Global Information Assurance Certification Paper

I Give A Damn About My System Accreditation!

Introduction to the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) for Information Systems

By Scott A. Hughston

GSEC Version 1.4b

Option 1

Abstract

The Department of Defense (DoD) is required to protect their information and processes to ensure that an appropriate level of confidentiality, integrity, availability, and accountability is maintained to facilitate successful mission accomplishment. The DoD maintains strict control over classified information and the Defense Information Technology Certification and Accreditation Process (DITSCAP) is a major tool that is utilized in order to achieve this level of control. The level of protection that is placed upon the information is based upon its value. The value of information is based upon the impact that the loss, alteration of, denial of access to, or unauthorized access to information would have on the DoD's ability to accomplish its vital missions. This value is placed upon information by the DoD and national-level decision makers and is derived from public laws, and national and DoD regulatory policies. The DITSCAP is a DoD instruction (5200.40) that defines the policies, responsibilities and procedures for accrediting information systems in a way that emphasizes the management of a DoD information system throughout it's lifetime. In a nutshell, the DITSCAP standardizes the Certification and Accreditation (C&A) process, and it applies to all organizations under the DoD. The DITSCAP applies to all systems that require C&A, and is designed to be capable of adapting to any system in any environment for any mission. The DITSCAP has four phases and should be utilized as a guide for the C&A process. Understanding the difference between certification and accreditation is important, one analogy that describes the difference is that certification is the test for your information system and accreditation is the passing grade. The National Information Assurance Certification and Accreditation Process (NIACAP) is similar to the DITSCAP, and provides direction for federal agencies on the implementation of a C&A process for national security systems that are within their operational control and is not discussed further within this document. National security systems fall under all U.S. Government Executive Branch departments, their agencies, and their contractors and consultants.

This document will discuss the C&A process from start to finish and will provide the reader with a basic understanding of the process. Resources for further reading on the DITSCAP are provided and should be utilized on an as needed basis to further your understanding of the process.

Definitions

(5. McGuinness, http://www.timmcguinness.com/ditscap/ditscap3.htm)

Prior to proceeding, the following terms need to be understood in order to facilitate understanding the C&A process utilizing the DITSCAP.

Accreditation: A formal declaration by the Designated Approving Authority (DAA) that an information system is approved to operate in a particular security mode while using a prescribed set of safeguards with an acceptable level of risk.

Certification: The comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a specified set of security requirements. The DITSCAP methodology standardizes the certification process.

Certification 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.

Communications Security (COMSEC): Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

Designated Approving Authority (DAA): The official that has the authority to formally assume the responsibility for operating an AIS at an acceptable level of risk.

Information Systems Security Officer (ISSO): An individual that reports to the DAA, and is responsible for ensuring that the security requirements of an Automated Information System (AIS) are implemented.

Information System (IS) / Automated Information System (AIS): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and includes computer software, firmware, and hardware.

Information Technology Security (ITSEC): The protection of information technology against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and

counter such threats. ITSEC provides the protection and maintenance of confidentiality, integrity, availability, and accountability.

Site Accreditation: Evaluates applications and systems at a specific, self-contained location.

System Accreditation (SA): Evaluates a major system application or a clearly defined independent system.

System Security Authorization Agreement (SSAA): A formal agreement among the DAA(s), the CA, the IT system user representative, and the program manager. It is used throughout the entire DITSCAP to guide actions, document decisions, specify ITSEC requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

Systems Administrator: An individual that reports to the ISSO, and is responsible for the day to day operations of an Automated Information System (AIS).

TEMPEST: Short name referring to the investigation, study, and control of compromising emanations from IT equipment.

Type Accreditation: Evaluates a common application or system that is distributed to a number of different locations.

Why is the DITSCAP important to Information Security Professionals?

The DITSCAP may not be the most exciting topic, but achieving and maintaining C&A of government systems has become increasingly more popular in the world of information security for many reasons. The fall of many internet start-ups over the past view years has pushed many IT workers toward working for organizations that specialize in Government Contracting. This is especially true in the Northern Virginia / Washington, D.C. area. The government is funneling more and more funding into information technology with a significant focus on information security. The Defense Information Security Agency (DISA), the National Institutes of Science and Technology (NIST), the National Security Agency, and numerous other organizations are key players in the Government's information security arena. The tragic events of September 11th and Operation Iraqi Freedom have fueled a renewed interest in the criticality of keeping our information private to maximize the DoD's ability to accomplish its vital mission. The Government has recognized that civilian employees and military members are being stretched to their limits and are utilizing outsourcing to accomplish many specialized and labor intensive tasks. Since the C&A process is one such process, security professionals should try to obtain at least a basic understanding of this process in order to have a well-rounded understanding of Government information system security requirements.

Characteristics of the DITSCAP

The DITSCAP must be extremely flexible and have the ability to accommodate many variations of information systems, architecture, software loads, and implementation plans while maintaining the ability to adapt adequately with the continual changes in technology. In order to accommodate this required flexibility, the DITSCAP is made to be tailorable, scalable, predictable, understandable, relevant, effective, evolvable, repeatable, and responsive. The preceding nine (9) characteristics allow the process to accommodate to nearly any given situation.

The DITSCAP utilizes one main document to record all information gathered during the C&A process. This document is the Systems Security Authorization Agreement (SSAA). The SSAA is utilized to document the agreed upon level of security required prior to the building or development of the system begins or changes are made to an existing system. Upon successful completion of the C&A process, the SSAA becomes the foundation document of the security configuration for the applicable information system.

The DITSCAP certification processes are based upon the system being labeled at one of the possible four certification levels. The certification level that is utilized on a particular system is based upon the many factors, such as the organization's mission, classification of information being processed, the architecture of the information system, the criticality of the system to the mission of the organization, and even the types of users (Corporal Nobody vs. Secretary of Defense). The CA analyses the factors and makes a determination based upon the analysis as to what certification level is recommended. The certification levels are as follows: Level 1 – Basic Security Review; Level 2 – Minimum Analysis; Level 3 – Detailed Analysis; or Level 4 – Comprehensive Analysis. The DITSCAP certification is then performed utilizing one of these four certification levels.

The DITSCAP will assist in mitigating risks for the information system by assisting in the identification of risks, vulnerabilities, and threats. Risks must be managed by identifying, measuring, controlling, and minimizing the security risk that an information system is exposed to a level that is commensurate with the value of the information and assets that are being protected. Risks are the coexistence of a threat and vulnerability. A threat is an event that has the potential to cause harm to an AIS through unauthorized access, destruction of information, disclosure of information, modification of data, and/or denial of service. Vulnerability is a weakness in an overall system that could be exploited. There are threats everywhere, but without vulnerability, the threat is not able to penetrate into the system. Since it is impossible to eliminate vulnerabilities, the goal is to reduce them to an acceptable level for each system.

Phases of the DITSCAP

The C&A process is divided into four phases as previously mentioned. These phases must be accomplished in order and each must be completed prior to moving to the next phase. These phases require significant understanding of the entire C&A process which would indicate that time should be allotted to fully understand all aspects of this process prior to initiating the following phases.

Phase 1 – Definition Phase

The Definition Phase is derived of three process activities. The first activity is documenting the justification or need for the AIS to accomplish the mission. The second activity is the registration activity where the SSAA is drafted. The third activity is the negotiation activity where all parties involved with the AIS from it's inception to accreditation agree on the methods to meet the security requirements that are delineated by the SSAA. During the third phase the following are also identified: System mission; Environment; Architecture, Threats, CA, and DAA. During Phase 1, the security requirements for C&A are documented in the SSAA. This phase is finalized with a documented agreement between the Program Manager, DAA, CA, and the User Representative that represents the results of this phase. These activities are broken down further as follows:

Mission Need: Documentation of the mission need initiates the DITSCAP process. The following are the types of information that need to be documented during this portion of Phase 1: System requirements and capabilities; System mission, function, and interfaces; Organizations operating systems; Operational environment; Information types and classifications; Expected system life cycle; System user characteristics; Intended system/network interfaces. There are two types of documents that are utilized to facilitate this process, the Mission Need Statement (MNS) and the Operational Requirements Document (ORD). The MNS is a high-level requirements document that defines the intended operational capabilities of the AIS. The MNS discusses the threats as they relate to the mission needs. The ORD should be completed during the initialization of the AIS and is derived from the MNS. The ORD identifies the minimum acceptable performance parameters for the AIS such as: Range; Accuracy; Payload; Speed; Mission reliability; Readiness; Diagnostics' effectiveness; Survivability; Safety; and Security.

Registration: The process activity that starts the dialogue between the Program Manager, DAA, and the User Representative is the registration. The nine tasks that must be completed during the registration are as follows: Notify the DAA and User Representative; Prepare the mission description and system identification; Prepare the environment and threat description; Prepare the system architecture description; Determine the system ITSEC class (classification level); Determine the system security requirements; Identify organizations involved and resources

required; Prepare the DITSCAP plan; and Draft the SSAA. The DITSCAP provides a foundation to work from, but there are National, DoD, Service, and Agency security directives, as well as any pertinent organizational or departmental requirements that may also be necessary in order to complete the C&A process. These requirements will be utilized to determine the degree of assurance needed for Confidentiality, Integrity, and Availability within the AIS. Once this is derived, it is utilized to determine the certification level for the system, which in turn delineates the tasks that must be accomplished during the C&A process. Each of the four certification levels require a different level of effort as follows: Level 1 requires that only the checklist be completed; Level 2 requires that the checklist be completed and a minimum level of analysis is conducted; Level 3 requires that the checklist be completed and a detailed analysis is conducted; and Level 4 requires that the checklist be completed and extensive analysis is conducted.

Negotiation: The third and final process in this phase is the negotiation. During negotiation, three goals will need to be accomplished.

The first goal is to work with all parties involved to derive an agreement on the implementation strategy that will be utilized to meet the security requirements that were identified during the registration phase. Two areas that need to be agreed upon are: The AIS certification analysis level and the C&A tasks that are required for that level; and the implementation strategy for each AIS security requirement.

The second goal is to conduct a review of the certification requirements with all key members involved. Specifically, the Project Manager, User Representative, DAA, and CA will need to be present. This review will help the system owner to prepare for the C&A process. This review should result in a successful agreement regarding the level of effort that will be required and it will document the approach that is to be taken to implement the needed security requirements.

The third and final goal of the negotiation process is to utilize the information that was agreed upon and incorporate this information into the SSAA. Upon completion of Phase 1, the next phase will be initiated.

Phase 2 – Verification

The Verification Phase verifies that the system complies with previously agreed upon security requirements. For each life-cycle development activity, there is a corresponding set of security related activities that verify system compliance with the security requirements and evaluates vulnerabilities of the system. This phase consists of two processes, the system development activity and the certification analysis.

The system development activity is commenced by reviewing the SSAA. This review is an initial review as the SSAA is continually reviewed throughout the verification phase. The SSAA is also continually revised during the development and modification of the information system. The development or modification of the information system occurs as the system is being designed or the

modifications are being considered. The SSAA must reflect these modifications and will need to be modified to account for changes in the system. A vulnerabilities list is developed as vulnerabilities are discovered. Documenting these vulnerabilities at this phase will assist in mitigating them as the C&A process moves forward. Test plans will also be developed during this phase and will first validate the interoperability of the system resources, and then will test the effectiveness of countermeasures to the vulnerabilities that were previously identified. Any changes to the previously agreed upon security posture in the SSAA, must be approved by the DAA, Project Manager, and User Representative and then incorporated into the SSAA.

The certification analysis is the second process of the verification phase and is comprised of the following 6 tasks: System architecture analysis; Software design analysis; Network connection rule compliance analysis; Product integrity analysis; Life cycle management analysis; and vulnerability assessment. For each of the preceding tasks, there are four certification levels of analysis that can be performed. Level 1 requires the minimum analysis while, levels 2, 3, and 4 require progressively increasing levels of security related analysis. Upon completion of each of the 6 tasks, a task analysis summary report is generated to document the findings. The summary report should include the following: record of findings, evaluation of vulnerabilities found during the system evaluations, summary of the analysis level of effort, summary of tools used, results obtained, and recommendations. These six tasks can be accomplished concurrently or sequentially. Upon completion of Phase 2, the next phase will be initiated.

Phase 3 – Validation

The Validation Phase evaluates the fully integrated system to validate the system's operation in the specified computing environment within an acceptable level of risk. This phase will also ensure that the system is in compliance with the previously defined requirements of the SSAA. The goal of this phase is to obtain authorization to operate the system at an agreed upon acceptable level of risk. This authorization is the accreditation of the system.

There are three process activities in this phase. The first activity is certification evaluation, which will certify that the fully integrated and operational information system complies with the security requirements of the SSAA. This certification is accomplished by performing rigorous testing of the information system. The second activity is the development of recommendations regarding the accreditation of the information system, and the third activity is the act of making the accreditation decision for the information system. These four activities are broken down further in the following sections.

The Certification Evaluation of the information system is comprised of eight possible tasks. These tasks are as follows: System Security Testing and Evaluation; Penetration Testing; TEMPEST and Red/Black Verification; Validation of COMSEC Compliance; System Management Analysis; Site Accreditation Surveys; Contingency Plan Examination; Risk Management Review. Just like in the Verification Phase, there are four certification levels of

evaluation that may be performed. The level is based upon the ITSEC class that was determined during the Definition Phase.

Security testing and evaluation (ST&E) is performed and the objective is to evaluate the technical implementation of the information system security design and to that the automated procedures follow the SSAA and perform in an acceptable manner.

Penetration testing may also need to be accomplished to address the system's ability to withstand intentional attempts to circumvent security mechanisms. This is accomplished by exploiting the internal, external, technical, and non-technical vulnerabilities of the system in an effort to gain un-authorized access. This penetration testing is accomplished utilizing the minimal security activity checklist that is provided in the DITSCAP at a minimum.

TEMPEST and red/ black Verification is not usually required for Level 1 systems, but is usually required for Level 2, 3, & 4 systems. There are many resources available to verify compliance with TEMPEST and Red/Black Separation requirements available and full compliance is beyond the scope of this document.

If communications security (COMSEC) applies to the information system, validation of the appropriate use of COMSEC equipment and materials must be performed. This includes evaluation of COMSEC operational and security requirements, cryptography usage and key management. COMSEC does not usually apply to Level 1 systems, but may apply to systems at Levels 2, 3, & 4.

System management analysis is conducted which validates that security management procedures are in place, operational, and effective. This analysis also verifies that a configuration management and change control policies are being utilized to consider the security implications on all modifications of the information system prior to their implementation.

A site accreditation survey is conducted to evaluate the installation of the information system, site procedures and practices, and environmental requirements that are unique to each particular location. This survey ensures that the information system is installed in accordance with the approved design.

Evaluation of the Contingency Plans ensures that reasonable continuity of information system support if a contingency prevents normal operations from continuing.

The risk management review is an evaluation of the system security design against the concept of operations, operational environment, security policy requirements, and known threats. This review verifies that the risks to confidentiality, integrity, and availability are at an acceptable level. A risk analysis is conducted and focuses on five key areas: physical/personnel security; administrative/operational security; communications/emanations security; hardware/software/firmware security; and data/information security. This risk assessment will determine if countermeasures are adequate to limit the probability or impact of loss to an acceptable level. The assessment will identify the risks, recommend appropriate countermeasures, and discuss the pros and cons to implementing each countermeasure.

Developing recommendations is the second process activity of the Validation Phase. The recommendations that are developed during this phase are provided to the DAA and are based upon the certification evaluation findings, deficiencies, and risks to the mission and operation. The findings and the certifier's recommendations are documented in a task analysis summary report, which is then submitted to the DAA for consideration.

The Accreditation decision is the final process activity in the Validation Phase. The DAA can accredit or approve the information system, grant interim approval to operate (IATO) the information system, or disapprove the system. Special circumstances could cause the DAA to provide an IATO if critical mission requirements are prevalent, but provide only temporary authorization to operate and require the remaining parts of the process to be completed as soon as possible or as directed. If the DAA disapproves the information system, the DITSCAP will have to be restarted from the beginning. Disapproval rarely occurs if the DITSCAP was properly utilized and followed during the C&A process.

Phase 4 – Post Accreditation

The Post Accreditation Phase begins upon successful completion of the C&A of the information system. This phase monitors system management and operation to ensure that the system continues to operate within the previously agreed upon acceptable level of risk. Security management, change management, and periodic re-validation reviews are conducted.

The first process activity in the Post Accreditation phase is system operation. This activity includes all of the tasks necessary to maintain the information system at an acceptable level of residual risk and for managing system change. Maintaining the SSAA is instrumental in this process and should be accomplished by the Information System Security Officer (ISSO) periodically. Revisions that are deemed necessary by the ISSO must be submitted to and approved by the DAA, the Project Manager, and the User Representative. Ensuring that the system maintains a secure state is an ongoing process and must be effectively managed. Changes to the threat environment must also be tracked, since threats are continually becoming more and more sophisticated. Tracking these threats will assist in strengthening the countermeasures that are utilized to mitigate the risk to an acceptable level.

The second process activity in the post-accreditation phase is compliance validation. This activity ensures that the information system is continually in compliance with the security and operational requirements that are in the SSAA. Compliance validation also includes periodic re-testing, system evaluations, and inspections of facilities, equipment, and procedures as defined in the SSAA. During compliance validation, there are five tasks that need to be completed and each task has the same four possible certification levels that correspond to the levels that have been used throughout this document.

The first task is to evaluate the operations of the previously accredited system to ensure that it continues to comply with the SSAA.

The second task is to review the contingency plans to evaluate whether the

appropriate level of contingency planning has been maintained for the applicable certification level.

The third task is to evaluate compliance with TEMPEST requirements as applicable.

The fourth task is to evaluate how well COMSEC requirements are being maintained within the system as defined in the SSAA.

The fifth and last task is to perform risk management analysis to determine if counter-measures are adequate to maintain the probability or impact of loss at an acceptable level.

The findings of the compliance validation are documented in the task analysis summary report which should contain an evaluation of the vulnerabilities discovered, summary of analysis level of effort, summary of tools used and the results obtained, and recommended actions. This report is submitted to the DAA for approval. The Post-Accreditation phase of the DITSCAP assists in ensuring compliance with the SSAA while assisting the information system to continually operate in a secure manner.

Summary

These are the four main phases of the DITSCAP that provide a foundation from which to certify and accredit information systems that are associated with the DoD. This process is very thorough and requires an extensive number of man-hours and a significant amount of communication to accomplish correctly. If utilized properly, this tool can be used to facilitate the successful completion of the accreditation of even the most complex DoD information systems.

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

2. The Department of Defense Information Technology Certification and Accreditation Process (DITSCAP) Application Manual, July 31, 2000, http://www.dtic.mil/whs/directives/corres/pdf/85101m_0700/p85101m.pdf

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

4. NIST Certification and Accreditation Project Website, http://csrc.nist.gov/sec-cert/ca-process.html

5. McGuinness, Tim, The DITSCAP Web Resource Site, DITSCAP Definitions, http://www.timmcguinness.com/ditscap/ditscap3.htm

6. NIST Special Publication 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, October 2002, http://csrc.nist.gov/sec-cert/SP-800-37-v1.0.pdf

7. National Security Telecommunications and Information Systems Security (NSTISS) Red/Black Installation Guidance, NSTISSAM TEMPEST/2-95, Revised 10 September 1998.

8. Information Assurance, DoD Directive 8500.1, 24 October 2002.

9. National Security Telecommunications and Information Systems Security Committee (NSTISSC), National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, September 2000.