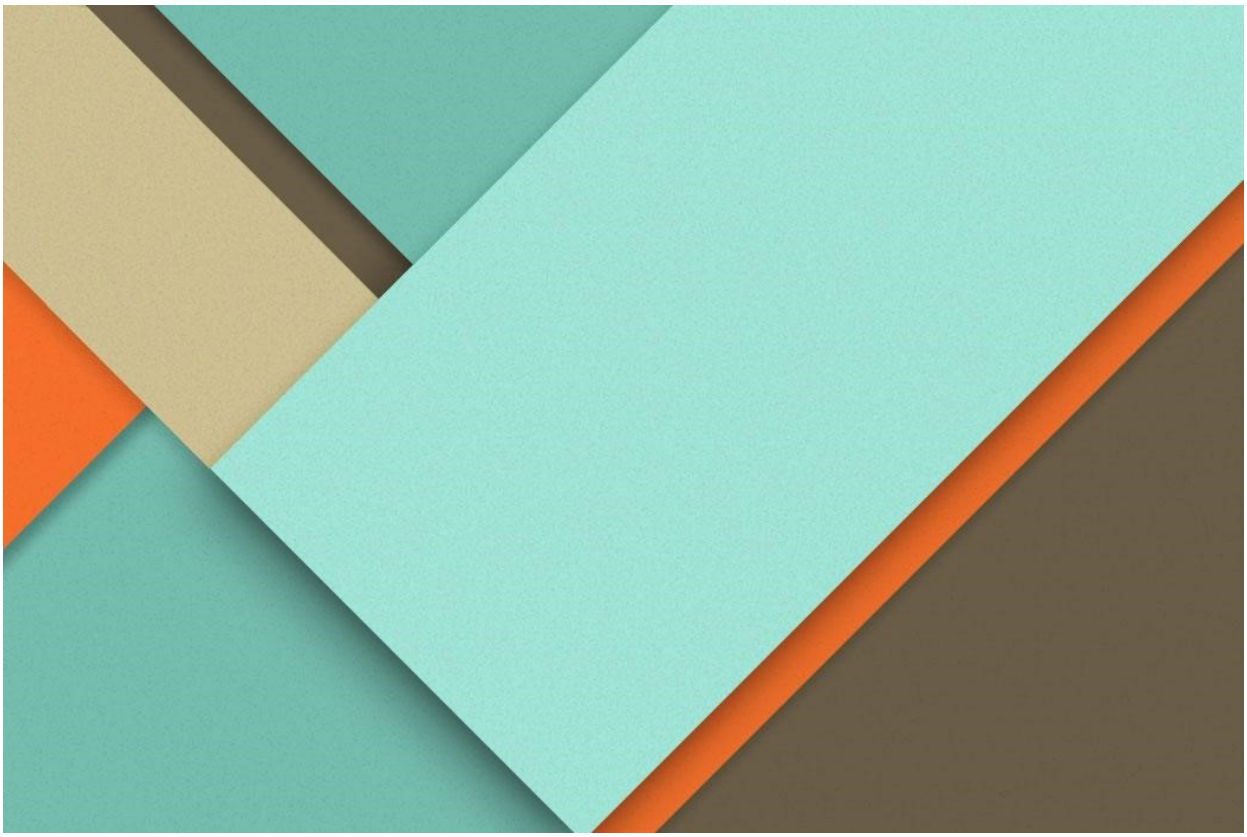

DIACAP IA CONTROLS

Requirements Document

10.13.2015

Sasa Basara
University of Missouri-St. Louis

1 University Blvd
St. Louis, MO 63121

Overview

This task is creating threshold (shall) requirements for the DoD 8500.2 IA Controls. Students required to select a classification and Mission Assurance Category (MAC) level.

Goals

1. Become familiar with authoring Information Assurance (IA) requirements.
2. Develop skills in developing security focused requirements.

Requirements Matrix

A total of 35 requirements are chosen from the MAC [1], [Classified].

	Control Number	Control Name	Requirement (student write)	Method to Test Implementation (student write) - Use Validation Procedures Tab
#	COAS-2 (Sample)	Alternate Site Designation	An alternate site shall be identified that permits that restoration of all mission or business essential functions.	1. Inspect alternative site documentation. 2. Observe alternative site. 3. Inspect service agreement documentation for restoration. 4. Test restoration abilities of alternate site.
1	COBR-1	Protection of Backup and Restoration Assets	A method of assuring physical assets meeting fire rated standards shall be implemented across the facility. A technical security control shall be invoked to ensure.	1. All employees issued RCA access tokens for hardware 2. Employee badge must use HID to enter secure physical areas

2	COMS-2	Maintenance support	All key IT assets shall have 24x7 immediate support	1. All employees of key IT assets have to have on-call schedule 2. Employees must be readily available to answer key IT asset related maintenance support
3	COED-2	Schedule Exercise and Drills	A schedule of drills and exercises shall be implemented on a regular cycle as well as surprise drills	1. Implement a schedule of drills throughout the calendar year 2. Coordinate drills among management teams and cross-functional teams 3. Assure drill does not interpret normal process 4. Track results of drill and meet for discussion afterwards
4	COPS-3	Power Supply	A electric system should allow key IT process to run uninterrupted this shall include a uninterrupted source as well as an emergency backup	1. Implement electric system to run key IT assets 2. Provide a alternative backup source such as emergency generators or off-site power
5	COSP-2	Spares and Parts	Spare parts and maintenance for parts shall be available 24x7	1. Assure that all spare parts are on –hand for a 24x7 repair cycle 2. Assure that all product parts are compatible with current system parts 3. Have availability of supplies on 24x7 period notice
6	COSW-1	Backup Copies of Critical SW	Backups copies of OS systems and other critical system shall be kept in a fire rated container	1. Assure the container is fire-rated to store critical system backups 2. Assure access to container is maintained by physical level control
7	DCBP-1	Best Security Practices	The DoD info sys security design shall incorporate best security practices	1. Incorporated practices such as PKE, SSO, smart card, and biometrics shall be implemented throughout key IT asset areas. 2. Practices should be referenced by utilizing accredited industry, government, academia or collaborations of all three.
8	DCCS-2	Configuration Specifications	For security technical implementation guide the DoD reference documents shall be followed. If DoD documents are not available utilized the DISA or NSA to draft configuration guidance.	1. Refer to DoD documentations for system components where applicable 2. Maintain all major system software components that require configuration 3. Follow the DIACAP knowledge base or other repository to access DISA STIG for OS, and Software application. ‘ 4. Utilize the STIG manual or automated config guidance for OS, Software
9	DCCT-1	Security Design and Configuration	All security upgrades, patches, and new AIS applications shall be	1. Each component shall maintain a test procedure that verifies modification to field systems and assures there will be no

			tested before deployment	interruptions. 2. Maintain a up to date understanding of vendor upgrades or patches. 3. All patches should come from approved place and have been tested prior to production push
10	DCDS-1	Dedicated IA services	IA shall have dedicated services, for services such as firewalls, key management service, etc- that are approved by the DoD component CIO	1. Any component entering should have a document format risk level to allow evaluation of said software 2. Use the DoDI 8500.2 enclosure 2.3 as the minimum factors considered when evaluating dedicated IA services
11	DCID-1	Interconnection Documentation	AIS application shall maintain deployment planning and coordinate the exchange of connections rules and requirements. Enclaves shall list all hosted AIS applications and interconnection outsources IT-based process and interconnected IT platforms.	1. Each system connection to another system shall agree on the operations parameters 2. Items that include data handling methods, personal clearance, and operating shall be approved y bother DAA's 3. Maintaining and agreement shall be implemented by each system 4. All changes to be reviewed for IA accreditation impact
12	DCII-1	IA Impact Assessment	Any changes to DoD shall be assed for IA and accreditation impact prior to implementation	1. Maintain a formal process that identifies changes that will affect IA 2. Utilize the CCB and DIACAP to access changes for IA and accreditation impact
13	DCIT-1	IA for IT Services	All acquisitions or outsourcing of IT shall explicitly address government, service provider, and end user IA roles and responsibilities.	1. During acquisitions or outsourcing IT services contracts and other documents that hold ID roles should have IA roles examples, PM, IAM, User Representative, CA DAA, SIA and CIO.
14	DCNR-1	Non-repudiation	When implementing encryption system shall use NIST FIPS 140-2 validation	1. Assure timestamps are made for non-repudiation 2. NIST FIPS 140-2 validate cryptography shall use implemented encryption key change and hash. 3. When possible adopt newer standards
15	DCPA-1	Partitioning the application	User interfaces services shall be physical or logically separated form data store and management system.	1. Separate systems by logic so that one system can not directly invoke the other 2. Utilized different database systems to separate the systems so that they do not interact with one another
16	DCPB-1	IA Program and Budget	A separate budget for IA shall be enacted	1. Different budget for IA should be invoked for the all systems
17	DCSL-1	System	A system shall be	1. Control the libraries by CCB

		Library management controls	installed to maintain programming code	2. Access shall be minimum to these libraries 3. Maintain a access log
18	DCSP-1	Security Support Structure Partitioning	The support structure shall maintain isolation from other systems	1. Implement architecture to avoid overlap between systems 2. Ensure that the systems are maintained separated through domains, partitions etc.
19	DCSQ-1	Software Quality	The system shall maintain software quality by utilizing the CJCSI- IA, IEEE 12207.0 for SDLC	1. Ensure that developers follow procedure to ensure quality of software 2. Have formal software test methodologies that adhere to all SDLC
20	DCSS-2	System State Changes	System shall maintain system integrity state when shutdowns and aborts occur	1. Identify that the translations of the system are appropriate for SIA or NSA requirements.
21	PEFI-1	Fire inspection	The environment shall be inspected by the fire marshal for standards	1. Undergo period fire marshal inspection 2. Document any issues noted by marshal 3. Promptly resolve any fire hazard issue
22	PEFS-2	Fire Suppression	A fully automated fire suppression system shall be installed and active that detects heat, smoke or particles	1. Install a system to monitor all fire type hazards this includes heat, smoke, etc. 2. Document testing of said system to allow assurance that the system is capable 3. Test the fire system regularly to allow understanding of capabilities
23	PEHC-2	Humidity Controls	A automatic humidity control system shall be installed	1. Install system to monitor humidity and alert personal of equipment failure 2. Test the system regularly for faults 3. Document the testing of the system
24	PEMS-1	Master Power Switch	A master power switch shall be installed to stop all power	1. Install power switch and make available to staff when needed. 2. Maintain the power switch so it does not turn on by accident 3. Test the master power switch to assure proper usage
25	PRNK-1	Access to Need to know information	Personnel with valid requirements shall only have access to systems	Invoke the DoD 5200.2-R regulations to need to know situations
26	PETN-1	Environmental Control Training	All employees shall receive initial and periodic training in the operation of environment controls	1. Employees should receive regularly training only for their job duties 2. Document the employee trainings to keep track of employees who received training
27	PEVC-1	Visitor control to Computing Facilities	Visitors shall be signed in and maintained during the entire visit	1. Maintain a log of visitors 2. Track visitor through various areas and maintain a log of their actions

28	PEDI-1	Data Interception	Position displays or outputs shall be placed to where they cannot be seen by pass bys	1. Make sure displays are positioned so others can not see the output of the data
29	PEEL-2	Emergency lighting	A system shall be installed to maintain systems after a emergency lighting strike	1. install an automatic emergency lighting system shall be installed that covers emergency 2. The automatic emergency lighting shall be in code with building standards
30	PECF-2	Access to computing facilities	Access to the facilities shall only be granted to those with access	1. those will access shall have a special HID card to allow access to areas where they can 2. if access is needed to an area the there must be an approval process
31	IAAC-1	Account Control	A account management system shall maintain access level control per individual basis	1. Install a system that implements different level of control for different users utilizing the DISA STIG vendor documentation to ensure quality 2. Follow the CJSCM 6510.01 procedure 3. System admin shall be control over access level
32	ECRR-1	Audit Record Retention	When system has DoD info sys methods with SAMI then system shall retain audit for 5 years, otherwise maintain for 1 year	1. Keep a active log of all user activity 2. limit access to the audit logs 3. ensure procedures to allow storing of audit trails
33	EBCV-1	VPN Controls	The VPN traffic shall be visible to IDS	1. Ensure that the network intrusion detection system are placed on VPN traffic 2. Utilize DoD guidelines to ensure proper monitoring
34	EBRP-1	Enclave Boundary Defense	Remote access for privileged functions shall be permitted only for compelling operations needs	1. When remote is utilize use the VPN network 2. Each remote access shall be audited 3. After ever event review the audit log by IAM/IAO
35	PSEL-1	Screen Lock	When system is not in use there shall be a function to block all system views from outside sources	1. Workstation lock shall be expected on each workstation 2. Access to workstation after screen lock only thru valid credentials