

The DoD evaluates a system or enclave's security posture via the Defense Information Assurance Certification and Accreditation Process (DIACAP). This framework evaluates different aspects relating to system security, many in disciplines that may not be under the control or direction of the information assurance directorate. The Falkland Group can help you navigate the DIACAP process and re-use existing solutions to ensure DIACAP compliance. The following paper provides a brief overview of the methodology and controls used to evaluate system security under DIACAP.

Department of Defense Certification and Accreditation Information Assurance (IA) Controls

All Information Systems (IS) on the Department of Defense (DoD) network are required to go through the DoD Information Assurance Certification and Accreditation Process (DIACAP). The guidelines for this process are set forth in the Department of Defense Instruction (DoDI) 8510.1 dated November 28, 2007. The DIACAP Process can take several months depending on the size of the IS and the knowledge and skills of the personnel executing the DIACAP process on the system.

The DIACAP process is a five (5) phase process which include the following:

- Initiate and Plan IA Certification and Accreditation (C&A)
- Implement and Validate assigned IA Controls
- Make certification determination decision
- Maintain Authorization to Operate and conduct review
- Decommission

The baseline IA control sets are taken from DoDI 8500 - 2 IA Control Checklists. There are approximately 240 baseline IA controls that are taken from DoDI 8500 - 2. Also, there are additional controls that are taken from the various regulations such as Army Regulation 25 – 2 and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS). There are hundreds of IA controls associated with the DIACAP process for an IS.

In the first phase the IA Controls are assigned based on the Mission Assurance Category (MAC) and Confidentiality Level (CL). The MAC Level reflects the importance assigned to the information based on the warfighters combat mission. There could be anywhere between 100 and 106 controls based on the MAC level of the system. Additional IA Controls may be added to the baseline for additional security measures. The IA Controls are safeguards that are either in place or need to be put in place to minimize the security risks to the IS. Also, an additional objective of IA controls is to provide testable conditions where compliance is measurable. The 8500.2 document is the DoD Instruction for IA Implementation. The 8500.2 controls can be further broken down into an IA Control Checklist wherein each item listed therein can be verified based on a specific set of procedures. Each control is then noted as: Validation procedures have been met, non-compliant: Expected results have not been met or Not Applicable: IA control does not affect the security of the IS. Validation procedures are accomplished via documentation provided to the security analyst or by technical analysis done by an engineer using tools such as Gold Disk, Retina, and Web Inspect etc.

There are three Mission Assurance Categories in DIACAP:

- 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.

- Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces.
- 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.

There are three Confidentiality Levels:

- Classified
- Sensitive
- Public

The 8500.2 checklist contains seven (7) IA Control families. The Continuity Control family requires the system owner to provide evidence of how the site will continue operation should the primary site shutdown in an emergency situation. Ex. Alternate site designation Security Design & Configuration controls address software, hardware and how the network is configured. Ex. Ports, Protocol and Services Identification & Authentication controls question how users are identified within the system and how access to the system is handled. The Enclave & Computing Environment IA controls that address security features that are within the network and enclave. Physical & Environmental Controls speak to the physical security of a location as well as safety issue ex. Emergency Lighting, Fire Detection and Fire Inspection. Personnel security controls deal with training and the access level that are given to each individual that will have direct access to the information system. Ex. Security Rules of Behavior or Acceptable Use Policy, Access to information and Maintenance Personnel. Vulnerability & Incident Management deals with the process of applying patches to the IS. This control also requires and explanations of what methods are used to identify any hardware or software vulnerabilities Ex. Incident Response Planning and Vulnerability Management

The DIACAP process can be an arduous task however, these measures must be taken to protect and defend information and information systems by ensuring the availability, integrity, authentication, confidentiality and non-repudiation.

REFERENCE

Department of Defense Instruction (DoDI) Number 8500.2:
<http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>