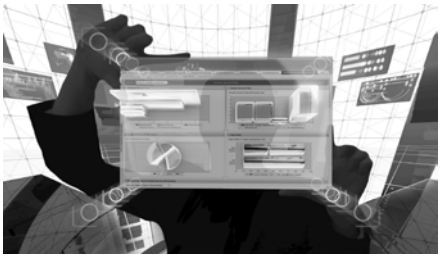
MIGRATING FROM DIACAP TO DOD RMF USING RSA ARCHER® FEDERAL SOLUTIONS



QUICK FACTS

- The DoD RMF is based on NIST RMF, defined in NIST SP 800-37.
- NIST SP 800-53 replaces DoDI 8500.2 as the security control catalog in DoD RMF.
- NIST's 800 series of Special Publications are available at http://csrc.nist.gov/publications/PubsSPs.html
- CNSSI 1253 defines the DoD RMF's most significant deviation from NIST SP 800-37: the methods for categorization and control allocation. The rest of DoD RMF follows NIST RMF very closely.
- DoD Instruction (DoDI) 8510.01 released in Mar 2014 reissues and renames prior DoD Instruction 8510.01 from Nov 2007.
- The DoD RMF provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems.

HANDOUT

INTRODUCTION

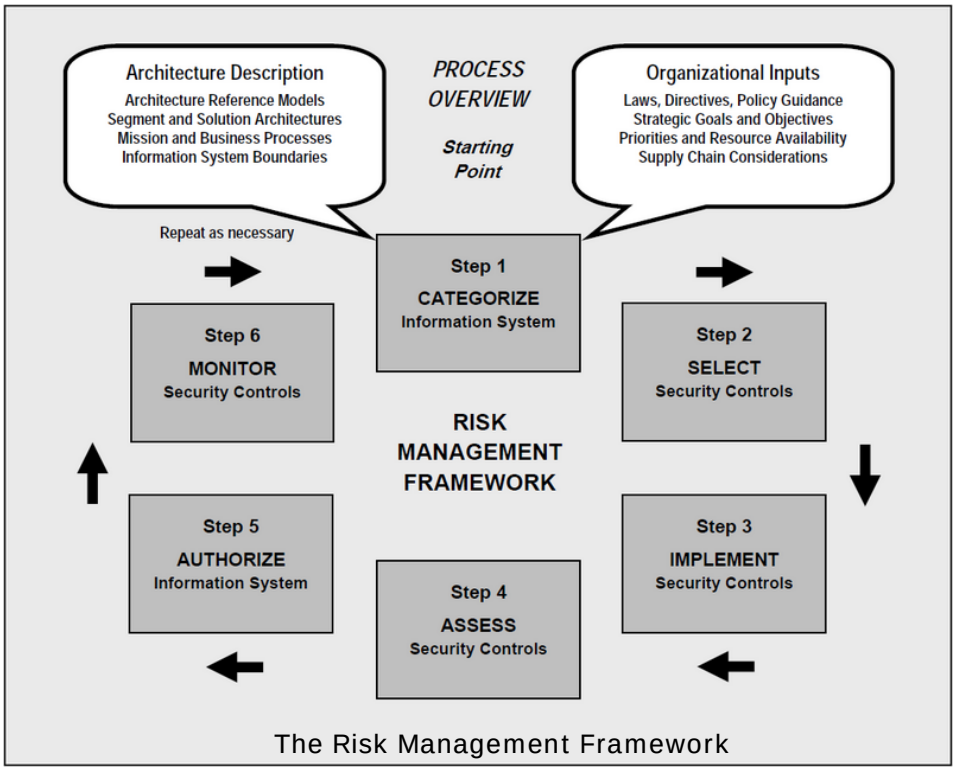
The time has finally come to migrate from DoD Information Assurance Certification and Accreditation Process (DIACAP) to the DoD Risk Management Framework (RMF). As a DoD Information Assurance (IA) professional, you might be wondering how your organization will adjust and what sorts of challenges and surprises the next few years may bring. The good news is that the processes are very similar at the foundational level and there are tools to help you minimize the stress of migration.

SIMILARITIES AND DIFFERENCES: DIACAP VS DOD RMF

The basic attributes of the information systems will still be documented in very similar ways. For example, the primary documents like the SIP/DIP and SSAA become one System Security Plan (SSP). You will also continue to use many of the same supporting documents, such as Assessment Plans and Risk Assessment Reports (RAR).

Categorize: Categorizing information systems is done in a slightly different way. Instead of defining a system by its Mission Assurance Category (MAC) and Classification Level (CL), systems now have a 3-part Security Category. Just like the MAC and CL, the Security Category is defined by each system's sensitivity and criticality based on the missions it supports and the data it stores and processes.

Select Controls: In just the same way that groups of DIACAP controls are allocated based on the MAC and CL, each Security Category in the RMF comes with a recommended "baseline" of controls which can be tailored on the individual control basis as well as enhanced by overlays, which add groups of related controls based on mission or technology.



The Risk Management Framework

RSA

EMC²

QUICK FACTS

Many of the adjustments to the RMF are minor. For example:

- Certification & Accreditation (C&A) is more often called Assessment and Authorization (A&A)
- The DAA is the Authorizing Official (AO)
- An ST&E is a control assessment or a Security Control Assessment
- The certifier/CA is the Security Control Assessor (SCA)

Implement and Assess. The final control set is implemented and documented in the same way in the RMF. When the controls are all implemented and documented, they are assessed by an independent assessor. Findings from the control assessments are managed in the same way: remediating or creating exception requests (RBDs) or Plan of Action and Milestones (POA&Ms).

Authorize. The requirements for the final authorization package are very similar: A security plan, control assessment findings, POA&Ms, and risk metrics. The Authorizing Official (OA, formerly DAA) makes authorization decision based on this package.

Overall, the process is very similar. The largest transition is around adjusting to the security categorization and control allocation processes defined in CNSSI 1253, and learning a new (and considerably larger) control catalog.

USING RSA ARCHER FEDERAL SOLUTIONS

Easy to Learn: For DoD Information Assurance professionals accustomed to DITSCAP and DIACAP, the new NIST-based RMF may be unfamiliar, and even daunting. So, first, and most importantly, the RSA Archer Assessment & Authorization (A&A) solution has an RMF workflow which is laid out in a sequential, intuitive way that is extremely easy for a new person to follow.

Streamline and Automate: The RSA Archer A&A solution will streamline and automate many RMF steps, taking answers you provide and compiling and formatting them into all of the artifacts you need to submit with your authorization package. The same answers also drive automated, behind-the-scenes risk scoring to provide unprecedented risk insight with no additional effort.

Leverage Your Existing Work: RSA Archer has many ways to ingest the current C&A/A&A data. For example: How long did it take to gather and write implementation details for all of your DoDI 8500.2 controls? These can be saved from a DIACAP authorization package and imported in to the appropriate NIST 800-53 controls in a new package via RSA Archer's Data Import feature. This will save many hours of work for each authorization package.

Accommodate Everyone: RSA Archer A&A solution supports DIACAP, NIST RMF, DoD RMF and FedRAMP. So, different types of authorization packages can be accommodated in one environment. This enables reciprocity, mixed environments, tenant systems, cloud systems, and migration between methodologies (like from DIACAP to DoD RMF). All can be managed and monitored in one place.

Leverage Other Integrated RSA Solutions: You can, for example, multiply the effectiveness of your control assessor and security administrators by augmenting the A&A solution with the RSA Archer Continuous Monitoring (CM) solution to monitor many of your technical controls. RSA Archer CM solution can also solve a large portion of the OMB Memo 14-03 CDM-planning requirements. In addition, you can also integrate the RSA Archer Business Continuity Management solution to manage disaster recovery and COOP activities. RSA offers many related Information Assurance solutions that all share the same platform & database and easily share data. As a result, you are able to expand your capabilities as you need them.

CONTACT US

To learn more about how RSA Archer Federal Solutions can help solve your information assurance challenges, contact Reid Diehl

(RSA Archer DoD Account Manager)

reid.diehl@rsa.com

703-785-7207

—or visit us at http://www.emc.com/security/rsa-archer.htm#!modules

HANDOUT