Global Information Assurance Certification Paper

DITSCAP: Questions to Ask
-Mike Beal

Defense Informational Technology Certification and Accreditation Process (DITSCAP) provides the current guidance for the standardization of the certification and accreditation process for the Department of Defense (DoD). The objective of DITSCAP is to establish a standardized process and management structure to certify and accredit Information System (IS) to maintain the Information Assurance (IA) and security posture of the Defense Informational Infrastructure (DII). Standardizing the process is designed to minimize risks caused by non-standardized security policies and procedures.[2] This is a further concern due to the increasing use of shared data between computer systems and databases. This will result in an overall increase in the total security posture of the DII.

In developing the DITSCAP process the DoD identified nine characteristics needed for an efficient and effective program. Those characteristics are noted below:

1. Is **tailorable** – The process is applicable to any system regardless of the system status in its life-cycle or the program strategy. The life-cycle continues until the system is removed from DoD service. The process may be applied to any program strategy, e.g., grand design, incremental, or evolutionary.

2. Is **scalable** – The process is applicable to systems differing in security requirements, size, complexity, connectivity and data policies.

3. Is **predictable** – The process is uniformly applicable to any system. It will minimize personal opinion and subjectivity.

4. Is **understandable** – The process provides the participants with a consistent view of the C&A process.

5. Is **relevant** – The process identifies security requirements and solutions that are achievable, e.g., available, affordable and within the context of the development approach.

6. Is **effective** – The process will result in and maintain an accreditation.

7. **7.** Is able to **evolve** – The process incorporates the results of experience, as well as changes in security policy and technology, in a timely manner.

8. Is **repeatable** – The process provides corresponding results when applied or reapplied to similar information technologies.

9. Is **responsive** – The process accommodates timely responses essential for supporting emergent Military Deputy (MILDEP) and National Agency operational requirements and priorities.[4]

The DITSCAP process is divided into four phases. Each phase has distance and separate tasks. The phases are definition, verification, validation, and post -accreditation. Their definitions are:

> A. Definition: the activities and tasks to verify the systems mission, environment and architecture; to identify threats; to define the level of effort; to identify participants in the process and to document Certification and Accreditation security requirements (C&A).
>
> B. Verification: the activities to document the compliance of the system with the security requirement previously agreed upon in phase one.
>
> C. Validation: the activities to assure that the fully integrated system in its operating environment and configuration provides an acceptable level of residual risk. Validation ends with obtaining the approval to operate.
>
> D. Post Accreditation: the activities to monitor system management, configuration, and threats to ensure a maintained level of residual risk. A change in the environment could require the system to be reaccredited from phase one.[1]

For each system the DITSCAP process is documented in a System Security Authorization Agreement (SSAA). The goal of the document is to consolidate all security information into one document. The SSAA will document requirements necessary for accreditation and security criteria. This document is a formal agreement among all parties participating in the C&A process. The completed SSAA contains only those items agreed on by the Designating Approving Authority (DAA), the Certifying Authority (CA), User Representative and the Program Manager (PM). Each of the phases contains tasks that are documented in the SSAA.[2]

> Designated Approving Authority (DAA): the official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk.
>
> Certifying Authority (CA): the official responsible for performing the comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements.
>
> Program Manager (PM): the person ultimately responsible for the overall procurement, development, integration, modification, or operational maintenance of the IT system.[1]

With this in mind the goal of this paper is to review several subtasks for each of the phases in detail. While researching this topic you can easily find all the applicable regulations. After filtering through all the contractors that want to provide consulting

services to help certify DoD systems, you discover only several small articles; all providing a reader with the idea that the DITSAP is a simple process that starts with phase one and continues thru phase four. Correctly certifying and accrediting a system is more difficult than just documenting the requested information.

The first task is a preparation activity, where information and documentation is collected about the system. This is a complete review of all information and security regulations for the system being certified. It is the background information used in the registration activity and in writing the SSAA. It is the time consuming task of locating and reading all the information available on the system. It also requires researching skills. The researcher must be able to locate all DoD and Federal computer regulations. Also the researcher must be able to create a working relationship with each party involved in the certification process. This requires a full time commitment to the DITSCAP process, if the system in question is large and complex. This commitment to a full-time dedicated security resource is necessary for a successful security certification and accreditation.

The second task is the registration of the system to be certified and accredited. There are eight individual subtasks that are required for this activity. The first seven describe individual requirements to research for the SSAA. The last task is to develop the initial SSAA; by putting the first seven in a defined order. This is relatively simple because all the information comes from the initial preparation activity.[2]

Determining the system security requirements is a registration activity that is not well defined. The tasking requires the researcher to determine all the governing Security Requisites; which is defined in the DITSCAP Instructions (DoD 5200.40) as those security requirements that must be addressed in all systems. These requirements are set by policy, directive, or common practice; set by Executive Order, the Office of Management and budget (OMB), the Office of the Secretary of Defense (OSD), a Military Service or a DoD Agency. The DITSCAP Manual (DoD 8510-M, dated 31 July 2000) contains 48 separate references; which does not include any Executive Orders, Military Service or DoD Agency specific requirements. DITSCAP is designed to be predictable by uniformly applying the process to any system. It also reduces the understandability of the process. It does not provide a consistent view of the security requirements. Not having a single source of requirements reduces the standardization of the process. The more requirements that are considered revilement, the more secure the system.

The verification phase is used to verify that system development complies with the requirement in the SSAA. Most modifications to the system would be minor, if the system requirements were accurately developed. However during testing there are always deficiencies between design requirements and the completed applications. Changes to the system are made to correct the deficiencies. Configuration Management is the means used to see that these changes are documented and recorded. The concern for security personnel is that they are not informed of all the changes made to the system. Most changes are made to correct any functional deficiencies that were discovered during testing. Functional members of the development team do not inform security of the

changes. This will not allow security experts an opportunity to evaluate the changes for security issues. The SSAA will also be updated to contain current documentation of the system. All parties involved in the development of a new system or application must be concerned with security to insure a secure final product.[2]

Validation is the final task before developing a recommendation to the DAA for accreditation. This phase contains the actual testing of the system to insure that all the security requirements have been met. To assure this, the following items are tested and evaluated:

-Security Test and Evaluation
-Penetration Testing
-Tempest and RED-BLACK Evaluation (if applies)
-COMSEC Compliance Evaluation (if applies)
-System Management Analysis
-Site Accreditation Survey
-Contingency Plan Evaluation
-Risk Management Review[2]

The current distributive nature of computer systems is not adequately addressed in the DITSCAP manual. This is most evident for the Site Accreditation and Contingency Planning Evaluation. If a new computer application is designed and developed by a Military Service to meet a defense need, the application and database servers could be owned and operated by the Defense Information Systems Agency (DISA), a Defense Agency. Users could be located at any site where there is an Internet connection. The question then is who is responsible for the DITSCAP process. The DITSCAP Manual does indicate that a DAA can issue a type accreditation. This will allow identical copies of an application to be accredited for a typical operating environment. Further definition of tasks that are not needed to be completed or additional tasks need to be further defined in the manual.

The final task in the verification phase is to develop the recommendation for approval and to have the systems accreditation granted. The tasks include identifying and assessing system vulnerabilities and recommending risk mitigation measures. The final SSAA and a recommendation for or against accreditation are forwarded to the DAA for approval. If at any time the deficiencies in the system security were noted, the entire process should have revered back to the Definition Phase. If the DITSCAP process was done correctly, all of the residual risk should be at a level sufficiently low so as to permit the DAA to accredit the system.[2]

This is a logical place to discuss the requirements needed for security between the development and production environments. For a newly developed system the security is "age appropriate" for the current state of development. All the security requirements are written for the "to be" environment. All the reports the new system will generate are based on requirements written by the development team. New business rules and processes were developed for use with the new application. The DITSCAP has a

weakness in that it does not require sufficient participation by the eventual end-user of the application. Required updates for security issues need to be included in reports to the final production area with the same importance as functional and technical issues.

Post Accreditation is the activities required to maintain an acceptable level of risk. These tasks are assigned to the Information System Security Officer (ISSO). It is their responsibility to maintain the SSAA. A continuous review of the system to determine if any changes in the system or environment have caused a security risk is necessary. If there is an unacceptable level of risk, the DITSCAP process must start over from Phase 1 to address the new threat.[2]

Training is an issue that is not addressed by the DITSCAP. There is not required minimal security training. There is training available concerning the DITSCAP, however it only explains the regulations. Courses on how to write security tests, conduct penetration testing, and physical security are lacking. Contractors are available to provide the services to have a system initially certified and accredited. The long-term security maintenance will be conducted by military and civilian personal. The question is do they have the knowledge and skills necessary to recognize a security threat. Will management be willing to investigate their security issues?

Conclusion:

To determine the effectiveness of the DITSCAP, a person needs to review several other security models. Electronic Data Systems Corporation (EDS) has developed a similar life-cycle model. Their method is a continuous five- step circle that includes the following tasks:

1. Assess: to assess the organization's current security posture and recommend appropriate security policies and procedures

2. Protect: to develop and implement protective measures including policies, plans and architecture that mitigates the identified risks

3. Validate: to validate that the security mechanisms in place do support the security policy and address the identified risks

4. Training: to provide security awareness training for the companies employees and management.

5. Monitor: to address the need for constant, active vigilance at the system defensive perimeter; including security policies, practices, procedures and processes.[3]

The differences between the DITSCAP process and that of EDS are due to two issues. First the DITSCAP, while able to be tailored to an existing application, is basically a policy for a system in development. This allows for the validation of the security

measures before the verification or protection phase. The second issue is that EDS is a consulting firm whose customer has probably just had a security issue. For EDS it is important to show the ability to quickly reduce security vulnerabilities.

William Perry developed a second model in his text titled Management Strategies for Computer Security. He proposed a linear approach to the development of a computer security program. He proposed the following tasks:

-Establishing a Security Baseline
-Determining the Security Needed
-Evaluating Computer Security
-Establishing a Management Security Strategy
-Creating Enthusiasm for Computer Security
-Creating an Organizational Environment to Support Security
-Building Security Inside the Data Center
-Building Computer Security Outside the Data Center
-Assessing the Effectiveness of Computer Security5

The major difference in his concept is the addition of an organizational environment for security and evaluating the computer security. Evaluating computer security is the process of determining the cost benefit of having computer security. It is not a good business practice to spend more funds protecting data than the data is worth. In the DoD most data is required by regulation to be protected. The cost benefit analysis is minimal in the DITSCAP. Top-secret data will have more security than classified data, however a cost analysis is not done.

Overall the DITSCAP meets is goals and objectives. It provides a policy that clearly defines the certification and accreditation process. If the policy is followed, the results will be a system with lower residual security risks. The concern is that the personnel assigned to the Certification Team are not given the time and resources to thoroughly review all the needed data and run all the needed tests. Upper management needs to support the security process with as much support and enthusiasm as it places on the other aspects of the acquisition life cycle.

References:

[1]DoD Instruction 5200.40 DoD Informational Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997.
http://iase.disa.mil/ditscap/i520040.pdf (Active November 18, 2001)

[2]DoD Manual 8510.1-M, Department of Defense Information Technology Certification And Accreditation Process (DITSCAP) Application Manual, July 2000.
http://mattche.iiie.disa.mil/ditscap/appjuly00.pdf (Active November 18, 2001)

[3]McClelland, Mark. Information Assurance in the Digital Marketplace. September 2000.
http://www.eds.com/news/images/infoasr_mcclelland.pdf (Active November 18, 2001)

[4]Sherbure, Guy. "DoD Information Technology Security Information and Accreditation Process (DITSCAP)." USAMISSA Newsletter Vol.13, September 2000. http://usamissa.detrick.army.mil/news/newsletters/0009/ditscap.html (Active November 18, 2001)

[5]Perry, Williams. "Management Strategies for Computer Security." Boston:Butterworth Publishers 1985.