Global Information Assurance Certification Paper

Thomas Connelly
October 13, 2003
GSEC Practical Version 1.4b Option 1

Army C&A: An Updated Look at the DITSCAP

1.0 Introduction (Abstract)

This paper describes the process of a site-based Certification and Accreditation (C&A) of a Level 2 system using the Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP). While the DITSCAP is a DoD process, the Army has its own specific requirements that must be addressed when conducting the DITSCAP.

This paper will explain what the DITSCAP is, and then examine each task within each phase of the DITSCAP. For each task within Phase 1 Definition, the documentation required, regulations that mandate required actions or establish standards, and the resulting section of the SSAA will be discussed. Next, this paper will discuss each task within Phase 2 Verification, and give some suggestions on building tests for Phase 3 Validation, and then examine the requirements for the Phase 3 tasks. Finally, Phase 4 Post Accreditation, and some of the issues faced in this phase will be discussed.

2.0 What is the DITSCAP?

The DITSCAP is the process by which the DoD standardizes the C&A of all information systems in the environment in which the system is designed to operate. For example, a system that is used in an office environment is accredited for that environment, whereas a system that is designed for use on the battlefield is accredited for use in that environment. Since there is no standard security solution for every system, the DITSCAP is tailorable for any system, regardless of the type of system or where it is in its lifecycle. The DITSCAP applies to Collateral Classified, Sensitive, and Unclassified information systems. The DITSCAP does not apply to DoD Intelligence Information Systems (DoDIIS), Sensitive Compartmentalized Information (SCI) Systems, or cryptographic systems.

2.1 Certification

Certification is the comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements[1]. Certification encompasses physical, procedural, and personnel security, as well as all the technical aspects of information systems security, such as Identification and Authentication (I&A) and access controls. In other words, certification is the testing of the system to ensure it complies with the identified security

[1] DoD 8510.1-M p. 9.

requirements and to validate that all countermeasures to protect the system function as advertised.

2.2 Accreditation

Accreditation is the formal declaration by a Designated Approving Authority (DAA) that a system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.[2] For an Army system, the DAA must at least be a GM/GS-14 or Lieutenant Colonel (LTC) or above.

2.3 Issues

When the DoD 8510.1-M DITSCAP Application Manual was written, some discrepancies were not resolved. One discrepancy was a result of policy outpacing the regulations. This caused the requirements for an SSAA in the DoD 8510-1.M to be different than the one in the Department of Defense Instruction (DoDI) 5200.40 DoD IT Security Certification and Accreditation Process (DITSCAP). For example, the DoDI 5200.40 discuses the term ITSEC Class, and TCSEC, which is now called the Certification Level in the DoD 8510.1-M. When there is a discrepancy between the DoDI 5200.40 and the DoD 8510.1-M, the DoD 8510.1-M should be used.

3.0 Phase 1: Definition

The DITSCAP begins with Phase 1 Definition. Throughout Phase 1, information about the system is developed and collected. As the SSAA is developed, the DAA, Certifier, User Representative, and Program Manager must arrive at a consensus on the following: the mission of the system, the certification and accreditation boundaries of the system, the security requirements of the system, the level of effort (or degree of analysis) that will be applied to the system, and the resources required to accredit the system. Phase 1, consists of three activities: Preparation, Registration, and Negotiation. In Phase 1, each activity contains unique tasks and all activities and tasks must be conducted.

3.1 Preparation

The first activity in Phase 1 is Preparation. Preparation consists of Task 1-1 Review Documentation.

3.1.1 Task 1-1 Review Documentation

In Task 1-1, all documentation that pertains to the system, the information the system processes, and all applicable regulations must be collected and analyzed. Determining what documentation is available (and whether it does or does not meet the required standard) will help determine the schedule for completing the DITSCAP, as well as any additional work that needs to be done. Additionally, if the system is being re-accredited, this will facilitate the process, as most of the documentation should be available.

[2] DoD 8510.1-M p. 8.

3.1.1.1 Business Case or Mission Needs Statement

When reviewing the documentation, the first item to assess is the business case analysis or Mission Needs Statement (MNS). This document is the justification for the existence of system. Most systems have neither a MNS nor a business case analysis. This does not mean one must be created when building the SSAA, however, the system must be described at the same level of detail as in the MNS or business case analysis. The DoDI 5200.40 DITSCAP[3] states the MNS consists of six parts:

1. System Mission, Functions, and System Interfaces. This section describes the mission of the system. The mission statement consists of the who, what, when, where, and why of the system. The first section of the mission needs statement also describes the functions that the system is designed to perform and all system interfaces.
2. Operational Organization. This section details the name and location of the organization the system supports.
3. Information Category and Classification. This section describes the type of information the system processes: Classified, Sensitive, or Publicly Available.
4. Expected System Lifecycle. This describes where the system is in its lifecycle. For a site-based accreditation it will most likely be in the operational stage.
5. System Users Characteristics. This section describes the users of the system, for example, the type of security clearance the users have and the type of personnel security investigation the users have gone through.
6. Operational Environment describes the surrounding area and conditions in which the system is designed to operate.

3.1.1.2 Regulations

The second items to review are the Federal and organizational Information Assurance (IA) and security policies. Some of the organizational policies are DoD, Army, Major Army Command (MACOM), and installation. Once all the regulations and policies have been reviewed, all available system documentation must then be reviewed. The reviewer will then determine if the system documentation is complete and to regulatory standards. If any document is not to standard it must be corrected. Understanding the standard before reviewing the system specific documentation will reduce the likelihood of having to return to Phase 1 at a later point in the certification effort to correct a portion of the SSAA, or one of its appendices. For example, a Contingency Plan must meet the standards set forth in AR 380-19 and DA Pam 25-1-1 Installation Information Services, Chapter 8, and Appendix E. If the Contingency Plan is not to standard, it is preferable to identify the problems and correct the deficiencies in this phase, than at Phase 2 or Phase 3 of the DITSCAP.

[3] DoD1 5200.40, p. 20.

3.1.1.3 System Specifications and Diagrams

After reviewing the regulations and policies, the next items to review are the system specifications, architecture and design documents, and network diagrams. These documents provide technical insight into the system. They will aid in determining if the system meets the Army Networthiness requirement and the Joint Technical Architecture-Army compliance requirement concurrently as the system is completing the DITSCAP. The Army Networthiness program is an attempt to determine the capabilities and risks associated with a system, and the impact of those risks to the entire Army network. The Army's Networthiness Implementation Guidance, which explains how to submit for the Networthiness Certification, has not been completed. Mission essential and mission critical systems may receive Networthiness Certification if they register in the Army Information Technology Registry (AITR), which may be done through Army Knowledge Online (AKO). Non-mission essential and Non-mission critical systems are currently not eligible for the Networthiness Certification.

The Army also requires systems to be compliant with the Joint Technical Architecture-Army version 6.5 by the end of fiscal year 2006[4]. A system is considered compliant if it meets the standards of the JTA-A or has an approved plan to meet the JTA-A standards. Technical Architecture (TA), defined in AR 25-1 is "The minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements of a system to ensure that a system satisfies a specified set of requirements. A TA identifies services, interfaces, standards, and their relationships."[5]

3.1.1.4 Configuration Management Documents

These documents are important because they mandate how change to the baseline of a system is managed. These documents also give insight into any future changes that are under consideration. For example, one major change coming for the Army is the migration to Windows 2000 Active Directory. The configuration management documents may provide insight to the timeline and the future structure of the system when the migration takes place.

3.1.1.5 User Manuals and Operating Procedures

This documentation consists of all available documentation for the system. For example, some documentation may describe how users interact with the system from initial logon to final logoff of the system. If there is scheduled maintenance that is performed on the system each week, this documentation details that maintenance. Some other items that may be covered include supply manuals, training manuals, or Standing Operating Procedures (SOP).

---

[4] AR 25-1, p. 20.

[5] AR 25-1, p. 106.

3.2 Registration

The second activity of Phase 1 is Registration. Registration consists of Task 1-2 through Task 1-9. In this activity, a baseline for the system is established and a draft SSAA is completed. When developing the SSAA it is best to explain all the details of the system in the appropriate appendices, and use a general description of the system in the SSAA document. This will facilitate maintaining the SSAA as changes to the system take place.

3.2.1 Task 1-2 Prepare System Functional Description and System Identification

In Task 1-2, the following items are defined[6]: System Name and Identification (1.1), System Description (1.2), Functional Description (1.3) and System CONOPS (1.4).

System Name and Identification (1.1) includes the name of the system entering the C&A, the organization that owns the system, and the location of the organization.

System Description (1.2) must include a description of the system's capabilities, diagrams, and components, as well as its purpose.

The Functional Description (1.3) includes all the capabilities and functions of the system to be accredited. This section will be broken down into the following subsections: System Capabilities (1.3.1), System Criticality (1.3.2), Classification and Sensitivity of Data Processed (1.3.3), System User Description and Clearance Levels (1.3.4), and Lifecycle of the System (1.3.5).

System Capabilities (1.3.1). This section describes the capabilities the system requires in order to perform its mission.

System Criticality (1.3.2). This section describes the importance of the system in performing the mission and details the implications of a non-operational system. The Mission Assurance Category (MAC) of the system is described in this section. The MAC is defined in DoDI 8500.2 Information Assurance Implementation as having three levels. MAC I systems are "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."[7] An example of a MAC I system is an automated weapon system, because if the weapon system was not operational, the mission effectiveness of the deployed or contingency forces would be degraded. MAC II Systems are: "Systems handling information that is important to the support of deployed and contingency forces."[4] An example of a MAC II system might be a system that processes intelligence information. MAC III Systems are: "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."[4] An example of a MAC III system is a system that processes training records or payroll.

Classification and Sensitivity of Data Processed (1.3.3). This section describes type and sensitivity of information the system processes, as well as any special handling

[6] The number in parenthesis refers to the actual location within the SSAA.

[7] DoDI 8500.2, p. 22.

requirements for the information. The Confidentiality Level of information the system processes as described in DoDI 8500.2 Information Assurance Implementation may also be described in this section. There are three Confidentiality Levels within the DoD: Classified, Sensitive, and Publicly Available. Identifying the MAC and Confidentiality Level of the system and ensuring the system complies with the appropriate appendices in the DoDI 8500.2 will help ensure that the system and information are protected accordingly. This will also aid the transition to the Defense Information Assurance Certification and Accreditation Process (DIACAP), when the DIACAP replaces the DITSCAP.

System User Description and Clearance Levels (1.3.4). This section describes the users of the system and their rights to access the data. First, it discusses the Security Clearance/Personnel Security Investigation, Formal Access Approval, and Need-to-Know to access the information on the system for each user. These three factors determine the Mode of Operation of the system: Dedicated, System High, Compartmented, and Multilevel.

In a Dedicated system, all users have met all three information access requirements: all users have undergone an investigation and received the highest level of clearance corresponding to the level of information processed on the system; they have been granted formal access approval to all information and have a need-to-know. If the system operates in the System High mode, all users have a clearance equivalent to with the highest classification of information processed on the system and formal access approval, but have the need-to-know only for some information. If the system operates in the Compartmented mode, all users have a clearance commensurate with the highest classification of information processed on the system, but users only qualify for the remaining access requirements for that information to which they have access. If the system operates in the Multi-level mode users meet all three requirements only for that information to which they have access.

Lifecycle of the System (1.3.5). This section describes where the system is in its lifecycle. Most systems undergoing a site-based Level 2 certification will be in the Operational/Maintenance phase.

System CONOPS Summary (1.4). This section summarizes the concept of how the system functions. This includes functions and interfaces with other systems, how the information is processed, what the information is used for, etc. It may also include diagrams. The full System CONOPS is in Appendix D of the SSAA.

3.2.2 Task 1-3 Register the System

In this task, key individuals such as, DAA, Certifier, User Representative, or the organization that will be certifying the system must be identified. Typically, this has already been done prior to the start of the certification effort.

3.2.3 Task 1-4 Prepare the Environment and Threat Description

For Task 1-4, the environment in which the system will operate is described. This will result in Section 2.1 Operating Environment, which includes the following subsections: Facility Description (2.1.1), Physical Security (2.1.2), Administrative Security (2.1.3),

Personnel (2.1.4), Communications Security (COMSEC) (2.1.5), Transient Electromagnetic Pulse Emanations Standards (TEMPEST) (2.1.6), Maintenance Procedures (2.1.7), Training Plans (2.1.8), System Development, Integration, and Maintenance Environment (2.2), and Threat Description and Risk Assessment (2.3).

Facility Description (2.1.1). This includes diagrams, descriptions of environmental controls (such as air conditioning), floor plans, etc in which the system resides.

Physical Security (2.1.2) describes, for example, how an individual might gain access to all levels of the system (e.g. server and workstation) if he or she started outside the installation that hosted the system. For example, before entering an installation, an individual may have to show a picture ID and submit to a vehicle search. Once on the installation, the person must now sign in at a guard desk. A user would then have to unlock his office door before finally gaining access to the system.

Administrative Security (2.1.3) covers all the security policies and procedures that act as countermeasures to mitigate threat. Some of these include an Acceptable Use Policy; Rules of Behavior, which is Appendix J of the SSAA; and Standing Operating Procedures.

The Personnel (2.1.4) section describes the users of the system. This will include the type of clearances, personnel security investigations, and functions the users have within the system.

The COMSEC (2.1.5) section describes how the system employs and protects cryptographic keys. This section states what type of cryptography is used (e.g. NSA approved, NIST approved), what the cryptography is used for, how the cryptography is used, and details the cryptographic key management procedures.

TEMPEST (2.1.6) section states if the system has any TEMPEST or Red-Black requirements. TEMPEST is the study of compromising emanations. The Red-Black requirements are discussed in NSTISSAM 2-95 TEMPEST. Red-Black refers to the physically and electrically separated cables and equipment which distinguish the classifications of information processed. Red cables and equipment process unencrypted classified information. Black cables and equipment process unclassified and/or encrypted information[8]. To determine if a system has TEMPEST requirements, the TEMPEST Control Officer must consult AR 381-14 (S) Technical Surveillance Countermeasures (TSCM and TEMPEST) (U).

The Maintenance Procedures (2.1.7) section details the preventive maintenance requirements of the system. If contractors are conducting maintenance on the system, the contractual requirements should be stated.

Training Plans (2.1.8). This section outlines the training requirements for the individuals responsible for administrating the system. The required training for the individuals depends on the positions they hold. The training plans must reflect the training requirements from the Army's Office of the CIO/G-6, DISC4 Message 10 September 2001. This requires individuals who hold an IA position to be certified in that position,

[8] NSTISSAM 2-95 TEMPEST, Section 4-3.

and take refresher training every eighteen months. System administrators are required to complete Level 1 and Level 2 training within six months of assuming their SA position[9].

System Development, Integration, and Maintenance Environment (2.2). This section only applies if the organization conducting the C&A is a developer, integrator, or maintainer of software or hardware, and if there is a correlation between the development activity and the operation of the system. If applicable, a determination must be made if the system is an open or closed environment. The system is considered a closed environment if all of the developers or integrators of the system have a clearance at least equal to the level of information processed on the system, and changes to the system are made only after the Configuration Control Board (CCB) has carefully reviewed and assessed the impact of the change. An IT security manager or a security engineer must be on the CCB. If these requirements do not apply, the system is in an open environment.

Threat Description and Risk Assessment (2.3) describes all of the potential threats and vulnerabilities to the system. The threats and vulnerabilities must be paired, and countermeasures selected for each threat/vulnerability pair. For each threat/vulnerability pair, a statement of residual risk, along with the rational for accepting this risk, must be written. This section is a summary of the risk assessment to the system with a full risk assessment in Appendix Q Residual Risk Assessment Results.

3.2.4 Task 1-5 Determine the System Security Requirements

This task results in a listing of all the requirements the system must meet and the regulation or policy from which the requirement was derived. All of these requirements are listed in a Requirements Traceability Matrix (RTM), which will be Appendix F of the SSAA. At the end of this task, National and DoD Applicable Instructions or Directives (4.1), Governing Security Requirements (4.2), Data Security Requirements (4.3), Security Concept of Operations (S-CONOPS) (4.4), Network Connection Rules (4.5), Configuration Management (4.6), Re-Accreditation Requirements (4.7), and Appendix F: RTM are completed.

National and DoD Applicable Instructions or Directives (4.1), Governing Security Requirements (4.2), and Data Security Requirements (4.3) describe the requirements the system must meet. These sections should be general descriptions and refer to Appendix F: Requirements Traceability Matrix (RTM) for a complete list of requirements and Appendix C References for a complete list of regulations and policies from which the requirements were derived.

Security Concept of Operations (S-CONOPS) (4.4) describes the security portion of Appendix D CONOPS, and the applicable portions of Appendix E Information System Security Policy and Appendix M Personnel Controls and Technical Security Controls. Additionally, if a Trusted Facility Manual (TFM) or Security Features Users Guide (SFUG) is available, these should also be referenced. The TFM and SFUG are DoD

[9] DISC4 MSG 100733Z Sep 01, Section 3F.

5200.28-STD (Orange Book) requirements. DoD Directive (DoDD) 8500.1 and DoDI 8500.2 canceled the DoDD 5200.28, DoD 5200.28-M, and DoD 5200.28-STD, however the SFUG may be available from a previous accreditation. The TFM is still a requirement for Type accredited items and may be available if the system includes any Type accredited items. The S-CONOPS should also discuss the Level of Robustness for an information system. For the DoD, there are three levels, High, Medium, and Basic. The Level of Robustness is determined from the system's internal and external exposure. The internal exposure is the difference between the actual access privileges users of the system have and what regulation mandates it should be. The external exposure of the system is determined by how isolated a system is from other systems, either physically or logically. If the system processes classified information, it is required to have a High Level of Robustness. A system that processes sensitive information is required to have a Medium Level of Robustness. A system that processes publicly available information is required to have a Basic Level of Robustness.

Network Connection Rules (4.5) state the requirements another system must meet in order to connect to the system undergoing the C&A. These requirements must also be stated in the Memorandum of Agreement with the connecting system.

Configuration Management (4.6) details the policies and practices of how change to the system's baseline is managed. In the interest of limiting the volume of the SSAA, it is recommended that only a summary of the CM policy and practices be documented in this section and detailed in Appendix I Applicable System Development Artifacts or System Documentation or a separate appendix. The DoD 8510.1-M only has specific requirements for Appendix A through Appendix R. All letters after 'R' are available.

Re-Accreditation Requirements (4.7). All systems will be reaccredited within three months if one of the conditions in AR 380-19 Information Systems Security occurs: "Addition or replacement of a major component or a significant part of a major system"[10] (e.g., replacing a server), "a change in classification level of information processed" [10] (e.g., the system used to process sensitive information, and now processes Secret information), "a change in security mode of operation" [10] (e.g., the system went from System High to Compartmented), "a significant change to the operating system or executive software" [10] (e.g., the system upgraded from Windows NT to Windows 2000 Server Active Directory), "a breach of security, violation of system integrity, or any unusual situation that appears to invalidate the accreditation" [10] (e.g., a hacker gained access to the system), "a significant change to the physical structure housing the AIS that could affect the physical security described in the accreditation" [10] (e.g., the system moved from one installation to a different installation), "the passage of 3 years since the effective date of the existing accreditation, a significant change to the threat that could impact Army systems, a significant change to the availability of safeguards, and a significant change to the user population" [10] (e.g., a high user turnover). For each of the conditions listed above, a determination must be made as to what constitutes a major change or changes significant enough to require re-accreditation.

[10] AR 380-19, p.17.

Once all applicable regulations have been identified, an RTM must be developed. An RTM is a list of all regulatory requirements that the system must meet. These requirements are broken down into categories such as Access Controls, Physical Security, Media Security, etc. In each of the categories, all of the corresponding requirements are listed, starting with national policy, followed by DoD policy, Army policy, local policy and finally, organizational policy. Developing an RTM is a very time intensive task. To facilitate the process, there is an RTM Database available from the DISA website (http://iase.disa.mil/ditscap/rtmdatabase.html). While this tool provides a good starting point, one major issue is the listed regulations are not current. For example, generating a basic RTM for an Army system with this tool will result in a document that is more than ninety pages long. A number of the requirements listed in this RTM are from DoDD 5200.28 (Orange Book). This means, when generating the RTM all references to the DoDD 5200.28 must be removed along with all other canceled regulations. Then they must be replaced with the most current DoD regulations. A second problem with the DISA RTM tool is the only Army policy that is referenced is AR 380-19. When creating the RTM all other applicable regulations and policies must be added. Some of those regulations include, but are not limited to: AR 380-5, AR 380-53, AR 25-1, AR 25-10, and DA Pam 25-1-1. A more comprehensive list of Army regulations can be found at the Army Publishing Directorate website (http://www.apd.army.mil), and policy may be found at the Information Assurance website (Army Knowledge Online (AKO) account required). Also, current Army policy states that AR 380-19 is still in effect except for those areas covered under DoDI 5200.40 and DoD 8510.1-M. This means that all AR 380-19 references in the DISA RTM tool must be verified to see if they are still valid.

3.2.5 Task 1-6 Prepare the System Architecture Description

Task 1-6 results in the completion of the following sections: System Architecture Description (3.1), System Interfaces (3.2), Data Flows (3.3), and Accreditation Boundary (3.4).

The System Architecture Description (3.1) includes a description of the hardware, software, and firmware. A short summary of the system's equipment should be provided, and a complete list of equipment should be in Appendix I Applicable System Development Artifacts or System Documentation or a separate appendix. This section may state if the system meets the Joint Technical Architecture-Army 6.5, and reference Appendix I Applicable System Development Artifacts or System Documentation or a separate appendix that describes how the system meets this future requirement. Letters after 'R' are available for use if these items are going to be placed in a separate appendix.

The System Interfaces (3.2) section describes all of the external connections of the system. Each external connection must also have a Memorandum of Understanding or Memorandum of Agreement (MOU/MOA), which outlines all of the security requirements to connect to the system. Each MOU/MOA is placed in Appendix N Memorandums of Agreement. This section also includes or references the Systems Architecture Diagrams that are outlined in AR 25-1 Information Management. The Systems Architecture is:

> A description, including graphics, of systems and interconnections, providing for or supporting warfighting functions. It defines the physical connection, location, and identification of key nodes, circuits, networks, and warfighting platforms and specifies system and component performance parameters.[11]

The Data Flows (3.3) of a system are defined in the Operational Architecture, which is described in AR 25-1 Information Management as, "a description (often graphic) of the operational elements, assigned tasks, and information flows required to accomplish or support a warfighting function."[12] The system's internal interfaces must also be defined.

The Accreditation Boundary (3.4) can be determined by first determining over which components of the system the DAA has direct physical and logical control. There are several ways to determine the accreditation boundary of an operational system. A system may be accredited as a single unit, such as a group of stand-alone systems in a room; as a single system, such as a LAN; or as a system of systems, such as LAN with similar functions grouped together. An example of a system of systems accreditation would be a DAA that is responsible for multiple LANs. That DAA may assign a GM/GS-14 or LTC to be the DAA of a LAN. The top DAA would then take the accreditations of those systems and use them as appendices to his SSAA.

3.2.6 Task 1-7 Identify the C&A Organizations and the Resources Required

This task outlines all of the responsibilities of the individuals and organizations conducting the DITSCAP. The following sections are completed: Organizations (5.1), Resources (5.2), Resources and Training Requirements (5.3), and Other Supporting Organizations (5.4).

The Organizations (5.1) section identifies which organizations or individuals hold the position of DAA, Certifier, Program Manager, and User Representative. The responsibilities of each of these individuals or organizations are also outlined.

Resources (5.2) to perform the certification are identified in this section. If a contractor is performing the role of the Certifier or Certification Team, funding must be allocated to pay for the contractor's services.

Resources and Training Requirements (5.3). It may be necessary to send an individual to training in order to complete the DITSCAP. For example, the system administrator may have to attend the Vulnerability Assessment Certification training in order to run scanning software on the network. Funding must be allotted to send the system administrator to this training. This section must include equipment needed for the training, the individual responsible for conducting the training and where the training will occur.

Other Supporting Organizations (5.4). Any other organizations that are involved in the DITSCAP are listed here, along with their responsibilities. For example, if a higher

[11] AR 25-1, p. 106.

[12] AR 25-1, p. 103.

headquarters reviews the SSAA for completeness and accuracy, this higher headquarters is named.

3.2.7 Task 1-8 Tailor the DITSCAP and Prepare the DITSCAP Plan

The Certification Level of the system is determined, and a certification plan is developed and tailored for the system in Task 1-8. This task results in the following sections: Tailor the DITSCAP (6.1), Adjust for Programmatic Considerations (6.1.1), Identify Security Environment (6.1.2), and Identify IS Characteristics (6.1.3), Level of Effort (6.4), Milestones (6.2), Schedule and Summary (6.3), and Roles and Responsibilities (6.5).

The DITSCAP was designed to be tailorable for any system, regardless of where the system is in its lifecycle. Task 1-8 tailors the DITSCAP for the system undergoing the C&A. Tailor the DITSCAP (6.1) has three subsections: Adjust for Programmatic Considerations (6.1.1), Identify Security Environment (6.1.2), and Identify IS Characteristics (6.1.3).

Adjust for Programmatic Considerations (6.1.1). If there is a planned major change to the system, that change is addressed in this section. For example, if the system were migrating to Windows XP Professional, this section would discuss the timeline of the migration and when that portion of the system would be tested.

Identify Security Environment (6.1.2). Any additional security requirements that would affect the C&A effort are discussed in this section.

Identify IS Characteristics (6.1.3). Any characteristics of the system that would affect the C&A effort should be discussed in this section. For example, there may be a cryptographic device that is part of the system that the C&A team is unable to test.

The Certification Level, or degree of analysis to which the system will be tested, is also determined in Task 1-8. Level 1 is Minimum Security Checklist, Level 2 is Minimum Analysis, Level 3 is Detailed Analysis, and Level 4 is Comprehensive Analysis. The Certification Level can be determined using the table in DoD 8510.1-M[13]:

Table C3.T9. System Characteristics an Weights

Characteristic	Alternatives and Weights	Weight
Interfacing Mode	Benign (w=0), Passive (w=2), Active (w=6)	
Processing Mode	Dedicated (w=1), System High (w=2), Compartmented (w=5), Multilevel (w=8)	
Attribution Mode	None (w=0), Rudimentary (w=1), Selected (w=3) Comprehensive (w=6)	
Mission-Reliance	None (w=0), Cursory (w=1), Partial (w=3), Total (w=7)	
Availability	Reasonable (w=1), Soon (w=2), ASAP (w=4) Immediate (w=7)	
Integrity	Not-applicable (w=0), Approximate (w=3), Exact (w=6)	
Information Categories	Unclassified (w=1), Sensitive (w=2), Confidential (w=3), Secret (w=5), Top Secret (w=6), Compartmented/Special Access Classified (w=8)	
	Total of all weights	

[13] DoD 8510.1-M, p. 53.

Interfacing mode characterizes the system's interaction with other systems. For example: A Benign system may be a stand-alone computer; a Passive System may receive information from another system, but not send that system any information; and an Active System would send and receive data to another system.

Processing Mode refers to the Mode of Operation of the system: Dedicated, System High, Compartmented, or Multilevel.

Attribution Mode refers to the requirements to trace the manipulation of information to users or processes. Since AR 380-19 requires a minimum amount of auditing, no system will be 'None'.

Mission-Reliance refers to how important the system is to the mission of the organization.

Availability refers to how soon the system and information is required to be on hand from a security standpoint.

Integrity refers to how important the exactness of the data or information on the system is to accomplishing the mission. For example, if a text document may be opened and read in either Notepad or MS Word, the level is Approximate. If the text document must be opened in only MS Word, the level is Exact.

Information Categories refers to the information processed on the system: Unclassified, Sensitive, Confidential, Secret, Top Secret, or Compartmented/Special Access Classified.

Once all of the system characteristics have been determined, the Certification Level is determined using the following chart from DoD 8510.1-M[14]:

Table C3.T10. Certification Level

Certification Level	Weight
Level 1	If the total of the weighing factors in Table C3.T1. are < 16.
Level 2	If the total of the weighing factors in Table C3.T1. are 12 - 32.
Level 3	If the total of the weighing factors in Table C3.T1. are 24 - 44.
Level 4	If the total of the weighing factors in Table C3.T1. are 38 - 50.

The overlapping of the numbers allows a DAA to be flexible in the certification of the system. However, if the system is certified at too high a level, unnecessary funding and time will be spent. If the system is certified at too low a level, the DAA may be held liable for any incident that occurs. How the Certification Level is determined is detailed in Level of Effort (6.4).

Tasks and Milestones (6.2) and Schedule and Summary (6.3) outline the plan to complete all tasks of the DITSCAP with approximate dates listed as goals for completion. This section also outlines when Compliance Validation is to be completed.

[14] DoD 8510.1-M, p. 59.

Compliance Validation is a Phase 4 activity that requires all applicable Phase 2 and Phase 3 tasks to be revalidated.

Roles and Responsibilities (6.5). This section refers to all individuals, organizations and their respective duties involved in the DITSCAP that were not covered in Organizations (5.1).

3.2.8 Task 1-9 Draft the SSAA

Now that Task 1-1 through Task 1-8 have been completed, all of the parts to the SSAA have been completed and must be assembled. If Task 1-2 through Task 1-8 have been completed concurrently, one individual should be responsible for ensuring the other tasks were completed to standard as he incorporates them into the SSAA. This person will most likely be the Certifier.

3.3 Negotiation

Negotiation is the final activity of Phase 1. In this activity, the DAA, Program Manager, Certifier, and User Representative must come to a consensus. The consensus is arrived at in Task 1-10 through Task 1-12.

3.3.1 Task 1-10 Conduct Certification Requirements Review and Task 1-11 Establish Agreement on Level of Effort and Schedule

Task 1-10 and 1-11 are conducted concurrently. In Task 1-10, the DAA, Certifier, User Representative, and Program Manager will review the SSAA to ensure it accurately describes the system, the requirements for the system to be certified, the level of effort of the certification, and the schedule of the certification. In Task 1-11, the four individuals come to an agreement on those items.

3.3.2 Task 1-12 Approve Phase 1 SSAA

This is the final task of Phase 1. In this task, the DAA, Certifier, User Representative, and Program Manager must all come to a consensus on the mission of the system, the level of effort of the certification, the security requirements, C&A boundaries, and the resources required. Since the DAA is the senior individual assuming the risk of operating the system, it is possible that the DAA tells the Certifier, User Representative, and Program Manager what the consensus will be, however, the intent of the DITSCAP is for a true agreement to be reached. By the end of this task the initial draft SSAA is complete, and the system is ready for Phase 2 Verification. DoD 8510-1.M only requires the DAA to approve the SSAA; however, it is recommended that the Certifier, User Representative, and Program Manager all sign the SSAA at the end of each phase. This will prevent any of those individuals from stating they had previously not agreed to something at a later point in the certification effort.

4.0 Phase 2 Verification

The purpose of Phase 2 Verification is to ensure that the system is described accurately in the SSAA and to prepare the validation method of all the security requirements that have been identified. Throughout this phase, the certification team may discover more about the system and its operational environment. This requires the SSAA to be

updated and all parties to agree upon the updates. Phase 2 consists of two activities, both of which must be conducted, but only tasks that apply to the system must be completed.

4.1 Systems Activities: Integration or Development

This activity consists of the actions required to integrate the components of the system to meet the functional and security requirements. This activity is for acquisition organizations and has no tasks.

4.2 Initial Certification Analysis

Before discussing each task, it is important to note that each task will result in a Task Analysis Summary Report (TASR). Each TASR has its own individual name; for example, the TASR for Task 2-1 System Architecture Analysis is called the System Architecture Analysis Summary Report. As each TASR is completed, it is put into Appendix P Test and Evaluation Reports. The inputs to the TASR will depend on the task, but the outputs are always as follows[15]:

- Record of Findings
- Evaluation of Vulnerabilities
- Summary of Analysis of Level of Effort
- Summary of Tools Used and Results Obtained
- Recommendations

Additionally, for each task, a Minimum Security Activity Checklist (MSAC) must be completed, regardless of the Certification Level of the system. These checklists may be found in Appendix 2 of the DoD 8510.1-M DITSCAP Application Manual. When conducting the checklist, the options are 'Yes', 'No', or 'Not Applicable'. If the answer is 'Yes' or 'Not Applicable', no further action is required. If the answer is 'No', action must be taken to make the answer a 'Yes'. An excerpt of the MSAC for Task 2-1 System Architecture Analysis[16] has been provided as an example:

Table AP2.T1. Task 2-1 Level 1 Checklist

System Architecture Analysis	YES	NO	N/A
1. Does the systems architecture documentation describe the architecture, including graphics, of the system and interconnections providing or supporting, system functions?			

For this example, if the answer is 'Yes', the item is complete. If the answer is 'No', the systems architecture documentation must be corrected to accurately describe the system. Additionally, some questions may need to be added to the checklist in order to completely and accurately evaluate the system.

[15] DoD 8510.1-M, p. 68.

[16] DoD 8510.1-M, p. 146.

4.2.1 Task 2-1 System Architecture Analysis

This task determines how well the security requirements of the system have been integrated into the system and if they have been accurately described in the SSAA. For a Level 2 system, the MSAC must be completed, and a determination must be made to ascertain that the system is consistent with the appropriate architecture, such as the Joint Technical Architecture-Army 6.5. Additionally, it must be verified that the system complies with the architectural security requirements as stated in the SSAA and that the system maintains its integrity despite external interfaces. The security requirements of these external interfaces are identified in MOU/MOA, which are included in Appendix N Memorandums of Agreement. The inputs for this task are all system architecture documentation and system design specifications. The results are documented in the TASR called the System Architecture Analysis Summary Report.

4.2.2 Task 2-2 Software, Hardware, Firmware Design Analysis

The purpose of this task is to ensure the software, hardware, and firmware complies with the requirements stated in the SSAA, and the security features of the system have been implemented correctly. For example, all firewalls should be on the Army's IA Approved Tools list and configured in accordance with the Army Firewall Guidance documentation. If a firewall is not on the IA Approved Tools list, it must be approved by the Office of the CIO/G-6, and be in compliance with NSTISSP 11. NSTISSP 11 states that all IA or IA enabled products must be evaluated in accordance with Common Criteria (CC), National Information Assurance Partnership (NIAP), or Federal Information Processing Standards (FIPS) approved processes[17].

For a Level 2 system, the MSAC and an analysis of the system design, hardware, software, and firmware specifications and design documentation must be completed. The security critical components of the HW, SW, and FW must be identified and analyzed to ensure those components perform as stated in the SSAA. The inputs to this task are the TASR for Task 2-1, all system and security architecture documentation, and system design specifications. The results are documented in a TASR called the Software, Hardware, and Firmware Design Analysis Summary Report.

4.2.3 Task 2-3 Network Connection Rule Compliance Analysis

This task evaluates all current and planned connections to the system and ensures the system maintains its security. All connections must be evaluated for compliance as stated in the connection rules. These connection rules are described in the SSAA and stated in a MOU/MOA. Test plans and procedures to validate the security of these connections are also developed. The inputs into this task are the TASR for Task 2-1 and Task 2-2. The results are documented in a TASR called the Network Connection Rule Compliance Analysis Summary Report.

[17] NSTISSP 11, p. 2.

4.2.4 Task 2-4 Integrity Analysis of Integrated Products

The purpose of this task is to ensure that the integration into the system of Commercial Off The Shelf (COTS), Government Off The Shelf (GOTS), and Non-Developmental Items (NDI) do not cause security issues and that they comply with the SSAA. For a Level 2 system, the MSAC must be completed, and if the product has been evaluated in accordance with the CC, the certification team must verify the product is being used correctly. The inputs into this task are the TASR for Task 2-1 and Task 2-2. The results are documented in a TASR called the Integrity Analysis of Integrated Products Summary Report.

4.2.5 Task 2-5 Lifecycle Management Analysis

The purpose of this task is to ensure the Configuration Management practices are compliant with the SSAA and do not violate the security of the system. For a Level 2 system, the MSAC must be completed, and the Configuration Management practices must be verified to ensure the security features of the system maintain their integrity. For example, in order to ensure security, a software update must be tested in a lab before moving the change across the entire system. The inputs into this task include the following: all Lifecycle Management Plans, all Configuration Management documentation, any available software engineering procedures, and any trusted distribution plans. The results are documented in a TASR called the Lifecycle Management Analysis Summary Report.

4.2.6 Task 2-6 Security Requirements Validation Review

In this task, the procedures are developed to validate the system is in compliance with all the requirements identified in the RTM, and the system performs as stated in the SSAA. Each requirement may be validated through either one or a combination of the following: Interview, Document Review, Test, or Observation. For example, to verify that each user has the appropriate security clearance, the Certifier may Interview the Personnel Security Manager and Document Review the personnel files of a percentage of the system users. When developing the tests, each test should evaluate as many requirements as possible. In other words, one test that validates fifty requirements is better than fifty tests that validate one requirement each. The tests should be written in a way that is clear. For example, “The system will lock out a user after three failed logon attempts.” Rather than, “The system should lock out a user after three failed logon attempts.” Finally, whenever possible, automate the test. This will make the test much easier to run and less prone to error. The test should follow the following format from DoD 8510.1-M[18]:

[18] DoD 8510.1-M, p. 83.

Table C4.T4. Test Procedure Format

Test Number	
RTM Number	
Source	
Requirement Statement	
Test Objective	
Test Methodology	
Test Scenario	
Desired Results	
Actual Results	
Conclusions	
Vulnerability Analysis	

In addition to the creating the validation procedures, the MSAC for Task 2-6 must be completed. This task will result in Appendix H Security Test and Evaluation Plan and Procedures. There is no TASR for this task.

4.2.7 Task 2-7 Vulnerability Assessment

This task evaluates the vulnerability of the system, determines the residual risk to the system, and ensures appropriate countermeasures have been selected. When conducting this task, threats and vulnerabilities should be paired, the potential impact of the vulnerability being exploited must be identified, and the severity of impact must be explained. For a Level 2 system, the MSAC must be completed and all vulnerabilities identified in previous tasks must be evaluated. The input into this task includes the following: the TASR for Task 2-1 through Task 2-6, all system and security documentation, and any Independent Verification and Validation (IV&V) reports. An example of an IV&V is a report that the US Army Auditing Agency developed after conducting an assessment of the system. The results are documented in a TASR called the Vulnerability Assessment Summary Report.

4.3 Phase 2 Complete

Once all tasks within Phase 2 have been completed, the SSAA is updated, and the DAA, Certifier, User Representative, and Program Manager should all sign the SSAA. At this point, the system has been accurately described in the SSAA, all tests to validate the system have been developed, and the system is ready for Phase 3 Validation.

5.0 Phase 3 Validation

The purpose of this phase is to validate that the fully integrated and operational system performs as stated in the SSAA and maintains an acceptable level of residual risk. The goal of this phase is to obtain an Approval to Operate (ATO) the system. Phase 3 also consists of two activities, both of which must be accomplished, but only tasks that apply to the system must be completed. Each task within Phase 3 has its own TASR. The

inputs into each TASR will change, but the outputs will remain the same. Additionally, each task within Phase 3 also has a MSAC that must be completed. As each test is completed, it will be placed in Appendix P Test and Evaluation Report.

5.1 Certification and Evaluation of Integrated System

In this activity, the actual testing of the system is completed. This is accomplished in Task 3-1 through Task 3-8.

5.1.1 Task 3-1 Security Test and Evaluation (ST&E)

This test validates that the security features of the IS have been correctly implemented as stated in the SSAA, and the confidentiality, integrity, and availability of the system is maintained. For a Level 2 system, a MSAC must be completed. If the system's HW, SW, or FW security requirements have a corresponding technical test, that test must be performed to validate compliance. The inputs for this task are the Test Plan and Procedures developed in Phase 2. The results are documented in a TASR called the Security Test and Evaluation (ST&E) Summary Report.

5.1.2 Task 3-2 Penetration Testing

This task assesses the systems ability to resist intentional exploitation of its technical security vulnerabilities. Penetration testing is only required for Level 3 or 4 systems, but Level 1 and 2 systems must still complete the MSAC. Individuals that conduct penetration testing must meet the requirements in AR 380-53 Information System Monitoring, which requires training from the Army Computer Emergency Response Team (ACERT)[19]. One option is to have the 1st Information Operations Command (Land) (1st IOC (Land)) evaluate the system. The 1st IOC (Land) has two teams to test systems. The 1st IOC (Land) Blue Team works with the organization to evaluate the system from the inside and make recommendations to secure the system, and then the Red Team attempts to exploit the vulnerabilities of the system.

For a Level 2 system, the only requirement is that the MSAC be completed. If the 1st IOC (Land) does evaluate the system, this information is used in generating the TASR. The inputs for this task are the following: TASRs for Task 2-1 through Task 2-7, and any IV&V reports. The results are documented in a TASR called the Penetration Testing Summary Report.

5.1.3 Task 3-3 TEMPEST and Red-Black Verification

Task 3-3 is only completed if the system has TEMPEST requirements. This task ensures the system meets the TEMPEST and Red-Black requirements. For a Level 2 system, the MSAC must be completed and the Red-Black cables must be inspected for compliance. The results are documented in a TASR called the TEMPEST and Red-Black Verification Summary Report.

[19] AR 380-53, p. 6.

5.1.4 Task 3-4 COMSEC Compliance Verification

This task is only competed if the system has COMSEC requirements. This task ensures the appropriate COMSEC is used and the key management procedures protect the cryptographic keys. For a Level 2 system, the MSAC must be completed, and the key management procedures must be evaluated to ensure they are performed as stated in the SSAA. The input for this task is the Key Management Plan. The results will be documented in a TASR called the COMSEC Compliance Verification Summary Report.

5.1.5 Task 3-5 System Management Analysis

This task validates that the way the system is managed maintains effective security. For a Level 2 system, the MSAC must be completed and the way management procedures are conducted is compared to what is written in the SSAA. Individuals such as the Information Assurance Security Officer (IASO) must understand their roles and responsibility. Security policy must be evaluated to determine if it is effective. The inputs for this task are the TASRs for Task 2-5 and Task 2-7. The results are documented in a TASR called the System Management Analysis Summary Report.

5.1.6 Task 3-6 Site Accreditation Survey

This task ensures that the system, in its operational environment, maintains its confidentiality, integrity and availability, and the residual risk to the system and information being processed is acceptable. For a Level 2 system, the MSAC must be completed, and a site accreditation survey must be done to ensure the operational environment is described accurately in the SSAA. The results are documented in a TASR called the Site Accreditation Survey Summary Report.

5.1.7 Task 3-7 Contingency Plan Evaluation

This task ensures that a contingency plan that can be successfully implemented exists, has been tested, and meets the standard of AR 380-19 and DA PAM 25-1-1, Chapter 8, and Appendix E. For a Level 2 system, the MSAC must be completed, and the plan must be evaluated for completeness and feasibility, and it must have been tested within the past year. The input for this task is Appendix L Contingency Plans. The results are documented in a TASR called the Contingency Plan Evaluation Summary Report.

5.1.8 Task 3-8 Risk Management Review

The purpose of this task is to evaluate the threats and vulnerabilities to the system and determine if those threats are acceptable. For a Level 2 system, the MSAC must be completed and for each threat and vulnerability identified, a countermeasure must be implemented. For each residual risk, a statement explaining the rationale for accepting that residual risk must be written. Appendix J Rules of Behavior, Appendix K Incident Response Plan Appendix, and O Security Education, Training, and Awareness Plan must be evaluated to determine their effectiveness. The input for this task is the TASR for Task 2-7, and Appendices J, K, and O from the SSAA. The results are documented in a TASR called the Risk Management Review Summary Report.

5.2 Develop Recommendation

Once the Certifier and the Certification Team have completed all Phase 3 tasks, the Certifier must develop a recommendation for the DAA as to whether or not to accredit the system. The DAA then takes that recommendation and may issue an Approval to Operate (ATO), an Interim Approval to Operate (IATO), or terminate operation of the system. If an IATO is issued, there are some security concerns that must be addressed. A DAA may issue an IATO for a period up to 90 days, and it may be renewed once. A plan of action and milestones will also be established to bring the system up to an approved residual level of risk. If an ATO is issued, Phase 3 is complete.

5.3 Phase 3 Complete

Once Phase 3 is complete, the DAA, Certifier, User Representative, and Program Manger must sign the accreditation documentation. The system is now ready for the next phase of the DITSCAP, Phase 4 Post Accreditation.

6.0 Phase 4 Post Accreditation

The purpose of Phase 4 is to ensure the accredited system continues to operate in a secure manner with an approved residual level of risk. Contractors that perform the Certifier duties are not required to perform Phase 4 tasks unless it is stipulated in the contract.

Phase 4 consists of two activities: Systems Operations and Security Operations and Compliance Validation. Both activities must be accomplished, but only tasks that apply to the system must be completed. (NOTE: DoD 8510.1-M DITSCAP Application Manual refers to Compliance Validation as an activity in the flowchart on page 28, and also refers to Compliance Validation as a task on page 126. For the purpose of this paper, Compliance Validation will be considered an activity).

As with Phase 2 and Phase 3, each task within Phase 4 has its own TASR. The inputs into each TASR will change, but the outputs will remain the same. When completed, each TASR should be compared to the appropriate TASR from the previous phase to determine if any change requiring re-accreditation has occurred and then place in Appendix P Test and Evaluation Reports. Additionally, MSACs from each applicable Phase 2 and Phase 3 task must be completed.

6.1 Systems Operations and Security Operations

Systems Operations are the day-to-day activities of operating the system, while Security Operations can be considered the “what if” of operating the system. For example, when AR 25-X Information Assurance replaces AR 380-19 Information Systems Security, systems must meet all the requirements in the new regulation. At a minimum, this will require Task 4-1 Maintain SSAA, and Task 4-2 Physical, Personnel, and Management Control Review to be conducted. The “what if” is what makes Phase 4 difficult. Each time a change occurs to a system, specific Phase 2 and Phase 3 tasks must be repeated. Systems Operations and Security Operations has seven tasks which are discussed next.

6.1.1 Task 4-1 Maintain SSAA

For this task, all Certification Levels must keep the SSAA current, and submit any changes to the DAA, User Representative, and Program Manager for approval. If the Certifier is an active participant in Phase 4, he should also sign the updated SSAA. There is no TASR for this task.

6.1.2 Task 4-2 Physical, Personnel, and Management Control Review

This task revalidates the results of Task 2-5 Lifecycle Management Analysis, Task 3-5 System Management Analysis, Task 3-6 Site Accreditation Survey, Task 3-7 Contingency Plan Evaluation, and Task 3-8 Risk Management Review, as these tasks are the input for Task 4-2. For a Level 2 system, the aforementioned tasks are executed again, and the results are compared to the previous TASRs. This will ensure the physical, personnel, and procedural security procedures are performed as stated in the SSAA. The results are documented in a TASR called the Physical, Personnel, and Management Control Review Summary Report.

6.1.3 Task 4-3 TEMPEST Evaluation

This task in only conducted if the system has TEMPEST requirements. For this task, Task 3-3 TEMPEST and Red-Black Verification is revalidated. The results are documented in a TASR called the TEMPEST Evaluation Summary Report.

6.1.4 Task 4-4 COMSEC Compliance Evaluation

This task is only conducted if the system has COMSEC requirements. For this task, Task 3-4 COMSEC Compliance Verification is revalidated. The results are documented in a TASR called the COMSEC Compliance Summary Report.

6.1.5 Task 4-5 Contingency Plan Maintenance

Since DA Pam 25-1-1 requires contingency plans to be reviewed and tested annually, it is advantageous to conduct Task 4-5 at this time. In this task, Task 3-7 Contingency Plan Evaluation is revalidated. The results are documented in a TASR called the Contingency Plan Maintenance Summary Report.

6.1.6 Task 4-6 Configuration Management

The inputs for this task are the following: Task 2-5 Lifecycle Management Analysis, Task 3-5 System Management Analysis and Task 4-1 Maintain SSAA. Hence, the results of these former tasks are revalidated in Task 4-6. For a Level 2 system, the system must be monitored for any indication that it requires a recertification. Additionally, an IA individual must attend Configuration Control Board meetings and review all changes to the system before implementation. The results are documented in a TASR called the Configuration Management Summary Report.

6.1.7 Task 4-7 Risk Management Review

For this task, the results of Task 2-6 Security Requirements Validation Review, Task 3-6 Site Accreditation Survey, Task 3-7 Contingency Plan Evaluation, Task 3-8 Risk

Management Review, and Task 4-1 through Task 4-6 are used to determine if there are any new threats or vulnerabilities to the system. These threats and vulnerabilities may have arisen due to the following: changes in the system, changes in information processed on the system, or changes driven by external agency audits, such as the US Army Auditing Agency (USAAA). The results are documented in a TASR called the Risk Management Review Summary Report.

6.2 Compliance Validation

The SSAA designates specific periods of time when the system must be checked to validate that it is still operating at an acceptable residual level of risk. Compliance Validation consists of conducting all Phase 2 and Phase 3 tasks that were conducted for the initial certification. After conducting all of the applicable Phase 2 and Phase 3 tasks, the results of the new TASR are compared with the results of the previous TASR to determine if the system is exposed to additional risks. If the system is exposed to additional risks, a determination must be made regarding whether or not to re-accredit.

7.0 Conclusion

Phase 4 ends when the system meets one of the re-accreditation requirements outlined in Section 4.7 of the SSAA. If the re-accreditation requirements are met, the system begins the C&A process again starting at Phase 1. If the SSAA and all of the other documentation are still valid, then they may be reviewed and updated. For example, if the system is upgraded from Windows NT Server to Windows 2000 Server Active Directory, this requires re-accreditation. However, some portions of the contingency plan and all of the personnel security and physical security plans are probably still valid. This material would now just have to be reviewed to ensure it is up to date.

The DITSCAP is a time intensive process designed to ensure a system is secure in the environment in which it operates. Attentiveness to both Army and new DoD requirements will maintain the security of the system and facilitate all future C&A efforts.

References

1. United States. Department of Defense. DoD 8510.1-M DITSCAP Application Manual. 31 July 2000. (http://www.dtic.mil/whs/directives/corres/pdf/85101m_0700/p85101m.pdf) (5 September 2003)[20].
2. ---.---. DoDI 5200.40 Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). 30 December 1997. (http://www.dtic.mil/whs/directives/corres/pdf/i520040_123097/i520040p.pdf) (5 September 2003).
3. ---. Department of the Army. AR 25-1 Army Information Management. 31 May 2002. (http://www.apd.army.mil/pdffiles/r25_1.pdf) (5 September 2003).
4. ---. Department of Defense. DoDI 8500.2 Information Assurance Implementation. 6 February 2003. (http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf) (5 September 2003).
5. ---. National Security Telecommunications And Information Systems Security. NSTISSAM 2-95 TEMPEST. 12 December 1995. (http://cryptome.org/tempest-2-95.htm)(5 September 2003).
6. ---. Department of the Army. DISC4 MSG DTG 100733Z Sep 01 (http://ia.gordon.army.mil/disc4msg3.htm) (5 September 2003).
7. ---. ---. AR 380-19 Information Systems Security. 27 February 1998. (http://www.apd.army.mil/pdffiles/r380_19.pdf) (5 September 2003).
8. ---. National Security Telecommunications And Information Systems Security. NSTISSP 11. January 2000. (http://niap.nist.gov/niap/library/nstissp_11.pdf) (5 September 2003).
9. ---. Department of the Army. AR 380-53 Information System Security Monitoring. 29 April 1998. (http://www.apd.army.mil/pdffiles/r380_53.pdf) (5 September 2003).
10. ---. Department of Defense. DoDD 8500.1 Information Assurance. 24 October 2002. (http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf) (5 September 2003).
11. ---. Department of the Army. AR 380-5 Department Of The Army Information Security Program. 29 September 2000. (http://www.apd.army.mil/pdffiles/r380_5.pdf) (5 September 2003).
12. ---. ---. AR 380-67 Personnel Security Program. 9 September 1988. (http://www.apd.army.mil/pdffiles/r380_67.pdf) (5 September 2003).

[20] On 6 Oct 2003, all DoD references moved to a restricted access website. This website only allows users coming from a '.mil' or '.gov' domain to access the site. The publications are still unclassified and available by contacting the Directorate for Public Information & Analysis, Office of the Assistant Secretary of Defense for Public Affairs at (703) 428-0711.

13. ---. ---. DA Pam 25-1-1 Installation Information Services. 27 August 1991. (http://www.apd.army.mil/pdffiles/p25_1_1.pdf) (5 September 2003).

14. ---. ---. DA Pam 25-6 Configuration Management for Automated Information Systems. 13 June 1991. (http://www.apd.army.mil/pdffiles/p25_6.pdf) (5 September 2003).

15. ---. ---. HQDA LTR 25-03-1 Transition Of Information Assurance Duties And Responsibilities. 25 April 2003. ((http://www.apd.army.mil/pdffiles/l25_03_1.pdf) (5 September 2003).