DIACAP to RMF Conversion

Emphasis on Continuous Monitoring

emagine it
consider it solved.

Address 3040 Williams Drive, Suite 400
Fairfax, VA 22031
Phone 202.587.5607
Fax 301.560.5865
Web www.eit2.com

DIACAP to RMF Conversion

- The recent Government mandate to convert from DIACAP to Risk Management Framework (RMF) has caused unnecessary delays in certifying programs. The root cause is a variety of uncommon approaches in conveying what programs currently have into RMF. To better understand and integrate current package into RMF a new approach to conversion is required for clarity into the DOD requirements. The RMF conversion is not difficult once the basics are properly applied to the program CONOPS. Substantial progress was made in the SP800-53 Rev4 that provides a continuous flow for all Information Assurance requirements. I wish to explain the benefits and coordination required via Areas of Responsibility (AOR), Team configuration and Control Overlap to complete this conversion in a timely manner. Careful planning and training can reduce the completion time and make the Continuous Monitoring model work more efficiently.

System Classification

Attachments - 6

- E4.A1. Mission Assurance Category I Controls for Integrity and Availability
- E4.A2. Mission Assurance Category II Controls for Integrity and Availability
- E4.A3. Mission Assurance Category III Controls for Integrity and Availability
- E4.A4. Confidentiality Controls for DoD Information Systems Processing Classified Information
- E4.A5. Confidentiality Controls for DoD Information Systems Processing Sensitive Information
- E4.A6. Confidentiality Controls for DoD Information Systems Processing Public Information

System Classification – MAC I

- E2.1.38.1. Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.

System Classification – MAC II

- E2.1.38.2. Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure assurance.

System Classification – MAC III

- E2.1.38.3. Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices (reference (a)).

System Classification

- DIACAP

Table E4.T2. Applicable IA Controls by Mission Assurance Category and Confidentiality Level

Mission Assurance Category and Confidentiality Level	Applicable IA Controls
MAC I, Classified	Attachments A1 and A4
MAC I, Sensitive	Attachments A1 and A5
MAC I, Public	Attachments A1 and A6
MAC II, Classified	Attachments A2 and A4
MAC II, Sensitive	Attachments A2 and A5
MAC II, Public	Attachments A3 and A6
MAC III, Classified	Attachments A3 and A4
MAC III, Sensitive	Attachments A3 and A5
MAC III, Public	Attachments A3 and A6

Security Objective	Low	Moderate	High
Classification	Public	Sensitive	Classified
Integrity	MAC III	MAC II	MAC I
Availability	MAC III	MAC II	MAC I

- RMF

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

The Differences

Table E4.T1. IA Control Subject Areas

Abbreviation	Subject Area Name	Number of Controls in Subject Area
DC	Security Design & Configuration	31
IA	Identification and Authentication	9
EC	Enclave and Computing Environment	48
EB	Enclave Boundary Defense	8
PE	Physical and Environmental	27
PR	Personnel	7
CO	Continuity	24
VI	Vulnerability and Incident Management	3

TABLE 1-1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

System Foundation

- Understand where your system is at.
  - Or where it needs to be.
- Categorize accordingly
- Remember the goal is ***Continuous Monitoring***
- ***Know*** what you have. (Configuration Management)
- Be able to ***Prove*** what you have. (Audit)

Areas of Responsibility (AOR), Team configuration and Control Overlap

Define the responsibilities and communication necessary for DIACAP to RMF Conversion to be successful.

- Start with the Obvious
- Areas of Responsibility (AOR)
- Team configuration recommendation
- Control Overlap Documented

Areas of Responsibility (AOR) - 1

TABLE 1-1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

Areas of Responsibility (AOR) - 2

TABLE J-1: SUMMARY OF PRIVACY CONTROLS BY FAMILY

ID	PRIVACY CONTROLS
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal

Areas of Responsibility (AOR) - 3

ID	PRIVACY CONTROLS
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Suggested Folder Structure

00-SSP	3/15/2015 5:34 PM	File folder
01-Access Control	3/15/2015 5:35 PM	File folder
02-Awareness & Training	3/15/2015 5:35 PM	File folder
03-Audit & Accountability	3/15/2015 5:35 PM	File folder
04-Security Assessment & Authorization	3/15/2015 5:35 PM	File folder
05-Configuration Management	3/15/2015 5:35 PM	File folder
06-Contingency Planning	3/15/2015 5:35 PM	File folder
07-Identification & Authentication	3/15/2015 5:36 PM	File folder
08-Incident Response	3/15/2015 5:36 PM	File folder
09-Maintenance	3/15/2015 5:36 PM	File folder
10-Media Protection	3/15/2015 5:36 PM	File folder
11-Physical & Environmental Protection	3/15/2015 5:36 PM	File folder
12-Planning	3/15/2015 5:37 PM	File folder
13-Personnel Security	3/15/2015 5:37 PM	File folder
14-Risk Assessment	3/15/2015 5:37 PM	File folder
15-System & Services Acquisition	3/15/2015 5:37 PM	File folder
16-System & Communications Protection	3/15/2015 5:37 PM	File folder
17-System & Information Integrity	3/15/2015 5:37 PM	File folder
18-Program Management	3/15/2015 5:38 PM	File folder
19-Authority and Purpose	3/15/2015 5:39 PM	File folder
20-Accountability, Audit, and Risk Mana...	3/15/2015 5:39 PM	File folder
21-Data Quality and Integrity	3/15/2015 5:39 PM	File folder
22-Data Minimization and Retention	3/15/2015 5:39 PM	File folder
23-Individual Participation and Redress	3/15/2015 5:41 PM	File folder
24-Security	3/15/2015 5:41 PM	File folder
25-Transparency	3/15/2015 5:41 PM	File folder
26-Use Limitation	3/15/2015 5:41 PM	File folder

Team Configuration – Operational

- AT Awareness and Training
- CM Configuration Management
- CP Contingency Planning
- IR Incident Response
- MA Maintenance
- MP Media Protection
- PE Physical and Environmental Protection
- PS Personnel Security
- SI System and Information Integrity

Team Configuration – Technical

- AC Access Control
- AU Audit and Accountability
- IA Identification and Authentication
- SC System and Communications Protection

Team Configuration – Management

- CA Security Assessment and Authorization
- PL Planning
- RA Risk Assessment
- SA System and Services Acquisition
- PM Program Management

Team Configuration – Privacy

- AP Authority and Purpose
- AR Accountability, Audit, and Risk Management
- DI Data Quality and Integrity
- DM Data Minimization and Retention
- IP Individual Participation and Redress
- SE Security
- TR Transparency
- UL Use Limitation

System Foundation – Control Overlap

- Map your system controls in your System Security Plan (SSP) by Identifying all required main controls. As shown in the example below.

NIST Control #	Control Name	NISPOM & DSS Reference
IA-1	Identification and Authentication Policy and Procedures	8-607
IA-2	Identification and Authentication (Organizational Users)	8-607
IA-3	Device Identification and Authentication	8-607
IA-4	Identifier Management	8-607
IA-5	Authenticator Management	8-607
IA-6	Authenticator Feedback	8-607
IA-7	Cryptographic Module Authentication	
IA-8	Identification and Authentication (Non-Organizational Users)	

System Foundation – Control Overlap

- **AU-13 MONITORING FOR INFORMATION DISCLOSURE**
  - Control: The organization monitors [*Assignment: organization-defined open source information and/or information sites*] [*Assignment: organization-defined frequency*] for evidence of unauthorized disclosure of organizational information.
  - Supplemental Guidance: Open source information includes, for example, social networking sites. Related controls: PE-3, SC-7.
- Control Enhancements:
  - *MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS*
  - **The organization employs automated mechanisms to determine if organizational information has been disclosed in an unauthorized manner.**
- Supplemental Guidance: Automated mechanisms can include, for example, automated scripts to monitor new posts on selected websites, and commercial services providing notifications and alerts to organizations.
  - *MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES*
  - **The organization reviews the open source information sites being monitored [*Assignment: organization-defined frequency*].**
- References: None.
- Priority and Baseline Allocation:
  - P0 **LOW** Not Selected **MOD** Not Selected **HIGH** Not Selected

Configuration Management

- Understand the difference between Static & Dynamic data within your documentation.
- Look for ways to automate your updates to reduce future maintenance incurred by Continuous Monitoring
- Don’t forget the Change Control Board (CCB)
- Tighten your Inventory Control and ensure that only Approved Products are utilized.
  - CCB must be involved in selection of new items.
    - To include Hardware, Software, Firmware and Patches
    - Patches should always include a back out plan.

Configuration Management

- Static Data
  - Regulations
  - Baseline Reference Documents
  - Required Password Settings
  - Process Maps
  - Organization Structure
    - To include positions of authority
  - Switch Configuration (sometimes)
  - Backup Plan
  - Restore Plan

Configuration Management

- Dynamic Data – (SNAPSHOT)
  - Approved Hardware, Software and Firmware
  - System Network Information
  - Access Accounts
  - Qualification Records
  - IA Awareness Training Records
  - Group Policies
  - Position of Importance Assignments
    - SIP Related Positions - DAA/ISSM/ISSO
    - Backup Lead
    - Restore Lead
    - Team Assignments
      - Recovery
      - Incident Response

Configuration Management

- Laundry List
  - Remove unused retired items from your systems
    - Don’t just unplug it!
  - Include a projected End of Life (EOL) for all Hardware & Software
    - Review via a defined cycle
  - Use a Decommission Process
    - Insure proper disposal of equipment and data storage devices

Audit Capability

- Proper Audit capability provides your organization a means to verify system status via Continuous Monitoring
- ACAS is the up and coming DoD standard.
  - Properly configured and resourced, ACAS can continuously monitor your systems from a vulnerability management standpoint.
  - Updates can be kept current on standalone or closed systems via “sneakernet”.
- Other tools are still required to fulfill compliance and should be utilized as per your organizations requirements.

Audit Capability

- Audits should be configured to provide, as needed, snapshots for the purpose of post update verifications and incident response.
- Keep in mind that Windows 2003 is at End of Life.
  - Audit IDs have the OLD numbering schema
  - Windows 2008 / Vista began a NEW numbering schema
  - Good reason to make the switch and reduce your audit burden.
- Audit records must be archived in accordance to your system requirements.
- Finally, Audit should be configured to prove that your Configuration Management is accurate.

Reference Information

- DoDI 8500.2 Information Assurance Implementations
- SP800-53 Revision 3-Recommended Security Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations

Q&A Session


Originally appeared at blog.unisyssecurityindex.com
Okay, everyone who opposes the new security policy, raise your hand.
©2011 Dave Blazek
Blazek

Contact Information

Marc E. St.Pierre , M.S Network Security, CISSP
emagine it
Enterprise Information Assurance Manager
Mobile (540) 841-5814
Fax (301) 560-5865
Email marc.stpierre@eit2.com
Web www.eit2.com