Global Information Assurance Certification Paper

An Introduction to Certification and Accreditation

Author: Joseph Zadjura
Date: September 21, 2003
Certification: GSEC
Version: 1.4
Option: 1

I. Abstract

Going through the formal process of Certification and Accreditation (C&A) insures that a clearly established set of Security Requirements is developed and implemented, any residual risk is minimized and clearly understood, and all aspects of the development and deployment of security controls and policies are described in the System Authority Authorization Agreement (SSAA). This paper will examine the C&A process, the guidance that helps define the Security Requirements, and the responsible parties and their roles, to provide a basic understanding of C&A.

II. Introduction

Certification and Accreditation is a federally mandated standard process to insure that national security information systems meet documented security requirements and maintain the accredited security posture throughout their system life cycle (NIACAP 1). Since C&A is mandated upon all systems of the federal government, often it is taken as just a required step in order to stand up an information technology system, and no longer considered once the process is complete. However C&A, if taken in its intended spirit, can be an invaluable tool to manage the security of a system throughout its life cycle. Much of the process of a formal C&A could easily be applied to the commercial world to better understand and mange the security posture of any publicly exposed information technology system.

In order to understand C&A, it is important to distinguish between certification and accreditation. "Certification is the technical evaluation of the security components and their compliance for the purpose of accreditation" (Harris 264). A certifier, usually an independent third party, audits a system for compliance with an established set of security requirements. Then, "accreditation is the formal acceptance of the adequacy of the system's overall security by the management" (Harris 264).

Often, critical pieces of the security coverage are not implemented, or security policies are established, but not followed. The C&A process forces the establishment of security configurations, controls, policies, and procedures, and verifies their correct implementation.

III. Overview

Both the DITSCAP and NIACAP define the C&A process by using a four-phase approach: definition, verification, validation, and post accreditation. Each guidance document describes the various tasks implemented in each phase. For example: "Phase 1, Definition, is focused on understanding the mission environment, and architecture to determine the Security Requirements and level of effort necessary to achieve accreditation." (DITSCAP 17) Unfortunately, the description of this phase lacks the details of how the Security Requirements are actually developed. So, instead of using the four-phase example, this paper will list the tasks necessary for achieving accreditation status, and then will describe each task in more detail.

A brief overview of the C&A tasks can be described as follows:

1. A list of guidance documents is compiled from all applicable directives and policy guidelines to define the rules that the C&A process will follow, and to help define a set of Security Requirements for the system.
2. Persons and organizations are chosen to fill the roles defined by the C&A guidance documents.
3. The scope of the system being certified is determined.
4. A list of Security Requirements that are relevant to the system are created based on the chosen guidance documents.
5. A System Security Authorization Agreement (SSAA) document is created containing all of the relevant information about the system.
6. A set of test procedures are developed from the security requirements.
7. A System Test and Evaluation (ST&E) is performed by the certifiers, and a report of the relevant findings is generated.
8. Once all of the security findings are sufficiently addressed and verified, a Risk Assessment is performed to describe the severity of the residual risk.
9. A recommendation is made by the Certifiers to the Designated Approving Authority (DAA).
10. The system is either accredited, granted an Interim Authority to Operate, or denied accreditation by the DAA.

Some of these steps can be performed in a different order, and additional steps can be added or removed depending on the specifics of the system. But the previous list represents the basic set of tasks necessary for achieving accreditation status. Next, each step will be described in more detail to demonstrate the effectiveness of the C&A process.

IV. Guidance

Process, Scope, and Roles

Currently the main documents that define the C&A process, scope, and roles are the DISTCAP and NIACAP. The DITSCAP, or Department of Defense Information Technology Security and Accreditation Process, is the C&A guidance for federal departments and agencies that fall under the Department of Defense. The NIACAP, or National Information Assurance Certification and Accreditation Process, is the guidance for all other departments, agencies, and bureaus of the executive branch of the federal government.

Many of the systems in the world of the DoD deal with classified information. As such, the protection of the confidentiality, integrity, and availability of these systems are a matter of national security. In other areas of the government, such as the IRS, the information is considered Sensitive but Unclassified or SBU. Thus, personal tax information or social security numbers are sensitive information, but not a mater of national security. Because of the different nature of the information being protected, the DISTCAP and NIACAP take a slightly different approach to the C&A of a system. For the most part, however, the two guidance documents are very analogous, and these two documents define the "standard process to insure that national security information systems meet documented security requirements and maintain the accredited security posture throughout their system life cycle" (DITSCAP 1).

Requirements

The security requirements are derived from various government laws and directives, government and commercial guidance documents, and security industry best practices. Here are some examples of requirements guidance:

- Office of Budget and Management Circular No. A-130. This circular establishes policy for the management of Federal information resources
- Treasury Directive TD-P 71-10, Department of Treasury Security Manual
- Treasury Directive TD 85-01, Department of the Treasury Information Security Program. This document contains Treasury policy on securing an IT Solution.
- FIPS 140-2. Security Requirements for Cryptographic Modules.

Document Content and Format

The C&A process involves creating a great deal of documents relating to the security of the IT System, and there is much guidance on the form and content of these documents. Here are some examples:

- NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems.
- NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems
- DISTCAP Annex A, System Security Authorization Agreement Outline.
- NIST Special Publication 800-30, Risk Management Guidelines for Information Technology Systems

The given examples are just a few of the many guidance documents that can come into play during the C&A process. Since the scope of this paper is just an introduction to C&A, an example will be used to illustrate how some of the guidance documents apply.

Guidance Document Example

Suppose that a fictitious bureau is seeking to certify and accredit an information technology system, such as a web site. This bureau, the Bureau of Fiction (BoF), is a part of the Department of Treasury, and requires a web site that is accessible to the general public to make available information about the BoF's fictitious functions. In addition, privileged members of the BoF must have administrative access through a Virtual Private Network (VPN) to the web site to post new information.

Here are the types of Guidance Documents would apply to our example.

Selection of Guidance Documents:

- Since the BoF is a bureau under the Department of Treasury, the NIACAP would be the defining document for the C&A process. The NIACAP would help define the scope of the C&A effort, the roles and responsible parties, the process to verify and validate the system, and the format of the System Security Authorization Agreement (SSAA).
- OMB A-130 would help establish policies for the management of the system (OMB A-130 1).
- Since this is a Treasury system, the TD 85-01 would define much of the security requirements.

- FIPS 140-2 would be necessary, since the VPN is using cryptographic modules (Casar 1).
- NIST 800-26 is a questionnaire that helps determine the current state of security controls and policy for the system (Swanson iv)
- NIST 800-18 shows the correct format and content of the Security Plan (Swanson 1)
- NIST Special Publication 800-30, Risk Management Guidelines for Information Technology Systems would apply and demonstrates how to perform a cost-benefit analysis, mitigate risk, and understand residual risk (Feringa 37)

V. Defining Roles

The NIACAP establishes a minimum set of Roles to be defined for the C&A:

- The Program Manager is the person responsible for the project as a whole.
- The Certifier or Certification team should be chosen such that there is, at a minimum, a separate chain of command from the project in order to eliminate any conflict of interest. A third party contracting company is ideal.
- A User Representative is responsible for insuring that the security implementation does not unnecessarily impede on the functionality of a system from the user's perspective.
- The Designated Approving Authority should be a person with the power to fund any necessary additional security implementations that are recommended by the certifiers.

Several other roles may be defined as needed, such as the Information Systems Security Officer (ISSO). The ISSO usually is a key player in the development and maintenance of the various security features and policies of the System. (DITSCAP 2)

The NIACAP and DITSCAP define the various roles, and their respective responsibilities in more detail.

VI. Scoping out the system

Once the roles have been established, the key players meet to determine the scope of the C&A effort. The system boundaries are determined by function and by determining whether or not the DAA has control of each particular part of the system. If a major portion of the system is not under the control of the DAA, an additional DAA would be necessary, and the final accreditation would be determined by the approval of both DAA's.

VII. Creation of Security Requirements

A set of Security Requirements are developed based on the various guidance documents that apply. The TD 85-01 and other guidance documents contain a great deal of required security implementations and policies. These can be intentionally vague because of the rapid pace of changes in the security arena and technology in general. The Security Requirements take the various guidance, and more specifically establishes formal requirements necessary to secure the system. The creation of a complete and comprehensive set of Security Requirements is essential to the C&A process, since it is the baseline on which the certification effort takes place.

Once the Security Requirements are established, a Requirements Traceability Matrix (RTM) is created. The RTM lists each requirement, the guidance document that the requirement is developed from, and the security feature or policy that satisfies that particular requirement. Now there is a direct mapping between each security directive from the various guidance documents and a security feature or policy that satisfies that directive through the security requirement.

VIII. Development of the SSAA

Development of the SSAA is a step that can begin at any time during the C&A effort. Ideally, the SSAA would start to be developed during the initial design of the system, since many of the Security Requirements can affect the design of the system. The NIACAP suggests having four phases of development of a system, and lists tasks associated with each of the four mandatory roles during each phase. This four-phase approach is the ideal scenario, but is not mandatory. In fact, the SSAA can be developed at any time during the C&A process, but clearly the earlier the SSAA is started, the more it benefits the system. If the SSAA is developed too late in the project, many changes to the system may be necessary to meet the requirements of the SSAA.

The NIACAP Annex A lists the basic outline of the contents of the SSAA, and they are as follows:

1.0 MISSION DESCRIPTION AND SYSTEM IDENTIFICATION
- 1.1 System Name and Identification
- 1.2 System Description
- 1.3 Functional Description
  - 1.3.1 System Capabilities

APPENDIX C. References
APPENDIX D. Security Requirements and/or Requirements Traceability Matrix
APPENDIX E. Security Test and Evaluation Plan and Procedures
APPENDIX F. Certification Results
APPENDIX G. Risk Assessment Results
APPENDIX H. Certifier's Recommendation
APPENDIX I. System Security Policy
APPENDIX J. System Rules of Behavior
APPENDIX K. Security Operating Procedures
APPENDIX L. Contingency Plan(s)
APPNEDIX M. Security Awareness and Training Plan
APPENDIX N. Personnel Controls and Technical Security Controls
APPENDIX O. Incident Response Plan
APPENDIX P. Memorandums of Agreement – System Interconnect Agreements
APPENDIX Q. Applicable System Development Artifacts or System Documentation
APPENDIX R. Accreditation Documentation and Accreditation Statement

Each section should contain as much information as can be defined for the system. Occasionally, there is a separate document that covers the contents of a section. For example, the Security CONOPS is usually a separate document, and can be summarized and referenced in section 4.4 of the SSAA. Much of the separate documentation is added as an appendix to the SSAA. This helps make the SSAA a very complete description of the state of security of the given system. It is vital to keep the SSAA up to date as changes are made to the system even after the system is accredited, so that the SSAA remains a complete security reference of the system.

IX. Development of Test Procedures

The test procedures are developed directly from the Security Requirements. For a successful certification effort, every Security Requirement MUST have a test procedure created, so that each requirement's implementation has been verified. There are several methods of testing a particular Security Requirement, depending on the type of implementation. Expanding on our previous example, BoF has a Security Requirement that states "passwords must expire after 90 days." The test procedure associated with this requirement should be a step-by-step guide to actually checking the configuration of each machine that is part of the system. This method of testing would be inspection. Another type of testing is documentation. Part of the SSAA document is to have a Security Awareness Training Plan. The certifier must validate that the training plan is complete and adequate for the system's security needs. Test procedures can also be tested by interview,

such as verifying that users have received proper security awareness training.

X. Security Test and Evaluation

Once the Test Procedures have been developed, the Security Test and Evaluation (ST&E) can begin. Members of the Certification Team take the test procedure and perform each test with the assistance of a representative of the system. For example, many test procedures deal with the configuration of the operating system of the various components of the system. In order to test that the correct configuration of the component has been achieved, a systems administrator that is responsible for that particular component will actually perform the test, and the certifier will validate the results. The reason the certifier does not actually perform the test procedure is to maintain the integrity of the test by demonstrating a distinct separation of duties.

Other test procedures deal with policies and procedures. In this case, the certifier will obtain copies of the various documents that satisfy the Security Requirements and review the documents for completeness and adequacy. Also, the certifier can interview members of the system's staff and management to ensure that the stated policies are understood by the critical personnel of the project.

In each test, a verdict is established. These verdicts are typically Pass, Fail, or Re-Test. In the case of Pass, the certifier must initial the test results to validate the test procedure. In the case of fail, a comment is noted on the test procedure giving the reason for the failure, and the certifier initials the results to validate the test procedure. In the case of Re-Test, a comment is noted why the test was not completed, and plan for retesting the procedure. Again the certifier must initial the results.

Once all of the test procedures have been performed, the findings are prepared. In the case of document review, a copy of comments made by the certification team should be presented to the author of the document and to the management. Changes are made to the documents to satisfy the Security Requirements, and are then validated by the Certification Team. In the case of configuration issues, any findings are sent to the administrators, and the management. Once the configuration issues have been resolved, the failed tests are repeated to validate that the Security Requirement has been satisfied.

Occasionally there are legitimate reasons why a specific Security Requirement can not be met. Suppose that the BoF web site consists of several servers that must communicate with each other. In order to pass

information, authentication credentials must be confirmed for each transaction. One of BoF's Security Requirements is that each account's password must expire after 90 days. In the case of a normal user, usually a warning is issued that the user's password is going to expire, and the user is given an opportunity to change the password. Unfortunately the system passwords could expire without any person receiving a warning. This would lead to the system losing function without warning. In this case, it would be better to have the system account passwords NOT expire, but have a policy established that the system administrator change the passwords in the 90 day interval. This example is a matter of balancing the risks. And as such, this particular case should be explained in detail in the Risk Assessment document.

XI. Risk Assessment

Satisfying each and every Security Requirement does not guarantee the complete security of a system. Any system with exposure to the outside world has some level of risk associated with it. The Security Requirements are developed to minimize the amount of risk involved without losing the necessary functionality of the system. Any residual risk left after all the Security Requirements are implemented must be addressed in a Risk Assessment. This is one of the most important parts of the C&A process, because this will be the main document used by the DAA in making the determination of accreditation. Most of the development of the Risk Assessment can be completed independent of the testing, since most, if not all, of the Security Requirements should eventually be met. But as illustrated in the ST&E section of this document, there are times that individual Security Requirements are not met, and must be addressed in the Risk Assessment. Therefore, the final Risk Assessment document should be considered complete after the complete review of the ST&E results.

XII. Presentation of Results and DAA Approval

Once the entire C&A package has been put together, it is presented to the DAA. It can be delivered to the DAA for review, but often times the DAA is briefed by the Certification Team. The DAA must review the entire package and make a determination. The DAA can approve of the C&A granting the system full operating status, grant an Interim Authority to Operate (IATO), or deny the C&A. Denials are very rare, since the DAA is usually kept in the loop as far as the progress and issues concerning the C&A. Therefore, the Certification Team, and project managers are well informed of the opinion of the DAA, and can make modifications to the security stature of the system in order to minimize the risk of a denial of accreditation. If the system is granted an accreditation, the C&A is valid for three years. A new C&A effort

must be made prior to the expiration of the previous C&A in order to maintain the accreditation status.

If the system has been granted an IATO, the DAA assigns a time period that the IATO is valid for. Normally the time frame is six months, but can be adjusted by the DAA depending on the situation. IATO's are usually granted in cases where there is not sufficient time to produce a full C&A package. The minimum set of requirements for an IATO is to produce a Security Plan, and perform the ST&E Testing including vulnerability scans, and create the ST&E Report. This way, the system can be developed, secured, and granted and IATO. During the IATO period, the C&A team can finish developing the rest of the necessary documentation, such as the SSAA and all associated attachments and appendices.

XIII. Conclusion

Going through the formal process of a C&A may seem cumbersome, but the results are well worth it. It would be a rare instance that an ST&E procedure has been performed without finding errors in the configuration of mandatory security controls. Validating these controls makes the C&A important, but there are a great deal of additional benefits of a C&A.

- Demonstrating compliance with all federal directives and laws
- Establishment of a complete set of Security Requirements
- Independent verification of the correct implementation of the Security Requirements
- A formal analysis of the residual risk once all the Security Requirements have been met
- All of the various documentation associated with the development, deployment, and maintenance of the system as it relates to security is contained in one set of documents, the SSAA

These are the major benefits of a formal C&A, but invariably each project will take away what it puts into the C&A process. Once an accreditation is achieved, in is vital that the C&A process continues as changes are made to the system.

XIV. The Future of C&A

Recently, a new set of guidance for C&A has come out of the National Institute of Science and Technology (NIST). So far NIST has released Special Publication 800-37 "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems." Once approved,

this publication will override the NIACAP and DITSCAP in order to standardize the C&A process across all federal departments and agencies. Much of the content is the same as the DITSCAP and NIACAP, so the process will change little. One interesting difference of the 800-37 in comparison to the NIACAP, is the 800-37 defines categories of accreditation, low, moderate, and high (Ross 12). A high level of accreditation means a higher level of security of the system, and therefore has more strict requirements for achieving accreditation. The problem with a one size fits all C&A is that many simple systems, such as BoF's web server, can spend more funds performing the C&A than on the system itself. And since the web site was intended to distribute publicly available information, the value of the loss of the system is well under the cost of the C&A to secure it.

With the NIST 800-37 categorization scheme, BoF's system would likely have a category low C&A. This would help control the costs of the C&A, but still insure that the system has met a minimum set of directives in order to secure the system.

Conversely, a critical system would seek to achieve a high category C&A in order to insure the system has achieved a maximum level of security. The difference of categories of C&A helps to customize the C&A process to the systems needs, and will help to streamline the process for simple systems, as well as maximize the security of complex systems.

XV. References

Casar, T., et al. "Federal Information Processing Standards Publication (FIPS) 140-2," May 25, 2001
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Department of Defense (DoD) Instruction No. 5200.40. "DoD Information Technology Security Certification and Accreditation Process (DISTCAP)," December 30, 1997
http://www.dtic.mil/whs/directives/corres/pdf/i520040_123097/i520040p.pdf

National Security Telecommunications and Information System Security Instruction (NSTISSI). "No.1000, National Information Assurance Certification and Accreditation Process (NIACAP)," April 2000
http://www.nstissc.gov/Assets/pdf/nstissi_1000.pdf

Feringa, A., et al. "NIST SP 800-30, Risk Management Guidelines for Information Technology Systems," January 30, 2002,
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Harris, Shon. All in One CISSP Certification Exam Guide. McGraw-hill/Osborne, 2002

Office of Management and Budget Circular No. A-130. "Management of Federal Information Resources," February 8, 1996
http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

Ross, R., Swanson, M. "NIST SP 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems," June 30, 2003,
http://csrc.nist.gov/publications/drafts/sp800-37-Draftver2.pdf

Swanson, M. "NIST SP 800-18, Guide for Developing Security Plans for Information Systems," December 1, 1998
http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.pdf

---. "NIST SP 800-26, Security Self Assessment Guide for Information Technology Systems," November 1, 2001
http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf

Treasury Directive Publication (TD P) 71-10, "Department of Treasury Security Manual," Aug. 23, 1999

Treasury Directive Publication (TD P) 85-01, "Treasury IT Security Program," February 13, 2003