GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Dan Commons
GSEC Practical Assignment version 1.2e

DITSCAP – DoD's Answer to Secure Systems

The majority of you will ask yourself a few simple questions " why?... Why should I care? Why should I be concerned or interested in reading about a government bureaucratic process?" Another group may ask, "how can I get my share of the pie." The security professional's question might be "how can I leverage the government's work for my own benefit?" A final group may shrug it off and say it will never impact me. A simple answer would be it's your money, to the tune of several billion dollars per year! The intent of this paper is to provide insight into a process that is rapidly being adapted, in part or as a whole, by an increasing number of local governments, the medical industry, and corporate America. After all "a risk assumed by one is imposed on all" is never more true than in today's increasingly interrelated world.

All things must have a legal caveat: "this paper will not make you an expert in the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)[1] or its federal government equivalent the National Information Assurance Certification and Accreditation Process (NIACAP).[2]" What it will do is provide a realistic look at what, on the surface, appears to be a complex, rigid, bureaucratic, and military process. Through the course of this paper we will look at the history of how we got here, a description of the key concepts, the process flow, and hopefully point you in the right direction to join the thousands of federal employees and contractors practicing a standard, structured approach to secure system implementation.

Historical Evolution

Twenty years ago, it was virtually unheard of to have Congress express any interest in what "those computer geeks" were doing. Today they cringe at the thought of not having their handhelds and personal communication devices. It wasn't until the early 90's that DoD began to realize that their brainchild, ARPANET, had escaped from the bottle and was expanding at an exponential rate. In 1992, the Assistant Secretary of Defense for Command, Control, Computers, and Intelligence issued the *Defense Information Systems Security Program Strategic Plan*[3]. The plan created standardized requirements and a process for the accreditation of computers, systems and networks that would meet the policies defined in the DoD Directive 5200.28, *The Computer Security Act of 1987*, and the Office of Management and Budget (OMB) Circular No. A-130, *Management of Federal Information Resources*.

The 1992 mandate lead to the development of a standardized approach to the security certification and accreditation of information systems in order to ensure the availability of mission essential communication paths. The result was a DoD instruction, DoDI 5200.40, *Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)*. DITSCAP intended to streamline the very expensive and labor-intensive process in place since the early 1980's. The initial early 80's process produced reams of documentation that became bookends, dust collectors, and improvised stools as they sat around taking up space. DITSCAP consolidates the paperwork while allowing elements within the department to measure performance across a wide range of missions and environments,

© SANS Institute 2000 - 2005 Author retains full rights.

employing standard conventions, criteria, and processes.

During the last few years, we have seen numerous congressional and presidential mandates designed to increase the security and reliability of our infrastructure and information systems. According to Congressional Research Service (CRS) reports[4], Congress is increasingly directing federal agencies to set goals and to measure performance as a direct input into Congresses annual appropriations processes. Twenty-eight laws in the 105th Congress contained references to the 1993 *Government Performance and Results Act* (*GPRA* or *Results Act*) or to mandatory performance measurements. In addition, 78 reports accompanying bills enacted into law contained similar language. Several key initiatives, primarily OMB A-130 and *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* have emphasized increased security vigilance, often through "threat of punishment," at all levels of the federal government. The capstone of this renewed interest was in 1998 with the Presidential Decision Directive 63 (PDD 63), *The Clinton Administration's Policy on Critical Infrastructure Protection*[5] directing increased vigilance and security of our national infrastructure. The directive required the completion of a National Infrastructure Assurance Plan with milestones for accomplishing the following items:

Vulnerability Analyses: Each government sector must conduct an initial vulnerability assessment, followed by periodic updates.
Remedial Plan: A plan to identify corrective actions for the identified vulnerabilities
Warning: Establish a national center for attack and incident warning.
Response: Develop plan to respond to attacks in progress.
Reconstitution: Be able to recover from successful attacks
Education and Awareness: Provide security and information assurance training.
Research and Development: Conduct and fund infrastructure protection research.
Intelligence: Develop and implement a plan to collect and analyze infrastructure threats.
International Cooperation: Foster cooperation with friendly nations, international organizations, and multinational corporations
Legislative and Budgetary Requirements: Evaluate budget priorities to comply with the directive's intent.

This increased oversight reinforces the need for a systematic approach to securing and controlling networks, protecting data, and ensuring the accessibility of communication media to accomplish the mission. The Department of Defenses DITSCAP serves as the foundation for the military's compliance with PDD 63 and a model for other government agencies to develop compliant plans and procedures. Faced with ever increasing mandates, it is imperative that the DoD process is developed and adhered to ensuring safe secure mission accomplishment.

DITSCAP Process

The DITSCAP provides insight into the application of policy, best practices, sound software design, and security practices. Additionally, it streamlines the volumes into one manageable document for the entire life cycle of the information system. Using the military's concept of "cradle to grave" the process is a standard certification accreditation method with a standard document that is developed at the inception, "cradle", and is matured, rewritten, and updated

© SANS Institute 2000 - 2005 Author retains full rights.

until the system is replaced, the "grave". This process is applicable to all projects, regardless of their size, scope, type of acquisition, or the method of development.

Up to this point, I've provided insight into the regulatory requirements without delving into the actual DITSCAP process. The DITSCAP process protects and secures the DoD infrastructure and mission essential information while maintaining the proper balance between the missions, risks to those missions, and life-cycle costs. The process consists of four phases, with numerous tasks within each phase, designed within a nine characteristic model. The DITSCAP's nine characteristics are:

1. Tailorable - Applicable to any system at any status in its life cycle
2. Scalable - Sized to fit the security requirements, complexity, connectivity, and policies.
3. Predictable - Known and standard process regardless of system
4. Understandable - Objective and defined security standards
5. Relevant - Identifies achievable of security requirements and solutions
6. Effective - Results in and maintains an accreditation for the target system.
7. Evolvable - Incorporates lessons learned, changes in security policy, and technology
8. Repeatable - Can be applied to similar systems with the same results
9. Responsive - Timely system changes based on operational requirements and priorities

The four well-defined steps (phases) run from the initial concept throughout the systems life cycle, the "cradle to grave" concept. Phase one, *Definition*, is the concept or birth of the project. The second phase, *Verification*, insures that the design of the system meets all the requirements identified in the system's security authorization agreement. The third phase, *Validation*, provides a safety check through security tests, government acceptance testing, and operational tests and evaluations. The fourth and final phase is *Post Accreditation.* Post accreditation follows the system from installation through out its operation to its ultimate retirement. Figure 1 illustrates a simplistic look at the relationship of the four phases.

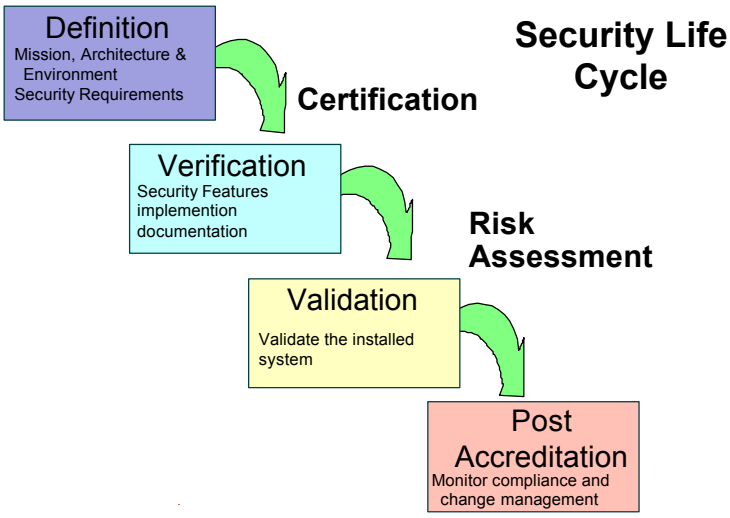

Figure 1. DITSCAP Phases

The Definition Phase develops the parameters of the system. Typical phase 1 activities

© SANS Institute 2000 - 2005 Author retains full rights.

include verifying the system mission, environment and architecture, identifying the threat, and defining the levels of effort. Additionally, the manual identifies the key process owners and players. The Designated Approving Authority (DAA) is the individual with the "authority and ability to evaluate the mission, business case, and budgetary needs for the system in view of the security risks." [1] The DAA is legally responsible for determining an acceptable level of residual risk and approving the system operation. The second key player is the Certification Authority (Certifier) who advises the DAA and possesses the technical knowledge to make accreditation recommendations. Typically, the Certifier creates a team that conducts the certification activities in each phase, determines the level of residual risk, and makes an accreditation recommendation to the DAA. The record created to document the team's effort is the System Security Authorization Agreement (SSAA) that serves as the single repository for all system information.

Phase one answers the typical who, what, where, when, why, and how questions. This phase defines the depth of involvement and the scope of the project. The key to the SSAA is properly sizing the project. If the system is a simple one that relies on known commercial products and accepted practices then the document may be concise. However, if the system is extremely large and complex it might require additional information to adequately address the system. Security and the tenants of a secure system (identification and authentication, access controls, auditing, confidentiality, and integrity) are negotiated and addressed during the formulation of the SSAA.

The SSAA serves as the tracking document and consists of numerous sections and appendix that outline the operation and features of the system. Many of the document's sections are already familiar to security professionals. The common Security Policy equates to the DITSCAP Information System Security Policy. Similarly, 75 to 80% of the contents of an SSAA exist under a different name in the corporate world today. Often it is in the form of policies, procedures, configuration guides, training manuals, etc.... The SSAA compiles the various documents into a single reference place for all system guidance. The following figure lists the typical sections of the SSAA (agencies may add/delete sections).

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

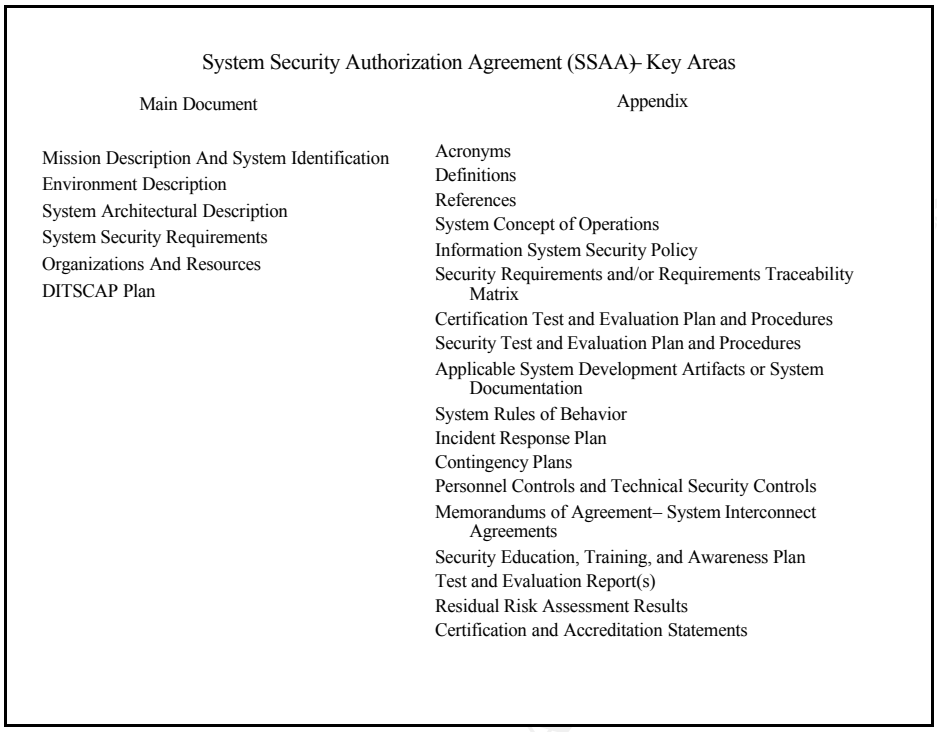

Figure 2 – SSAA Sections

It is critical to the success of the process to correctly determine the scope of the project and tailor the SSAA to fit. The *Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)-Application Manual* contains several charts and tables to assist in the tailoring effort. The Certifier defines the project scope by determining the appropriate level of certification. An analysis of the system business functions, policy and oversight security requirements, criticality of the system to the mission, software products used, computer infrastructure and network, data processed by the system, and types of users serves as the basis for certification decisions. The Certifier examines the information and determines the degree of confidentiality, integrity, availability, and accountability required for the system. After computing the weighted factors, as identified in the DITSCAP manual tables, the Certifier recommends one of four certification levels. Level 1 is a basic security review using the provided checklist. Level 2 is a more extensive look that includes the checklist review with additional, but not in-depth, testing. Level 3 encompasses the level 2 activities and includes a more extensive penetration and vulnerability test plan. Level 4 is the most stringent level of security analysis.

Once the initial SSAA is developed, and approved by the DAA, we progress to the second phase, Verification. During Verification the system is developed, the architecture designed and the security, mechanisms are incorporated. This phase typically relies upon hands-on involvement from several specialties, including the security experts, to ensure that the design of the system meets all the requirements identified in the SSAA. Phase one lays out the system description, requirements, architectures, and security specifications. If applied and developed properly it can minimize the infamous "version creep" so popular in today's hurry-to-market environment. If the vision is not reached or system problems require changes, then the SSAA needs to be adjusted to accurately reflect the end product—easily done, after all it's a living document. Any changes in the system that affect its security posture require DAA approval. The

© SANS Institute 2000 - 2005 Author retains full rights.

product of this phase is an information system that is designed to meet the customer needs and satisfies the initial project goals. The system is now ready to be certified.

Certification is the result of phase three, Validation. Validation provides a safety check through security tests, government acceptance testing, and operational tests and evaluations. It gives the security professional a "warm fuzzy" that he/she knows what the system does, its identified risks, and the countermeasures necessary to secure the application or network. The testing incorporates verification activities for compliance with the security requirements. Among the verification activities is a check for compliance with applicable governing documents and established architectures. Additionally, the system interfaces and data flow is identified and verified to ensure that other interfaced systems comply with the systems security policy and conditions. The Security Test and Evaluation (ST&E) is designed to catch any remaining system shortfalls and verify mechanisms work. The Testing After Action report is a risk assessment that identifies residual risks and recommends either further development or methods to reduce the shortfalls to an acceptable risk level.

Risk is unavoidable. The system administrator or security expert that practices risk avoidance is destined for failure. A sound approach applying the tenants of operational risk management seeking to minimize the risk, implementing electronic or physical countermeasures, and assuming an acceptable level of residual risk is the preferred practice in today's environment. As the complexities of systems grow, new vulnerabilities are discovered and exploited everyday. Risk management practices identified in the SSAA serve as the guiding tenants for the acceptable risk level. A good example of the constantly changing risk levels was provided by the Department of Defense (DoD) Chief Information Officer (CIO), Arthur Money, reported in the April 1999 issue of *The Government Executive*[5]. He states that 60 unauthorized intrusions occur in Pentagon computer networks each day, of which 60 per week are serious enough to be considered attacks. Regarding these attacks, then Deputy Defense Secretary John Hamre advised the House Armed Services Committee that about ten percent require detailed (i.e. law enforcement) investigations.

The product of the first three phases is an Approval to Operate (ATO) signed by the DAA. The DAA has the authority to formally assume responsibility for operating a system at an acceptable level of risk. At this point, the DAA has three options, deny accreditation to the system, accept it for an interim period, or issue an unconditional acceptance. Once the DAA issues the ATO the system enters into the final phase of the life cycle, Post Accreditation.

Post Accreditation follows the system from installation through out its operation to its ultimate retirement. As indicated by the DoD CIO the cyber world is the new wild untamed frontier with few effective controls (laws). It is critical that the SSAA lives and that the risk management process, the security analysis, and the configuration management efforts continue. As a living document, the SSAA requires periodic updates and recertification activities. If the DAA issued an interim accreditation, a time limit of up to one year was identified. The interim time line allows system shortcomings to be fixed while still reaping the benefits of the new system. If a full accreditation is granted it must be updated and re-accredited at the three year point.

Conclusion

While the Department of Defense Information Technology Security Certification and Accreditation Process may not have a direct impact on your job today, it might tomorrow. As

© SANS Institute 2000 - 2005 Author retains full rights.

industry continues to suffer from Denial of Service attacks, web defacements, and credit card thefts, they must embark upon a path that reduces their liability and risk. The concept of a process that provides a logical progression, standard analysis criteria, and flexibility while achieving security is appealing to corporate America. I hope that by now you can see that what appears to be a complex, rigid, bureaucratic, and military process is actually a flexible addition to your protective arsenal. The sole drawback to the process is the communities' tenacious desire to make it harder than it really is. After having analyzed nearly 400 System Security Authorization Agreements it's my assertion that the misinformed believe the heavier the document the better it is. The outstanding SSAA's answer the basic who, what, where, when, why, and how with the right combination of words and diagrams to explain the system without rebuilding it on my desk.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

LIST OF REFERENCES

1. DoD Instruction 5200.40, *DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP),* December 30, 1997. http://iase.disa.mil/ditscap/index.html

DoD Manual 8510.1-M, *Department Of Defense Information Technology Security Certification And Accreditation Process (DITSCAP) Application Manual,* July 2000 http://iase.disa.mil/ditscap/index.html

2. NSTISSI No. 1000, National *Information Assurance Certification and Accreditation Process (NIACAP),* April 2000, http://www.nstissc.gov/html/library.html

3. Office of Assistant Secretary of Defense Memorandum, *The Defense Information Systems Security Program (DISSP),* August 19, 1992.

4. CRS Report for Congress. (June 14, 2001). *Health Information Standards, Privacy, and Security: HIPAA's Administrative Simplification Regulations*. Received through the CRS Web Order Code RL30620. Retrieved on 22 July 2001, from http://www.house.gov/htbin/crsprodget?/rl/RL30620

CRS Report for Congress. (March 6, 1998). *Updated Government Performance and Results Act: Implementation During 1997 and Issues of Possible Concern, 105 Congress, Second Session*. Received through the CRS Web 97-1028 STM. Retrieved on 22 July 2001, from http://www.senate.gov/~dpc/crs/reports/pdf/97-1028.pdf

5. White Paper *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63,* **May 1998,** http://www.ciao.gov/CIAO_Document_Library/paper598.htm

6. John Kimbell and Marjorie Walrath, (Spring 01), Life Cycle Security and DITSCAP, *IAnewsletter*, Vol 4, no 2, pp 16-26

Holbrook, P. and Reynolds, J. *RFC 1244: Site Security Handbook*. http://csrc.ncsl.nist.gov/secplcy/rfc1244.txt

Guy Sherburne, (Sept 2000), DoD Information Technology Security Information and Accreditation Process (DITSCAP), Vol 13 http://usamissa.detrick.army.mil/news/newsletters/0009/ditscap.html

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.