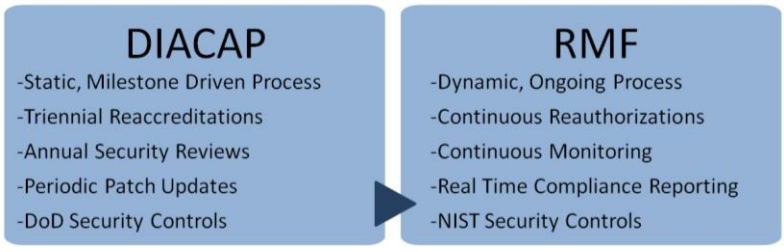

Figure 1 – DIACAP to RMF Transition

RMF REQUIREMENTS AND GUIDANCE

There are a number of significant changes that will take place with the transition from DIACAP to RMF. DIACAP required a system to perform a reaccreditation every three years, or triennially. RMF will initially continue with triennial reaccreditations, but will begin phasing in a process called continuous reauthorization (DODI 8510.01, p. 38). Continuous reauthorizations allow for a system to eliminate the formal triennial reaccreditation process as long as a number of conditions are met. Continuous monitoring and strong security compliance metrics will be paramount to obtaining a continuous reauthorization decision. Under DIACAP, periodic (typically quarterly) patch updates were a sufficient means of remaining in compliance with an Information Assurance Vulnerability Management (IAVM) Plan. With the release of RMF, the DOD is phasing in a requirement for real time reporting of patch status. The end goal of the reporting is to decrease the time between patch cycles and decrease the known vulnerability of installed systems. The next major change is moving from the DOD Instruction 8500.2 security controls to the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53 security controls. NIST SP 800-53 has a much more granular approach to security controls. Figure 2, RMF Process, below documents the RMF steps, which coincides with a system's life cycle. Figure 2 is referenced from DODI 8510.01 page 28 which further documents each step of the process.

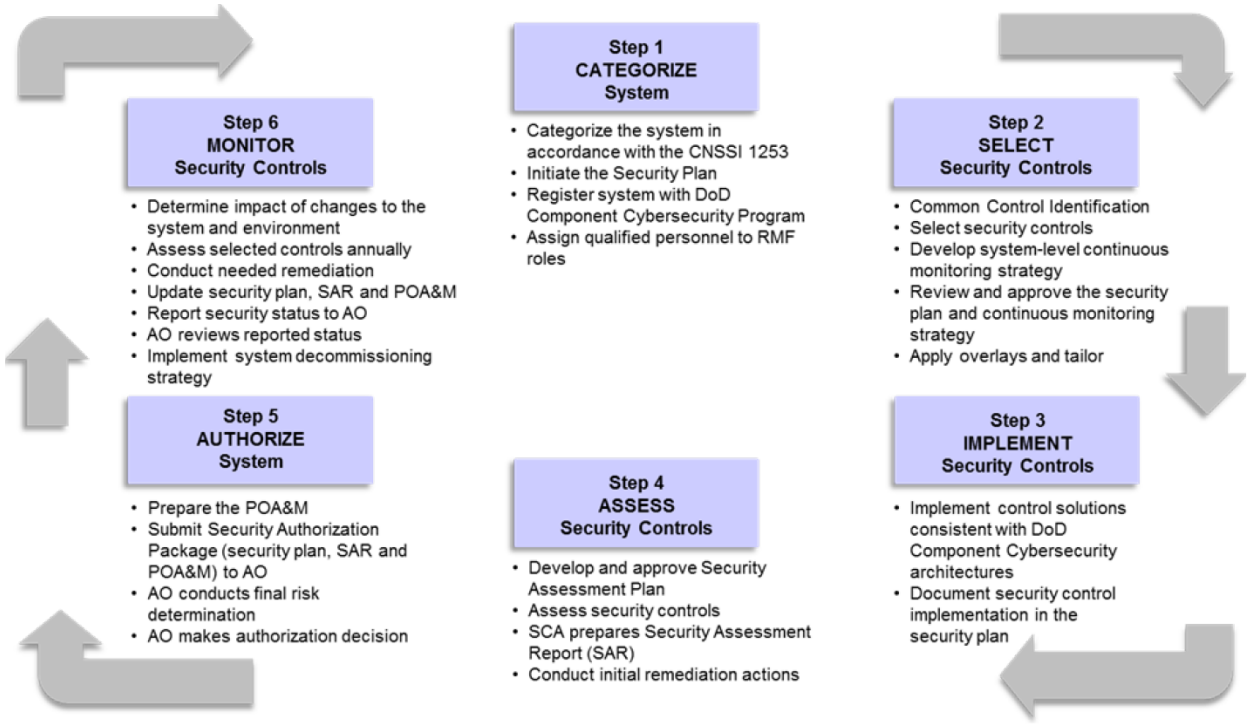

Figure 2 – RMF Process

There are a number of requirements publications associated with RMF governing policy, procedures, and technical security controls. Table 1, RMF Requirements Publications, outlines the high level guidance provided to support RMF implementation. The intent of the vast amount of guidance is to ensure agencies, contractors, and other stakeholders have the necessary information to minimize the cyber threat to systems.

Table 1 – RMF Requirements Publications

Number	Name	Summary
DODI 8500.01	Cybersecurity	Provides the foundation for establishing a DOD cybersecurity program for defense of networks, systems and information technology to include definitions of terms, security controls guidance, and enterprise governance.
DODI 8510.01	Risk Management Framework	Establishes a policy governing cybersecurity, assigns responsibilities, and details execution of the RMF process.
NIST SP 800-39	Managing Information Security Risk	Documents a program for understanding and assessing information security risk within an organization.
NIST SP 800-37	Risk Management Framework	Provides guiding principles for implementing RMF on federal information systems to ensure consistency, full integration, and more secure configuration of security controls on a system.
NIST SP 800-30	Risk Assessment	Documents a strategy for conducting risk assessments on information systems and organizations as a part of an overall risk management process.
NIST SP 800-53	Cybersecurity Controls and Enhancements	Establishes guidelines for assigning security controls for the purposes of achieving secure operations of information systems.
NIST SP 800-53A	Cybersecurity Control Assessment Procedures	Initial point for defining assessment procedures for applicable security controls for a given system.
NIST SP 800-137	Information Security Continuous Monitoring	Assists organizations in the implementation of a continuous monitoring strategy.
NIST SP 800-60	Mapping Types of Information to Security Categories	Supports organizations in the process of aligning information and information systems with the appropriate security category in a consistent manner.
NIST SP 800-160	Systems Security Engineering	Provides a comprehensive guideline of the principles and concepts of security engineering for federal information systems.
CNSSP 22	Policy on Information Assurance Risk Management Policy for National Security Systems	Serves as the requirement for establishing an organizational Information Assurance policy for National Security Systems.
CNSSI 1253	Security Categorization and Control Selection for National Security Systems	Provides a foundation for selecting and applying security controls from NIST SP 800-53 for implementation on a National Security System.
CNSSI 1253A	Implementation and Assessment Procedures	Establishes a guideline for assessing compliance with applicable security controls on a National Security System.
CNSS 4009	National Information Assurance Glossary	Documents a detailed glossary of Information Assurance related terms in an effort to minimize differences in terminology to ensure consistency and standardization.

Transition Guidance

As agencies interpret the DOD level guidance, each one is publishing transition guidance. The transition guidance PEO STRI has received is for an RMF implementation date of October, 2015.

RMF TOOLS SUPPORTING IMPLEMENTATION

Knowledge Service (KS)

The KS is a web-based resource that provides RMF users access to RMF policy and guidance on how to implement methods standards, and practices required to protect DOD systems. The KS contains the most updated guidance addressing the always-evolving security objectives and risk conditions. It provides access to security controls baselines, overlays, individual security controls and security control implementation guidance and assessment procedures. The KS website contains a library of tools, diagrams, process maps, etc. assisting users execute the RMF process. Access to the KS website (https://rmfks.osd.mil) is only available to users with a Common Access Card (CAC) or with external DOD sponsorship, for example, DOD contractors without a CAC (Department of Defense, 2014).

Enterprise Mission Assurance Support Service (eMASS)

The eMASS is also a web-based resource that automates the RMF process. It includes all the reports required by the RMF process, and it's able to generate new reports based on the user's needs. eMASS main vision is to allow users to share access to specific data in near real-time, and in a secure fashion. It integrates several capabilities, such as:

- Reporting on a system's cybersecurity compliancy
- Simplifying the RMF workflow automation.
- Standardizing the exchange of information
- Tracking systems-security engineering during the entire life cycle

Access to the eMASS website is only available to users with a Common Access Card (CAC) or with external DOD sponsorship (Department of Defense, 2014). At this time all systems for the Army must be transitioned into eMASS.

OTHER TOOLS SUPPORTING CONTINUOUS MONITORING REQUIREMENT

In the DIACAP process some compliance tools were standalone in nature. RMF instead is transitioning into more connection-dependent tools. DOD has combined three emerging security practices tasked with the sole purpose to provide training systems with near real-time IA situational awareness. These applications are the Assured Compliance Assessment Solution (ACAS), Host Based Security System (HBSS), and the Continuous Monitoring Risk Scoring (CMRS) system. These three tools all depend on one another to provide a system's accurate risk posture. The challenges users and system owners will be facing, is the ability to provide continuous data feeds in standalone or closed-restricted environments.

Assured Compliance Assessment Solution (ACAS)

The Assured Compliance Assessment Solution (ACAS) suite is provided at no cost to DOD agencies by the Defense Information System Agency (DISA). It is a scalable suite of COTS applications, which has the ability to provide automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, Security Technical Implementation Guides (STIG) compliance, and network discovery (ACAS, 2014). ACAS automates a lot of the vulnerability scanning ground work, but it is a suite that was geared towards a Global Information Grid (GIG) connected enterprise type of environment, and not a standalone/closed-restricted environment. Security professionals operating ACAS in standalone/closed-restricted environments, will have to download all the latest software updates from a connected system, and manually install them in the ACAS standalone architecture. This extra step introduces manual labor, and human error.

Host Based Security System (HBSS)

The HBSS suite is provided at no cost to DOD agencies by DISA, and it comes in the form of a pre-configured image (ePO server) and individual installation packages (all other point components). HBSS is a COTS suite of software applications which monitor, detect, and counter against acknowledged cyber-threats to systems and networks. Unlike ACAS, the HBSS solution is installed on each host (server, desktop, and laptop). HBSS is normally managed by local administrators and configured to lower intrusion risk using an Intrusion Prevention System (IPS) and a host firewall. Once installed, a manual security review is still required. (HBSS, 2014). Similar to ACAS, automated software

updates to the HBSS components depend on a connection to the GIG, adding an extra layer of complexity to security professionals administrating systems in standalone/closed-restricted environments.

Continuous Monitoring Risk Scoring (CMRS)

The CMRS suite is provided at no cost to DOD agencies by DISA. It is a web-based tool that visualizes and quantifies the cybersecurity risk of the system based on published asset inventory (provided by HBSS) and the compliance data (provided by ACAS), via a dashboard. CMRS allows users to gather decision-making information, implement prioritized mitigation decisions, and ensure effectiveness of security controls in order to support their cybersecurity risk management duties (CMRS, 2014). By using CMRS, network defenders will be able to determine if their assets are configured securely. If their configuration has changed, it will provide them with situational awareness on how to effectively apply cyber defense resources.

One of the challenges DOD faces is ensuring standalone/closed-restricted systems comply with the continuous monitoring requirement. For these types of systems, DISA proposes sneaker netting XML ACAS and HBSS feeds manually to the CMRS portal. Similar to the Vulnerability Management System (VMS) implemented in the DIACAP process, the CMRS will aggregate sensitive data, which must be accessed only by authorized users. DOD has implemented different safeguards to control access to the portal. For example, providing DOD sponsorship to authorized individuals only, and the usage of token-based technology, such as Common Access Cards (CACs).

Figure 3, Continuous Monitoring Emerging Security Practices shows the relationship between the different emerging technologies, and their corresponding users at the different levels. As shown below, the ACAS data and HBSS data is submitted to the CMRS in an XML format, and then is forwarded to the eMASS.

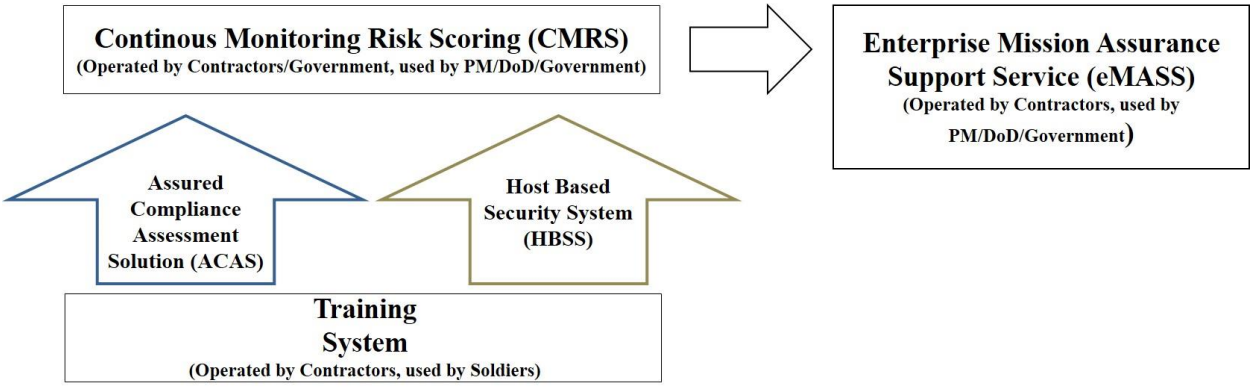

Figure 3 – Continuous Monitoring Emerging Security Practices

In the next sections, we'll be identifying the transition implications to the end-users, the DOD contractors, and members of DOD in general. Also, we'll address some of the transition implications involving technology.

The user community in most cases, is identified as the warfighters themselves who interact with these training systems. They normally train under the oversight of a DOD instructor. In other situations, the end-users are DOD contractors operating and maintaining these systems. Finally, members of DOD affected by the transition include but are not limited to the Program Management Offices (PMOs) and contractors. Their job is to ensure compliance with the continuous monitoring requirement, and security posture of the system. Figure 3, displays the roles and interaction between these three parties and the training system.

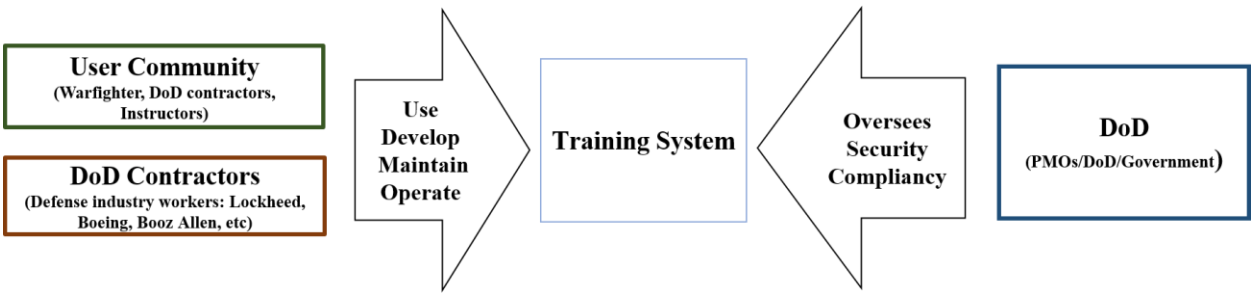

Figure 4 – Relationship between End-users, DOD Contractors and DOD

TRANSITION IMPLICATIONS FOR USERS

Privacy

Once RMF is implemented, privacy for the end-users will be affected as well. End-users will now be continuously monitored by the emerging tools mentioned in the last section. Network topologies, computer services, vulnerabilities, user accounts, and other data will now be reported by HBSS and ACAS to the CMRS. At the time this research was done, eMASS was deployed with minimal security controls protecting the need-to-know principal. In other words, all registered users have the capability of searching and viewing other organization's systems RMF information. In terms of privacy for CMRS, the overall compliancy scores are now reflected in almost real time, providing visibility to external entities such as auditors or authorizing officials. Under this new type of monitoring end-users are expected to comply with the applicable security controls. Violations and deviations will be tracked and reported by these tools, specifically HBSS. Similarly, the end user will lose the flexibility of keeping certain aspects of the system confidential. Previously under the DIACAP process, violations and security control deviations were only evident to the system owner.

Risk Scoring

The risk scoring capability will provide compliancy metrics visible to auditors, senior leadership, and other entities with the respective need to know. The concern users have is the accuracy of these metrics. The legitimacy of the actual risk score is directly dependent on the accuracy of the metrics. The risk scores are computed by a number of factors. For HBSS the risk factors include timeliness of reporting data, compliance to the HBSS software baseline, current antivirus signature file, patch compliance, and STIGs rule compliance. For ACAS the risk factors include timeliness of reporting data, patch compliance, and STIGs rule compliance (CMRS, 2014). A negative finding is triggered when a system does not report to CMRS regularly due to a configuration error, a network issue, or a hardware problem. Since stand-alone systems depend on manual feeds, lack of manpower required to do these XML feed uploads will also affect the risk compliance scores adversely. These negative findings raise the risk score of the system causing the appearance of a greater risk level than may be actually be present. Conversely, the risk score may also be increased if the system is reporting false positives. A false positive occurs when the vulnerability scanning software incorrectly reports a risk on a system that is not actually present.

TRANSITION IMPLICATIONS FOR CONTRACTORS

Integration of RMF Tools in Design Phase

There are a number of considerations contractors will need to address when developing systems under the RMF process. The government will be updating Statements of Work (SOW) to ensure the requirements are defined. The implications for contractors will include implementation and integration of the previously addressed government licensed Commercial Off The Shelf (COTS) tools into a system as it is developed. Contractors will want to pay particular attention to ensure the tools are configured to allow for secure operations while maintaining overall functionality. Additionally, processes will need to be developed and documented by the development contractor to ensure the life cycle support team has the ability to maintain secure operations of the continuous monitoring and reporting COTS tools.

Proposing Work for RMF
Accurately bidding hours to support a Request For Proposal (RFP) is one of the key concerns contractors have in any new process transition. At the time of the writing of this document, the RMF transition process is still being defined. The initial documents for RMF were released on March 14, 2014. As stated earlier in the paper the agencies are implementing RMF with some level of differences making proposing for work with RMF challenging. There are a number of unknowns in the assessment and authorization process that will be addressed with time. However, system security engineering principles and concepts remain the same for the development contractor. There are additions of new tools and technologies for RMF that will need to be clearly identified in future RFPs from the government as they are phased into implementation.

Training
The DOD will be responsible to ensure that adequate RMF training and guidance materials are available to industry. One of the challenges with implementing a significant change is ensuring industry has an understanding of the processes associated with safeguarding a system under RMF guidance. At the PEO STRI level, there is anticipated to be a number of training opportunities for our industry partners as well as the government cybersecurity workforce. In addition, there are a number of private companies already providing RMF training at a cost.

TRANSITION IMPLICATIONS FOR TECHNOLOGY

More Technical Expertise and New Hardware Requirements
In the DIACAP process, users generated vulnerability reports from scanning tools like Retina, Gold Disk, and the Security Content Automation Protocol (SCAP) Compliance Checker (SCC). All three tools operated in a Windows environment, so the tools could all reside in one operating system. Some emerging tools in RMF, are implemented in different operating systems (OS), requiring cyber security professionals to have a higher level of technical experience. For example, SecurityCenter, which is part of the ACAS suite, only operates in a Red Hat Enterprise Linux (RHEL) operating system, and all the other suite components run under a Windows OS. The training requirements for these emerging tools is more extensive. The ACAS and HBSS online trainings are both 32 hours long, and they're provided by the Federal Virtual Training Environment (FedVTE).

As far as hardware specifications are concerned, both HBSS and ACAS suites require a set of minimum requirements, so that they can operate efficiently. Based on STIG requirements, end-users cannot have all the emerging tools operate on one physical device. HBSS for example, must run independently in its own physical server.

Another transition impact is the increased dependence on network connectivity. Operators will now be entering data directly onto the eMASS portal and not into separate artifacts, such as the System Identification Profile and the DIACAP Implementation Plan. The dependence on a connection to access eMASS will increment, as at the time of the research, a stand-alone version of eMASS was not available.

Risk Scoring
For near real-time risk scoring, training systems will require a network connection to the CMRS portal or at least the capability to manually import XML feeds into the CMRS portal. This poses a challenge for standalone/closed-restricted environments, because failure to report to CMRS generates a negative impact on the risk score. So designers will have implement fail-safe measures in a connected environment. A way to mitigate network interruption, may be by ensuring a network redundancy if feasible, or implement an alerting mechanism which sends the system administrator an immediate alert if this happens. Or in the case of a standalone/closed restricted environment, the system owner may have to enforce a strict policy stating the duties and responsibilities of a system administrator, including time intervals in which these XML feeds need to be manually imported.

TRANSITION IMPLICATIONS FOR DOD

There are a number of challenges included with transition to RMF for the DOD community. By DOD community we are referring to stakeholders not previously mentioned such as Government Project Managers, DOD cybersecurity workforce, and RMF certification testing teams. The challenges associated with transition implications for the DOD community include ensuring adequate training for the cybersecurity workforce, defining RMF requirements in

Request For Proposals (RFP) for upcoming acquisitions, and budgeting for any possible increases in cost resulting from RMF. DOD is developing a number of training packages available to the cybersecurity workforce. As the process matures at the agency level more training opportunities will be available for both government and industry. At the time of writing this paper, PEO STRI is incorporating RMF language in all RFPs released after May 2014. This will ensure PEO STRI remains agile to meet RMF requirements for future systems going through the acquisition process.

FUTURE WORK

There are a number of future actions and work efforts that will take place with the transition to Risk Management Framework. The initial future work effort will be to document the lessons learned from the first system to transition and perform the Risk Management Framework process. After the initial system is authorized, there will be the opportunity at the PEO STRI level to refine in any way possible at our level. Additionally, future work will see an evolution in the Risk Management Framework related tools to provide greater automation and tighter access oversight.

ACRONYMS

Acronym	Name
ACAS	Assured Compliance Assessment Solution
BAM	Basic Accreditation Manual
CAC	Common Access Card
CISSP	Certified Information Systems Security Professional
CMRS	Continuous Monitoring Risk Scoring
COTS	Commercial Off The Shelf
DIACAP	DOD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DOD	Department of Defense
EMASS	Enterprise Mission Assurance Support Service
EPO	ePolicy Orchestrator
GIG	Global Information Grid
HBSS	Host Based Security System
IAM	Information Assurance Manager
IPS	Intrusion Prevention System
IT	Information Technology
KS	Knowledge Service
NIST	National Institute of Standards and Technology
OS	Operating System
PEO STRI	Program Executive Office for Simulation, Training, and Instrumentation
PM	Project Manager
PM TRADE	Project Manager Training Devices
PMO	Program Management Office
RFP	Request For Proposal
RMF	Risk Management Framework
SCC	SCAP Compliance Checker
SP	Special Publication
STIG	Security Technical Implementation Guides
VMS	Vulnerability Management System
XML	Extensible Markup Language

REFERENCES

Defense Information Systems Agency. (2014). *ACAS.* Retrieved on February 25, 2014, from http://www.disa.mil/Services/Information-Assurance/ACAS

Defense Information Systems Agency. (2014). *ACAS Components.* Retrieved on February 26, 2014, from https://east1.deps.mil/disa/cop/mae/netops/acas/SitePages/Components.aspx

Defense Information Systems Agency. (2014). *CMRS.* Retrieved on March 15, 2014, from https://east1.deps.mil/disa/cop/mae/netops/CMRS/SitePages/Home.aspx

Defense Information Systems Agency. (2014). *HBSS.* Retrieved on February 28, 2014, from http://www.disa.mil/Services/Information-Assurance/HBSS

Defense Information Systems Agency. (2014). *HBSS Components.* Retrieved on March 16, 2014, from https://east1.deps.mil/disa/cop/mae/CyberDefense/HBSS/SitePages/Components.aspx

Department of Defense. (2014). *Risk Management Framework (RMF) for DOD Information Technology (IT) Instruction 8510.01*. Retrieved April 17, 2014 from http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

Marzigliano, Len (2011). *Goodbye DIACAP, Hello DIARMF*. Retrieved from http://resources.infosecinstitute.com/goodbye-diacap-hello-diarmf/

National Institute of Standards and Technology. (2011). *Information Security Continuous Monitoring Special Publication 800-137*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

National Institute of Standards and Technology. (2010). *Guide for Applying the Risk Management Framework to Federal Information Systems Publication 800-37*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

Defense Information Systems Agency. (2012). *DIACAP to Risk Management Framework (RMF) Transformation.*

Program Executive Office for Simulation, Training and Instrumentation (PEO STRI), (2011). *Basic Accreditation Manual (BAM).*